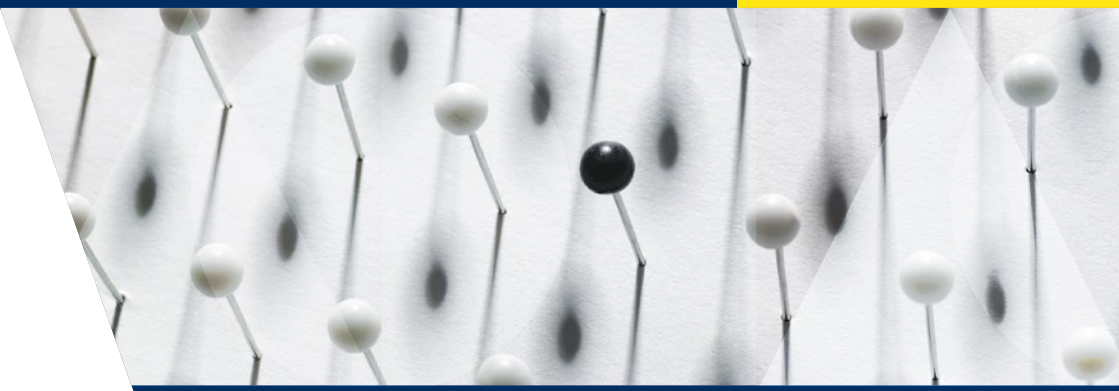
KÉZIKÖNYV



Európai adatvédelmi jogi kézikönyv

2018. évi kiadás

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

A kézikönyv kézirata 2018 áprilisában készült el.

Az aktualizált változatok a későbbiekben elérhetőek lesznek az FRA honlapján: fra.europa.eu, az Európa Tanács honlapján: coe.int/dataprotection, az Emberi Jogok Európai Bírósága honlapján az „Ítélkezési gyakorlat" (Case-Law) menüpont alatt: echr.coe.int és az európai adatvédelmi biztos honlapján: edps.europa.eu.

Fotó (borító és belső): © iStockphoto

Luxembourg: Az Európai Unió Kiadóhivatala, 2019

ET:	ISBN 978-92-871-9830-3		
FRA – print:	ISBN 978-92-9474-291-9	doi:10.2811/544942	TK-05-17-225-HU-C
FRA – web:	ISBN 978-92-9474-290-2	doi:10.2811/55214	TK-05-17-225-HU-N

Európai adatvédelmi jogi kézikönyv

2018. évi kiadás

Előszó

A társadalmak egyre digitalizáltabbakká válnak. A technológiai fejlődés sebessége, illetve a személyes adatok kezelésének a módja mindannyiunkra nap mint nap – ezeknek a változásoknak a fényében – sokféle módon hatással van. Az utóbbi időben kerültek felülvizsgálatra az Európai Unió (EU) és az Európa Tanács azon szabályozási keretei, amelyek a magánélet és a személyes adatok védelmét garantálják.

Európa világszinten is élen jár az adatvédelem területén. Az EU adatvédelmi szabványai az Európa Tanács 108. Egyezményén, uniós jogi eszközökön – köztük az általános adatvédelmi rendeleten, valamint a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelven –, valamint az Emberi Jogok Európai Bíróságának és az Európai Unió Bíróságának vonatkozó ítélkezési gyakorlatán alapulnak.

Az EU és az Európa Tanács által folytatott adatvédelmi reformok kiterjedtek, időnként összetettek, továbbá széles körű előnyökkel és hatásokkal járnak a magánszemélyekre és a vállalkozásokra nézve. A jelen kézikönyv célja az adatvédelmi szabályokkal kapcsolatos tudatosság növelése és az ezekkel kapcsolatos ismeretek fejlesztése, különösen a jogász szakma olyan nem szakosodott gyakorlói számára, akik munkájuk során adatvédelmi problémákkal szembesülnek.

A jelen kézikönyvet az Európai Unió Alapjogi Ügynöksége (FRA) készítette az Európa Tanáccsal (az Emberi Jogok Európai Bíróságának hivatalával együtt) és az európai adatvédelmi biztossal együttműködésben. A kézikönyv frissíti a 2014-es kiadást, és az az FRA és az Európa Tanács együttműködésében megvalósuló jogi kézikönyvsorozat részét képezi.

Köszönettel tartozunk Belgium, az Egyesült Királyság, Észtország, Franciaország, Grúzia, Írország, Magyarország, Monaco, Olaszország és Svájc adatvédelmi hatóságainak a kézikönyv tervezeteire vonatkozó hasznos visszajelzéseikért. Szeretnénk továbbá kifejezni elismerésünket az Európai Bizottság adatvédelmi osztályának, valamint a nemzetközi adatáramlási és adatvédelmi osztályának. Köszönettel tartozunk az Európai Unió Bíróságának a jelen kézikönyv előkészületi munkálatai során nyújtott dokumentációért. Végül szeretnénk kifejezni köszönetünket a Nemzeti

Adatvédelmi és Információszabadság Hatóságnak (NAIH) a kézikönyv fordításának ellenőrzésében végzett tevékenységéért.

Christos Giakoumopoulos

Az Európa Tanács Emberi Jogok és Jogállamiság Főigazgatóságának igazgatója

Giovanni Buttarelli

Európai adatvédelmi biztos

Michael O'Flaherty

Az Európai Unió Alapjogi Ügynökségének igazgatója

Tartalomjegyzék

Rövidítések és betűszavak

108. Egyezmény	Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (Európa Tanács). Az Európa Tanács Miniszteri Bizottsága a dániai Elsinore-ban megtartott 128. ülésén (2018. május 17–18.) elfogadta a 108. Egyezmény módosító jegyzőkönyvét (CETS 223). A továbbiakban a „Korszerűsített 108. Egyezményre" történő hivatkozás a CETS 223-as számú jegyzőkönyv által módosított egyezményre utal.
BCR	Kötelező erejű vállalati szabály
CCTV	Zárt láncú televízió
CETS	Az Európa Tanács Szerződéseinek Tára
Charta	Az Európai Unió Alapjogi Chartája
CRM	Ügyfélkapcsolat-kezelés
C-SIS	Schengeni Információs Rendszer „Központi Rész"
DPA	Adatvédelmi hatóság
DPO	Adatvédelmi tisztviselő
EAW	Európai elfogatóparancs
EDPB	Európai Adatvédelmi Testület
EDPS	Európai adatvédelmi biztos
EFSA	Európai Élelmiszerbiztonsági Hatóság
EFTA	Európai Szabadkereskedelmi Társulás
EGT	Európai Gazdasági Térség
EJEB	Az Emberi Jogok Európai Bírósága
EJEE	Az emberi jogok európai egyezménye
EK	Európai Közösség
ENISA	Európai Uniós Hálózat- és Információbiztonsági Ügynökség
ENSZ	Az Egyesült Nemzetek Szervezete
ESMA	Európai Értékpapírpiaci Hatóság
eTEN	Transzeurópai távközlő hálózatok
EU	Európai Unió

EUB	Az Európai Unió Bírósága (2009 decembere előtt: Európai Bíróság)
eu-LISA	A nagyméretű informatikai rendszerekkel foglalkozó ügynökség
EUMSZ	Az Európai Unió működéséről szóló szerződés
EuroPriSe	Európai adatvédelmi bizalompecsét
EUSZ	Az Európai Unióról szóló szerződés
FRA	Az Európai Unió Alapjogi Ügynöksége
GPS	Globális helymeghatározó rendszer
HL	Hivatalos Lap
ICCPR	Polgári és Politikai Jogok Nemzetközi Egyezségokmánya
IKT	Információs és kommunikációs technológia
ISP	Internetszolgáltató
JSB	Közös ellenőrző szerv
NGO	Nem kormányzati szervezet
N-SIS	Nemzeti schengeni információs rendszer
OECD	Gazdasági Együttműködési és Fejlesztési Szervezet
PIN	Személyi azonosító szám
PNR	Utasnyilvántartási adatállomány
SEPA	Egységes eurófizetési térség
SIS	Schengeni Információs Rendszer
SWIFT	Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság
UDHR	Az Emberi Jogok Egyetemes Nyilatkozata
VIR	Váminformációs rendszer
VIS	Vízuminformációs Rendszer

Útmutató a kézikönyv használatához

Ez a kézikönyv összefoglalja az Európai Unió (EU) és az Európa Tanács által meghatározott jogi előírásokat az adatvédelemhez kapcsolódóan. A kézikönyv olyan jogi szakembereknek nyújt segítséget, akik nem az adatvédelem területén dolgoznak; ügyvédeknek, bíráknak vagy más gyakorló jogi szakembereknek, valamint egyéb – például nem kormányzati (NGO) – szervezeteknél dolgozó munkatársaknak, akik munkájuk során adatvédelemmel kapcsolatos jogi kérdésekkel találkozhatnak.

A kézikönyv elsődleges hivatkozási alapul szolgál a vonatkozó uniós jogszabályok és az emberi jogok európai egyezménye (EJEE), valamint az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezménye (108. Egyezmény) és az Európa Tanács más jogi eszközei tekintetében.

Minden fejezet egy táblázattal kezdődik, amely összefoglalja az adott fejezetben tárgyalt témákra vonatkozó jogi rendelkezéseket. A táblázatok egyaránt kitérnek az Európa Tanács és az EU jogára, továbbá az Emberi Jogok Európai Bírósága (EJEB), valamint az Európai Unió Bírósága (EUB) válogatott jogeseteit is tartalmazzák. Ezután egyesével bemutatja a két európai jogrend vonatkozó jogszabályait, ahogyan azok a konkrét témákra vonatkoznak. Az olvasó ezáltal megismerheti a két jogrendszer hasonlóságait és különbségeit. Ez segíti a felhasználókat a saját helyzetükre vonatkozó legfontosabb információk megtalálásában is, különösen ha csak az Európa Tanács jogszabályainak hatálya alá tartoznak. Egyes fejezetekben a témakörök sorrendje ettől kissé eltérhet a fejezeten belül, ha ez a fejezet tartalmának tömör bemutatása szempontjából kedvezőbb. A kézikönyv rövid áttekintést nyújt az Egyesült Nemzetek Szervezetének keretéről is.

Azon nem uniós tagállamoknak a gyakorló szakemberei, amelyek az Európa Tanácsnak tagállamai, és ezáltal az EJEE-nek és a 108. Egyezménynek részes felei, a saját országukra vonatkozó információkat az Európa Tanácsra vonatkozó részekben találják meg. A nem uniós tagállamok gyakorló szakemberei is tartsák szem előtt, hogy az EU általános adatvédelmi rendeletének elfogadása óta az EU adatvédelmi szabályai a nem az EU-ban létrehozott szervezetekre és egyéb jogalanyokra is vonatkoznak, ha azok az Unióban személyes adatokat kezelnek, és uniós érintettek számára kínálnak árukat és szolgáltatásokat, vagy nyomon követik ilyen érintettek viselkedését.

Az uniós tagállamok szakembereinek mindkét részt tanulmányozniuk kell, mivel ezekre az államokra mindkét jogrend érvényes. Hangsúlyozni kell, hogy az európai adatvédelmi szabályok reformjára és modernizációjára mind az Európa Tanács (a CETS 223-as számú jegyzőkönyv által módosított „Korszerűsített 108. Egyezmény"), mind az EU (az általános adatvédelmi rendelet és az (EU) 2016/680 irányelv elfogadása) által párhuzamosan került sor. Mindkét jogrendszer szabályozói kiemelt gondosságot fordítottak annak biztosítására, hogy a két jogi keret következetes és összeegyeztethető legyen. Ennek következtében a reformok az Európa Tanács és az EU adatvédelmi jogszabályainak nagyobb mértékű harmonizációját eredményezték. Azoknak, akik egy konkrét kérdésről szeretnének többet megtudni, a kézikönyv végén található, speciálisabb anyagokat is tartalmazó „Irodalomjegyzék" című részt érdemes tanulmányozniuk. A módosító jegyzőkönyv hatályba lépéséig alkalmazandó 108. Egyezménnyel és annak 2001-es kiegészítő jegyzőkönyvével kapcsolatos információkat az olvasók a kézikönyv 2014-es kiadásában találják.

Az Európa Tanács jogszabályainak ismertetéséhez röviden bemutatjuk az EJEB válogatott ügyeit. Ezeket az EJEB adatvédelmi kérdésekről szóló nagyszámú ítélete és határozata közül választottuk ki.

A vonatkozó uniós jog az eddig elfogadott jogalkotási intézkedéseket, valamint a Szerződések és az Európai Unió Alapjogi Chartája vonatkozó rendelkezéseit foglalja magában az EUB ítélkezési gyakorlatából következő értelmezés szerint. Emellett a kézikönyv bemutatja a 95/46/EK irányelv 29. cikke alapján létrehozott, a személyesadat-feldolgozás vonatkozásában az egyének védelmével foglalkozó munkacsoport (a továbbiakban: 29. cikk szerinti munkacsoport) által elfogadott véleményeket és iránymutatásokat. A munkacsoport az adatvédelmi irányelv értelmében megbízott tanácsadó szervezet, amelynek a feladata, hogy szakértő tanáccsal lássa el az uniós tagállamokat, és amelyet 2018. május 25-től felvált az Európai Adatvédelmi Testület (EDPB). Az európai adatvédelmi biztos véleményei szintén fontos betekintést nyújtanak az uniós jog értelmezésébe, ezért ezek is szerepelnek a kézikönyvben.

A kézikönyvben bemutatott vagy idézett ügyek az EJEB és az EUB jelentős ítélkezési gyakorlatából hoznak példákat. A kézikönyv végén szereplő iránymutatások az ítélkezési gyakorlat online keresésében kívánják segíteni az olvasókat. A EUB bemutatott ítélkezési gyakorlata a korábbi adatvédelmi irányelvhez kapcsolódik. Az EUB értelmezései azonban továbbra is érvényesek az általános adatvédelmi rendelet által létrehozott megfelelő jogokra és kötelezettségekre.

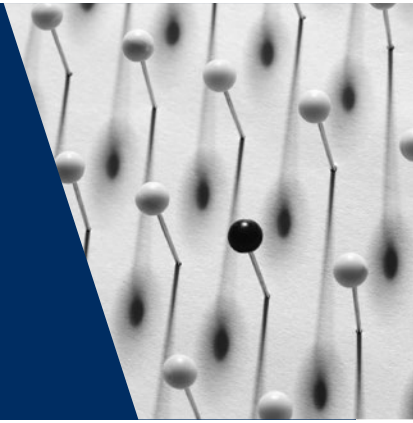
Ezenfelül, a kék hátterű keretes szövegekben gyakorlati példákat hozunk feltételezett esetekkel, amelyek az európai adatvédelmi szabályok gyakorlati alkalmazását szemléltetik, különösen azokban az esetekben, ahol az EJEB-nek vagy az EUB-nak nincs a témában konkrét ítélkezési gyakorlata. Egyéb – szürke hátterű – keretes szövegek az EJEB és az EUB ítélkezési gyakorlatától eltérő forrásokból származó példákat mutatnak be, például a 29. cikk szerinti munkacsoport által kiadott jogszabályokat vagy véleményeket.

A kézikönyv az EJEE és az európai uniós jog által létrehozott két jogrendszer szerepének rövid leírásával kezdődik (1. fejezet). A 2–10. fejezet a következő kérdéseket tárgyalja:

- adatvédelmi terminológia;
- az európai adatvédelmi jog alapelvei;
- az európai adatvédelmi jog szabályai;
- független felügyelet;
- az érintettek jogai és e jogok érvényesítése;
- a személyes adatok határokon átnyúló továbbítása és áramlása;
- adatvédelem a rendőrségi és büntető igazságszolgáltatási területen;
- konkrét területek egyéb egyedi európai adatvédelmi szabályai;
- a személyes adatok védelmének modern kori kihívásai.

1

Az európai adatvédelmi jog kontextusa és háttere



EU	Tárgyalt kérdések	Európa Tanács
Az adatvédelemhez való jog		
Az Európai Unió működéséről szóló szerződés, 16. cikk Az Európai Unió Alapjogi Chartája (Charta), 8. cikk (a személyes adatok védelméhez való jog) 95/46/EK irányelv a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról (adatvédelmi irányelv), HL L 281., 1995 (2018 májusáig hatályos) A Tanács 2008/977/IB kerethatározata a büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés keretében feldolgozott személyes adatok védelméről, HL L 350., 2008 (2018 májusáig hatályos) (EU) 2016/679 rendelet a természetes személyeknek a személyes adatok kezelése tekintetében történő védelméről és az ilyen adatok szabad áramlásáról, valamint a 95/46/EK rendelet hatályon kívül helyezéséről (általános adatvédelmi rendelet), HL L 119., 2016		EJEE, 8. cikk (magán- és családi élet, lakás és kapcsolattartás tiszteletben tartásához való jog) Korszerűsített egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (Korszerűsített 108. Egyezmény)

EU	Tárgyalt kérdések	Európa Tanács
(EU) 2016/680 irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről (a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv), HL L 119., 2016 2002/58/EK irányelv az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), HL L 201., 2002 45/2001/EK rendelet a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról (uniós intézmények adatvédelmi rendelete) HL L 8., 2001		
A személyes adatok védelméhez való jog korlátozásai		
Charta, 52. cikk, (1) bekezdés Általános adatvédelmi rendelet, 23. cikk EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010		EJEE, 8. cikk, (2) bekezdés Korszerűsített 108. Egyezmény, 11. cikk EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008
A jogok közötti egyensúly		
EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010	Általánosságban	
EUB, *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy* [nagytanács], C-73/07. sz. ügy, 2008 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014	A véleménynyilvánítás szabadsága	EJEB, *Axel Springer AG kontra Németország* [Nagykamara], 39954/08. sz. ügy, 2012 EJEB, *Mosley kontra Egyesült Királyság*, 48009/08. sz. ügy, 2011 EJEB, *Bohlen kontra Németország*, 53495/09. sz. ügy, 2015

EU	Tárgyalt kérdések	Európa Tanács
EUB, *Európai Bizottság kontra The Bavarian Lager Co. Ltd.* [nagytanács], C-28/08. P. sz. ügy, 2010 EUB, *ClientEarth, Pesticide Action Network Europe (PAN Europe) kontra Európai Élelmiszerbiztonsági Hatóság (EFSA), Európai Bizottság*, C-615/13. P. sz. ügy, 2015	A dokumentumokhoz való hozzáférés	EJEB, *Magyar Helsinki Bizottság kontra Magyarország* [Nagykamara], 18030/11. sz. ügy, 2016
Általános adatvédelmi rendelet, 90. cikk	Szakmai titoktartás	EJEB, *Pruteanu kontra Románia*, 30181/05. sz. ügy, 2015
Általános adatvédelmi rendelet, 91. cikk	A vallás, illetve a meggyőződés szabadsága	
	A művészet és a tudomány szabadsága	EJEB, *Vereinigung bildender Künstler kontra Ausztria*, 68354/01. sz. ügy, 2007
EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008	A tulajdon védelme	
EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017	Gazdasági jogok	

1.1 Az adatvédelemhez való jog

Főbb pontok

- Az EJEE 8. cikke értelmében a személyes adatok kezelésével szembeni védelemhez való jog a magán- és családi élet, a lakás és a kapcsolattartás tiszteletben tartásához való jog részét képezi.
- Az Európa Tanács 108. Egyezménye az első, és jelenleg az egyetlen nemzetközi, jogilag kötelező erejű eszköz, amely kifejezetten az adatvédelemmel foglalkozik. Az egyezmény egy korszerűsítési folyamaton esett át, amely a CETS 223. sz. módosító jegyzőkönyv elfogadásával ért véget.

- Az uniós jog különálló alapjognak ismeri el az adatvédelmet. Az EU működéséről szóló szerződés 16. cikke, valamint az EU Alapjogi Chartájának 8. cikke megerősíti ezt.
- Az uniós jogban az adatvédelmet elsőként az adatvédelmi irányelv szabályozta 1995-ben.
- Figyelemmel a gyors technológiai fejlődésre, az EU 2016-ban új jogszabályt fogadott el az adatvédelmi szabályok digitális korhoz igazítása érdekében. Az általános adatvédelmi rendelet 2018 májusától hatályos, és hatályon kívül helyezi az adatvédelmi irányelvet.
- Az általános adatvédelmi rendelettel együtt az EU elfogadott egy jogszabályt a személyes adatok állami hatóságok által bűnüldözési célokra történő kezeléséről. Az (EU) 2016/680 irányelv létrehozza azokat az adatvédelmi szabályokat és elveket, amelyek szabályozzák a személyes adatoknak a bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelését.

1.1.1 A magánélet tiszteletben tartásához való jog és a személyes adatok védelméhez való jog: rövid összefoglaló

Bár szorosan kapcsolódik egymáshoz a magánélet tiszteletben tartásához való jog és a személyes adatok védelméhez való jog, ezek különálló jogok. A magánélethez való jog – amelyre az európai jog a magánélet tiszteletben tartásához való jogként hivatkozik – a nemzetközi emberi jogban az 1948-ban elfogadott Emberi Jogok Egyetemes Nyilatkozatában jelent meg, mint az alapvető védett emberi jogok egyike. Az Emberi Jogok Egyetemes Nyilatkozatának elfogadását követően Európa szintén hamar elismerte ezt a jogot az emberi jogok európai egyezményében (EJEE), amely jogilag kötelező érvényű a részes felekre nézve, és amelyet 1950-ben fogalmaztak meg. Az EJEE úgy rendelkezik, hogy mindenkinek joga van arra, hogy tiszteletben tartsák magán- és családi életét, lakását és kapcsolattartását. E jog gyakorlásába hatóságnak beavatkoznia tilos, kivéve, ha a beavatkozás törvényben meghatározott, fontos és jogos közérdekből történik, továbbá az egy demokratikus társadalomban szükséges.

Az Emberi Jogok Egyetemes Nyilatkozata és az EJEE elfogadására jóval a számítógépek és az internet fejlődése, valamint az információs társadalom kialakulása előtt került sor. Ezek a fejlemények jelentős előnyöket hoztak az egyének és a társadalom számára, javították az életminőséget, a hatékonyságot és a termelékenységet. Ugyanakkor új kockázatot is jelentenek a magánélet tiszteletben tartását illetően.

Eleget téve a személyes adatok gyűjtését és felhasználását szabályozó egyedi szabályok iránti igénynek, kialakult a magánélet újfajta fogalma, amely néhány jogrendszerben adatvédelemként, másokban pedig információs önrendelkezési jogként ismert.[1] Ez a fogalom vezetett el azon külön törvények és rendeletek kidolgozásához, amelyek biztosítják a személyes adatok védelmét.

Az adatvédelem Európában az 1970-es években kezdődött a személyes adatok közjogi hatóságok és nagyvállalatok általi feldolgozásának ellenőrzésére irányuló jogszabályok – egyes államok általi – elfogadásával.[2] Az adatvédelmi szabályozó eszközöket akkoriban európai szinten[3] hozták létre, és az évek során az adatvédelem külön értékké nőtte ki magát, amely immár nem a magánélet tiszteletben tartásához való jog részét képezte. Az uniós jogrend az adatvédelmet alapjogként ismeri el, amely a magánélet tiszteletben tartásához fűződő alapjogtól elkülönülő jog. Ez az elkülönülés felveti a kérdést e két jog közötti kapcsolatot és különbségeket illetően.

A magánélet tiszteletben tartásához való jog és a személyes adatok védelméhez való jog szorosan kapcsolódnak egymáshoz. Mindkettő hasonló értékek, vagyis az egyének önállóságának és emberi méltóságának megvédésére törekszik azáltal, hogy olyan személyes szférát biztosít számukra, amelyben szabadon fejleszthetik személyiségüket, szabadon gondolkodhatnak és formálhatnak véleményt. Ilyenformán ezek a többi alapvető szabadság, mint a véleménynyilvánítás és a békés gyülekezés szabadsága, valamint a vallásszabadság elengedhetetlen előfeltételét képezik.

A két jog egymástól megfogalmazásában és terjedelmében is különbözik. A magánélet tiszteletben tartásához való jog tartalmazza a beavatkozás általános tilalmát,

1 A német Szövetségi Alkotmánybíróság egy 1983-as ítéletében megerősítette az információs önrendelkezési jogot (*Volkszählungsurteil*, BVerfGE Bd. 65, S. 1skk.). A bíróság úgy ítélte meg, hogy az információs önrendelkezési jog a német alkotmányban védett, személyiség tiszteletben tartásához fűződő alapvető jogból ered. Az EJEB egy 2017-es ítéletében elismerte, hogy az EJEE 8. cikke „rendelkezik az inormációs önrendelkezési jog egy formájáról". Lásd: EJEB, *Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország* [Nagykamara], 931/13. sz. ügy, 2017. június 27., 137. pont.

2 A német Hessen tartomány fogadta el az első adatvédelmi törvényt 1970-ben, amely csak abban a tartományban volt érvényes. 1973-ban Svédország fogadta el az első nemzeti adatvédelmi törvényt. A 1980-as évek végére több európai állam (az Egyesült Királyság, Franciaország, Hollandia és Németország) szintén elfogadott az adatvédelemre vonatkozó jogszabályt.

3 Az Európa Tanácsnak a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményét (108. Egyezmény) 1981-ben fogadták el. Az EU 1995-ben fogadta el az első átfogó adatvédelmi eszközt: 95/46/EK irányelv a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról.

amely néhány olyan közérdekű szempont függvénye, amelyek egyes esetekben indokolhatják a beavatkozást. A személyes adatok védelmét modern és aktív jognak tekintik,[4] amely a fékek és ellensúlyok rendszerét vezette be annak érdekében, hogy védelmet biztosítson az egyének számára személyes adataik kezelése esetén. A személyes adatok kezelését a személyes adatok védelmének alapvető komponenseivel összhangban, nevezetesen független felügyelet biztosítása és az érintettek jogainak tiszteletben tartása mellett kell végezni.[5]

Az EU Alapjogi Chartájának (a Charta) 8. cikke nemcsak megerősíti a személyes adatok védelméhez való jogot, hanem pontosan meghatározza az e joghoz kapcsolódó alapvető értékeket is. Előírja, hogy személyes adatokat tisztességesen, meghatározott célokra, az érintett személy hozzájárulása alapján vagy valamilyen más, a törvényben rögzített jogalapon lehet kezelni. Az egyének számára biztosítani kell a jogot, hogy a róla gyűjtött személyes adatokat megismerje, és azokat kijavíttassa, és e jog tiszteletben tartását független hatóságnak kell ellenőriznie.

A személyes adatok védelméhez való jog minden olyan esetben jelentőséget kap, amikor személyes adatokat kezelnek, így ennek köre tágabb, mint a magánélet tiszteletben tartásához való jogé. A személyes adatok minden kezelése megfelelő védelem alá tartozik. Az adatvédelem a személyes adatok minden fajtájára és az adatkezelés minden módjára kiterjed, függetlenül a magánélettel való kapcsolattól, illetve a magánéletre gyakorolt hatástól. A személyes adatok kezelése, az alább bemutatott példák szerint, sértheti a magánélethez való jogot is. Nem szükséges azonban igazolni a magánélet tiszteletben tartásához való jog megsértését az adatvédelmi szabályok alkalmazásának kiváltásához.

A magánélethez való jog olyan helyzeteket érint, ahol a magánérdek, vagy az egyén „magánélete" került veszélybe. Az e kézikönyvben bemutatottak szerint a „magánélet" fogalmát az ítélkezési gyakorlatban tágan értelmezik. Az értelmezések szerint e fogalomba értendők az intim helyzetek, az érzékeny vagy bizalmas információk, azok az információk, amelyek hátrányosan befolyásolhatják a nyilvánosság észlelését egy egyénnel szemben, sőt, még valamely személy szakmai élete és nyilvános szereplése is ide tartozik. Annak értékelése azonban, hogy

4 Sharpston főtanácsnok az ügyet két külön jogot, a magánélet védelméhez való „klasszikus", és egy „modernebb", az adatvédelemhez való jogot érintő ügyként ismertette. Lásd: EUB, *Volker und Markus Schecke GbR kontra Land Hessen*, Sharpston főtanácsnok indítványa, C-92/09. és C-93/09. sz. egyesített ügyek, 2010. június 17., 71. pont.

5 Hustinx, P., EDPS beszédek és cikkek, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, 2013. július.

megvalósul-e, vagy történt-e beavatkozás a „magánéletbe", az egyes ügyek kontextusától és tényeitől függ.

Ezzel szemben a személyes adatok kezelésével járó minden tevékenység az adatvédelmi szabályok hatálya alá tartozhat, és kiválthatja a személyes adatok védelméhez fűződő jog alkalmazását. Például, ha egy munkáltató a munkavállalók nevéhez és részükre kifizetett javadalmazáshoz kapcsolódó adatokat rögzít, ezen információk puszta rögzítése nem tekinthető a magánéletbe való beavatkozásnak. Ha viszont a munkavállalók adatait a munkáltató harmadik feleknek átadja, akkor már lehet magánéletbe való beavatkozásról beszélni. A munkáltatóknak minden esetben be kell tartaniuk az adatvédelmi szabályokat, mivel a munkavállalók adatainak rögzítésével adatkezelés valósul meg.

Példa: A *Digital Rights Ireland* ügyben[6] az EUB-t arra kérték, hogy döntsön a 2006/24/EK irányelv érvényességével kapcsolatban, figyelemmel a személyes adatok védelméhez és a magánélet tiszteletben tartásához való, és EU Alapjogi Chartájában megerősített alapvető jogokra. Az irányelv előírta a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtói, illetve a nyilvános hírközlő hálózatok szolgáltatói számára, hogy a polgárok távközlési adatait legfeljebb két évig őrizzék meg annak biztosítására, hogy az adatok hozzáférhetők legyenek súlyos bűncselekmények megelőzése, nyomozása és üldözése céljából. Az intézkedés csak a metaadatokra, a hellyel kapcsolatos adatokra és az előfizető vagy a felhasználó azonosításához szükséges adatokra vonatkozott. Nem vonatkozott az elektronikus kommunikáció tartalmára.

Az EUB az irányelvet a személyes adatok védelméhez való alapvető jogba való beavatkozásnak tekintette, mivel az „személyes adatok kezeléséről rendelkezik".[7] Ráadásul megállapította, hogy az irányelv beavatkozott a magánélet tiszteletben tartásához való jogba.[8] Együttesen véve, az irányelv értelmében megőrzött személyes adatok, amelyekhez a hozzáférést az illetékes hatóságok számára lehetővé tették: „igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete

6 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

7 *Uo.*, 36. pont.

8 *Uo.*, 32–35. pont.

vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében".[9] A két jogba való beavatkozás széles körben megvalósult, és különösen súlyos volt.

Az EUB a 2006/24/EK irányelvet érvénytelennek nyilvánította. Megállapította, hogy annak ellenére, hogy az jogszerű célt szolgált, súlyosan megsértette a személyes adatok védelméhez és a magánélethez való jogot, és nem korlátozódott a feltétlenül szükséges mértékre.

1.1.2 Nemzetközi jogi keretek: Egyesült Nemzetek Szervezete

Az Egyesült Nemzetek Szervezete nem ismeri el alapvető jogként a személyes adatok védelméhez való jogot, annak ellenére, hogy a magánélethez való jog a nemzetközi jogrendben régóta fennálló alapvető jog. Az egyén magánéletének mások – különösen az állam – beavatkozása elleni védelméhez való jogát nemzetközi jogi dokumentumban először az Emberi Jogok Egyetemes Nyilatkozatának (UDHR) a magán- és családi élet tiszteletben tartásáról szóló 12. cikkében mondták ki.[10] Annak ellenére, hogy az UDHR jogilag nem kötelező nyilatkozat, szerepe, mint a nemzetközi emberi jogi törvények alapító okirata, nem elhanyagolható, és hatással volt egyéb európai emberi jogi szabályozó eszközök kidolgozására. A Polgári és Politikai Jogok Nemzetközi Egyezségokmánya (ICCPR), amely 1976-ban lépett hatályba, deklarálja, hogy tilos bármely személy magánéletének, otthonának, kapcsolattartásának önkényes vagy jogellenes zavarása, becsületének vagy jó hírének jogellenes megsértése. Az ICCPR egy nemzetközi szerződés, amely 169 részes felét arra kötelezi, hogy tartsák tiszteletben és biztosítsák az egyének polgári jogait, beleértve a magánélethez való jog gyakorlását.

Az új technológiák fejlődésére és a néhány államban folytatott tömeges megfigyelésekről napvilágot látott hírekre (Snowden-szivárogtatás) válaszul az ENSZ 2013 óta két állásfoglalást fogadott el a magánélettel kapcsolatos kérdésekre vonatkozóan

9 *Uo.*, 27. pont.

10 ENSZ, Emberi Jogok Egyetemes Nyilatkozata (UDHR), 1948. december 10.

„Magánélethez való jog a digitális érában”[11] címmel. Ezek szigorúan elítélik a tömeges megfigyelést, és kiemelik, hogy az ilyen megfigyelések milyen hatással lehetnek a magánélethez és a véleménynyilvánítás szabadságához való alapvető jogokra, valamint egy virágzó és demokratikus társadalom működésére. Noha a határozatok jogilag nem kötelezőek, éles nemzetközi, magas szintű politikai vitát váltottak ki a magánélettel, az új technológiákkal és a megfigyeléssel kapcsolatban. Ezenkívül egy a magánélethez való joggal foglalkozó különleges előadó kinevezéséhez is vezettek, akinek feladata, hogy előmozdítsa és védje ezt a jogot. Az előadó konkrét feladatai kiterjednek a magánélettel kapcsolatos nemzeti gyakorlatokra és tapasztalatokra, valamint az új technológiákból eredő kihívásokra vonatkozó információk gyűjtésére, a bevált gyakorlatok cseréjére és megosztására, valamint a lehetséges akadályok azonosítására.

Míg a korábbi állásfoglalások a tömeges megfigyelés negatív hatásaira és az államok hírszerzési hatóságok hatáskörének korlátozására irányuló felelősségére összpontosítottak, a későbbi állásfoglalások a magánéletre vonatkozóan az ENSZ-en belül zajló vita jelentős fejlődését tükrözik.[12] A 2016-ban és 2017-ben elfogadott állásfoglalások megerősítik azt, hogy korlátozni szükséges a titkosszolgálatok hatáskörét és el kell ítélni a tömeges megfigyelést. Ugyanakkor azt is kifejezetten leszögezik, hogy „az üzleti vállalkozások arra irányuló egyre növekvő képessége, hogy személyes adatokat gyűjtsön, kezeljen és használjon fel, kockázatot jelenthet a magánélethez való jog élvezete szempontjából a digitális korban”. Így tehát, az állami hatóságok felelősségén túl az állásfoglalások a magánszektor felelősségére is rámutatnak az emberi jogok tiszteletben tartását illetően, és felhívják a vállalatokat, hogy tájékoztassák a felhasználókat a személyes adatok gyűjtéséről, felhasználásáról, megosztásáról, valamint megőrzéséről, továbbá dolgozzanak ki átlátható adatkezelési szabályzatokat.

1.1.3 Az emberi jogok európai egyezménye

Az Európa Tanács a második világháború utóhatásaként alakult meg, hogy összefogja az európai államokat a jogállamiság, a demokrácia, az emberi jogok és

11 Lásd: ENSZ, Közgyűlés, Resolution on the right to privacy in the digital age (Állásfoglalás a magánélethez való jogról a digitális korban), A/RES/68/167, New York, 2013. december 18.; és ENSZ, Közgyűlés, Revised draft resolution on the right to privacy in the digital age (Átdolgozott állásfoglalás-tervezet a magánélethez való jogról a digitális korban), A/C.3/69/L.26/Rev.1, New York, 2014. november 19.

12 ENSZ, Közgyűlés, Revised draft resolution on the right to privacy in the digital age (Átdolgozott állásfoglalás-tervezet a magánélethez való jogról a digitális korban), A/C.3/71/L.39/Rev.1, New York, 2016. november 16.; ENSZ, Emberi Jogi Tanács, *The right to privacy in the digital age* (A magánélethez való jog a digitális korban), A/C.3/34/L.26/Rev.1, New York, 2017. március 22.

a társadalmi fejlődés előmozdítása érdekében. E célból 1950-ben elfogadta az EJEE-t, amely 1953-ban lépett hatályba.

A részes feleket nemzetközi kötelezettség terheli az EJEE betartása tekintetében. Mára már az Európa Tanács minden tagállama beépítette nemzeti jogába vagy hatályba léptette az EJEE-t, így köteles az egyezmény rendelkezéseinek megfelelően eljárni. A részes felek kötelesek intézkedéseik vagy hatáskörük gyakorlása során tiszteletben tartani az egyezményben meghatározott jogokat. Ebbe beletartoznak a nemzetbiztonság érdekében tett intézkedések. Az Emberi Jogok Európai Bírósága (EJEB) alapvető jelentőségű ítéletei a nemzetbiztonsági jog és gyakorlat érzékeny területein tett állami intézkedéseket is érintenek.[13] A Bíróság habozás nélkül megerősítette, hogy a megfigyelési tevékenységek a magánélet tiszteletben tartásához való jogba való beavatkozást testesítenek meg.[14]

Annak biztosítása céljából, hogy a részes felek eleget tegyenek az EJEE értelmében fennálló kötelezettségeiknek, 1959-ben Strasbourgban létrehozták az EJEB-et. Az EJEB azzal biztosítja, hogy az államok betartsák az egyezmény alapján fennálló kötelezettségeiket, hogy foglalkozik az egyezmény állítólagos megsértésére vonatkozó, magánszemélyektől, személyek csoportjaitól, civil szervezetektől vagy jogi személyektől érkező panaszokkal. Az EJEB az Európa Tanács egy vagy több tagállama által egy másik tagállam ellen indított államközi ügyeket is vizsgálhatja.

2018-ban az Európa Tanács 47 részes állammal rendelkezett, amelyek közül 28 egyben az Európai Uniónak is tagja. Az EJEB-hez keresettel forduló személynek nem kell valamely részes állam állampolgárának lennie, jóllehet, az állítólagos jogsértés vizsgálatának feltétele, hogy az valamely részes állam jogrendszerében valósuljon meg.

A személyes adatok védelméhez való jog az EJEE 8. cikke alapján védelemben részesülő jogok közé tartozik, amely cikk garantálja a magán- és családi élet, a lakás és a kapcsolattartás tiszteletben tartását, és meghatározza azokat a feltételeket, amelyekkel e jog korlátozható.[15]

13 Lásd például: EJEB, *Klass és társai kontra Németország*, 5029/71. sz. ügy, 1978. szeptember 6.; EJEB, *Rotaru kontra Románia* [Nagykamara], 28341/95. sz. ügy, 2000. május 4., és EJEB, *Szabó és Vissy kontra Magyarország*, 37138/14. sz. ügy, 2016. január 12.

14 *Uo.*

15 Európa Tanács, Emberi jogok európai egyezménye, CETS 005, 1950.

Az EJEB több adatvédelmi kérdést érintő esetet vizsgált. Többek között olyanokat, amelyek a kommunikáció lehallgatását,[16] az állami és magánszektor általi megfigyelés különféle formáit,[17] illetve a személyes adatok állami hatóságok általi tárolását érintették.[18] A magánélet tiszteletben tartásához való jog nem abszolút jog, ennek a jognak a gyakorlása más jogokat érinthet – például a véleménynyilvánítás szabadságát és az információszabadságot, és fordítva. Ezért a Bíróság törekszik egyensúlyt teremteni a szóban forgó különböző jogok között. A testület megállapította, hogy az EJEE 8. cikke nemcsak arra kötelezte az államokat, hogy tartózkodjanak az olyan fellépéstől, amely sértheti ezt az egyezményben foglalt jogot, hanem azt is rögzítette, hogy az államokat bizonyos körülmények fennállása esetén pozitív kötelezettség is terheli abban a vonatkozásban, hogy valóban biztosítsák a magán- és családi élet tényleges tiszteletben tartását.[19] A megfelelő fejezetek részletesen ismertetnek számos ügyet.

1.1.4 Az Európa Tanács 108. Egyezménye

Az információs technológia 1960-as évekbeli fejlődésével egyre szükségesebbé vált az egyének (személyes) adatainak védelmére vonatkozó részletes szabályok megállapítása. Az 1970-es évek közepéig az Európa Tanács Miniszteri Bizottsága az EJEE 8. cikkére való hivatkozással számos határozatot fogadott el a személyes adatok védelmével kapcsolatban.[20] 1981-ben az Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során (108. Egyezmény)[21] nyílt meg aláírásra. A mai napig a 108. Egyezmény az egyetlen jogilag kötelező erejű nemzetközi eszköz az adatvédelem területén.

16 Lásd például: EJEB, *Malone kontra Egyesült Királyság*, 8691/79. sz. ügy, 1984. augusztus 2.; EJEB, *Copland kontra Egyesült Királyság*, 62617/00. sz. ügy, 2007. április 3., vagy EJEB, *Mustafa Sezgin Tanrıkulu kontra Törökország*, 27473/06. sz. ügy, 2017. július 18.

17 Lásd például: EJEB, *Klass és társai kontra Németország*, 5029/71. sz. ügy, 1978. szeptember 6.; EJEB, *Uzun kontra Németország*, 35623/05. sz. ügy, 2010. szeptember 2.

18 Lásd például: EJEB, *Roman Zakharov kontra Oroszország*, 47143/06. sz. ügy, 2015. december 4.; EJEB, *Szabó és Vissy kontra Magyarország*, 37138/14. sz. ügy, 2016. január 12.

19 Lásd például: EJEB, *I. kontra Finnország*, 20511/03. sz. ügy, 2008. július 17.; EJEB, *K.U. kontra Finnország*, 2872/02. sz. ügy, 2008. december 2.

20 Európa Tanács, Miniszteri Bizottság (1973), (73)22. sz. határozat az egyének magánéletének az elektronikus adatbankokkal szembeni védelméről a magánszektorban, 1973 .szeptember 26.; Európa Tanács, Miniszteri Bizottság (1974), (74)29. sz. határozat az egyének magánéletének az elektronikus adatbankokkal szembeni védelméről az állami szektorban, 1974 .szeptember 20 .

21 Európa Tanács, Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során, CETS 108, 1981.

A 108. Egyezmény vonatkozik mind a magánszektor, mind az állami szektor által végzett valamennyi adatkezelésre, ideértve a bírósági és bűnüldözési hatóságok adatkezelését is. Megvédi az egyént a személyes adatok gyűjtésével és kezelésével összefüggő visszaélésektől, ugyanakkor törekszik a határokon átnyúló személyesadat-áramlás szabályozására. A személyes adatok gyűjtésére és kezelésére vonatkozóan az egyezményben meghatározott elvek előírják az adatok tisztességes és törvényes gyűjtését, valamint az automatizált és meghatározott célból történő adatkezelést. Ez azt jelenti, hogy az adatokat nem szabad ezekkel összeegyeztethetetlen célokra felhasználni, és nem szabad a szükségesnél hosszabb ideig tárolni. Az elvek érintik ezenkívül az adatok minőségét, főleg azt, hogy az adatoknak megfelelőnek, relevánsnak kell lenniük, és nem haladhatják meg a kezelés célját (arányosság), továbbá pontosaknak is kell lenniük.

Azonkívül, hogy az egyezmény garanciákat nyújt a személyes adatok kezelésével és az adatbiztonságra vonatkozó kötelezettséggel kapcsolatban, megfelelő jogi biztosítékok hiányában tiltja a „különleges" adatok feldolgozását, azaz a faji eredetre, politikai véleményre, vallásos vagy más meggyőződésre és az egészségre, a szexuális életre vonatkozó, valamint a büntető ítéletekkel kapcsolatos személyes adatok feldolgozását.

Az egyezmény az egyén azon jogáról is rendelkezik, hogy tudomást szerezhessen a róla tárolt adatokról, továbbá szükség esetén helyesbíttethesse azokat. Az egyezményben megállapított jogok korlátozása csak magasabb rendű érdekek, például az állambiztonság vagy -védelem érintettsége esetén lehetséges. Ezenkívül az egyezmény a személyes adatoknak az egyezmény részes államai közötti szabad áramlásáról rendelkezik, és bizonyos korlátozásokat is előír az olyan államokba történő adatáramlás tekintetében, ahol a jogi szabályozás nem nyújt azonos szintű védelmet.

Fontos kiemelni, hogy a 108. Egyezmény kötelező az egyezményt megerősítő államok számára. Nem tartozik az EJEB bírói felügyelete alá, azonban az EJEB ítélkezési gyakorlatában figyelembe veszi az EJEE 8. cikkének összefüggésében. Az évek során a Bíróság akként határozott, hogy a személyes adatok védelme a magánélet tiszteletben tartásához való jog (8. cikk) fontos részét képezi, és a 108. Egyezmény elvei szolgáltak iránymutatásul annak meghatározásában, hogy megvalósult-e a beavatkozás ebbe az alapvető jogba.[22]

22 Lásd például: EJEB, *Z kontra Finnország*, 22009/93. sz. ügy, 1997. február 25.

A 108. Egyezményben meghatározott általános elvek és szabályok továbbfejlesztése érdekében az Európa Tanács Miniszteri Bizottsága számos ajánlást elfogadott, amelyek jogilag nem kötelező erejű dokumentumok. Ezek az ajánlások hatással voltak az európai adatvédelmi jog kialakulására. Éveken keresztül például az egyetlen eszköz, amely Európában a rendőrségi ágazatban iránymutatást nyújtott a személyes adatok felhasználására vonatkozóan, a rendőrségi ajánlás volt.[23] Az ajánlásban foglalt elveket, például az adatállományok megőrzésének módjait, és az ezen állományokhoz hozzáféréssel rendelkező személyekre vonatkozó világos szabályok végrehajtásának szükségességét részletesebben kidolgozták, és azok megjelentek a későbbi uniós jogszabályokban.[24] Az újabb ajánlások igyekeznek megoldást nyújtani a digitális kor kihívásaira, például a személyes adatok kezelésével kapcsolatban a munkaügy területén (lásd a 9. fejezetet).

Valamennyi európai uniós tagállam ratifikálta a 108. Egyezményt. 1999-ben javaslat született a 108. Egyezmény olyan módosítására, amelynek értelmében, lehetővé vált volna az EU számára a csatlakozás, azonban a módosítás azóta se lépett hatályba.[25] 2001-ben elfogadtak egy kiegészítő jegyzőkönyvet a 108. Egyezményhez. A dokumentum az egyezményben nem részes, úgynevezett harmadik országokba történő, országhatárokat átlépő adatáramlásra és a nemzeti adatvédelmi hatóságok kötelező létrehozására vonatkozóan vezetett be rendelkezéseket.[26]

A 108. Egyezmény azon országok számára is nyitva áll a csatlakozásra, amelyek nem tagjai az Európa Tanácsnak. Az, hogy az egyezmény az egész világon érvényes normává válhat, annak nyílt jellegével együtt, alapul szolgálhat az adatvédelem globális előmozdításához. Eddig 51 ország részese a 108. Egyezménynek. Ezek között van az Európa Tanács összes tagállama (47 ország); Uruguay az első Európán kívüli ország, amely 2013 augusztusában csatlakozott az egyezményhez, Mauritius, Szenegál és Tunézia pedig 2016-ban és 2017-ben csatlakozott.

23 Európa Tanács, Miniszteri Bizottság (1987), R(87)15. sz. ajánlás a tagállamoknak a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, Strasbourg, 1987. szeptember 17.

24 Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL L 281., 1995.11.23.

25 Európa Tanács, A személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezmény (ETS 108.) módosítása, amely lehetővé teszi az Európai Közösségek csatlakozását – elfogadta a Miniszteri Bizottság Strasbourgban, 1999. június 15-én.

26 Európa Tanács, Kiegészítő jegyzőkönyv a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményhez, az adatvédelmi hatóságokra és az országhatárokat átlépő adatáramlásra vonatkozóan, CETS 181, 2001. A Korszerűsített 108. Egyezmény hatályba lépését követően ez a jegyzőkönyv többé nem lesz alkalmazandó, mivel a benne foglalt rendelkezéseket a Korszerűsített 108. Egyezmény tartalmazza.

Az egyezmény a közelmúltban korszerűsítésen ment keresztül. Egy 2011-ben folytatott nyilvános konzultáció folyományaként megerősítést nyert a munka két fő célkitűzése: a magánélet védelmének erősítése a digitális korszakban, valamint az egyezmény nyomonkövetési mechanizmusának megerősítése. A korszerűsítési folyamat ezekre a célkitűzésekre összpontosított, és a 108. Egyezményt módosító jegyzőkönyv (CETS 223. sz. jegyzőkönyv) elfogadásával fejeződött be. A munka a nemzetközi adatvédelmi eszközök egyéb reformjaival párhuzamosan, valamint az uniós adatvédelmi szabályok 2012-ben indított reformjával egyidejűleg zajlott. Az Európa Tanács és az uniós szintű szabályozók kiemelt gondosságot fordítottak annak biztosítására, hogy a két jogi keret következetes és összeegyeztethető legyen. A korszerűsítés megőrzi az egyezmény általános és rugalmas jellegét, továbbá erősíti a benne rejlő lehetőséget, hogy általános adatvédelmi jogszabállyá váljon. Ismételten megerősít és stabilizál fontos elveket, és új jogokkal ruházza fel az egyéneket, miközben ezzel egyidejűleg fokozza a személyes adatokat kezelő szervezetek felelősségét, és nagyobb fokú elszámoltathatóságot biztosít. Azon egyéneknek, például, akiknek a személyes adatait kezelik, jogukban áll megismerni az adatkezelés okát, és jogukban áll tiltakozni az adatkezelés ellen. Az online világban egyre gyakrabban használt profilalkotás ellensúlyozása érdekében az egyezmény továbbá létrehozza az egyén arra vonatkozó jogát, hogy véleménye figyelembevételével mentesülhessen a kizárólag automatizált adatkezelésen alapuló döntések hatálya alól. Az egyezmény gyakorlati végrehajtásának alapvető feltétele az adatvédelmi szabályok hatékony érvényesítése független felügyeleti hatóságok közreműködésével a részes országokban. Ennek érdekében a Korszerűsített 108. Egyezmény hangsúlyozza, hogy a felügyeleti hatóságokat hatékony hatáskörrel és funkciókkal kell felruházni, és azoknak valódi függetlenséget kell élvezniük küldetésük teljesítése során.

1.1.5 Az Európai Unió adatvédelmi joga

Az uniós jog az elsődleges és a másodlagos uniós joganyagból áll. A Szerződéseket, azaz az Európai Unióról szóló szerződést (EUSZ) és az Európai Unió működéséről szóló szerződést (EUMSZ) az EU valamennyi tagállama megerősítette. Ezeket nevezzük az „elsődleges uniós joganyagnak". Az EU rendeleteit, irányelveit és határozatait a Szerződések szerint erre felhatalmazott uniós intézmények fogadják el; ezek gyakori megnevezése a „másodlagos uniós joganyag".

Adatvédelem az elsődleges uniós joganyagban

Az Európai Közösségek eredeti szerződései nem tartalmaztak hivatkozást az emberi jogokra vagy azok védelmére, tekintettel arra, hogy az Európai Gazdasági Közösség az eredeti tervek szerint a gazdasági integrációra és egy közös piac létrehozására összpontosító regionális szervezet lett volna. Az Európai Közösségek létrehozását és fejlődését alátámasztó egyik alapelv – amely még ma is érvényes – a hatáskörmegosztás elve. Ezen elv szerint az EU kizárólag a tagállamok által, a Szerződésekben foglaltak szerint ráruházott hatáskörök határain belül jár el. Az Európa Tanáccsal ellentétben az uniós Szerződések nem tartalmaznak kifejezett hatáskört alapjogi kérdésekben.

Ahogy azonban olyan ügyek kerültek az EUB elé, amelyekben feltételezték az emberi jogok megsértését az uniós jog hatálya alá tartozó területeken, az EUB fontos értelmezést szolgáltatott a Szerződések tekintetében. Ahhoz, hogy az egyénnek részére védelmet biztosítson, az EUB az alapvető jogokat az európai jog úgynevezett általános elvei közé sorolta. Az EUB szerint ezek az általános elvek tükrözik a nemzeti alkotmányokban és az emberi jogi szerződésekben, különösen az EJEE-ben foglalt emberi jogvédelmi szabályokat. Az EUB kijelentette, hogy gondoskodik arról, hogy az uniós jog megfeleljen ezeknek az elveknek.

Az EU 2000-ben kihirdette az Európai Unió Alapjogi Chartáját („Charta"), miután felismerte, hogy szakpolitikái hatással lehetnek az emberi jogokra, és törekedett arra, hogy a polgárok „közelebb" kerüljenek az EU-hoz. A Charta azzal, hogy szintetizálja a közös tagállami alkotmányos hagyományokat és nemzetközi kötelezettségeket, az európai polgárok polgári, politikai, gazdasági és szociális jogainak teljes skáláját felöleli. A Chartában leírt jogok hat fejezetre oszlanak: méltóság, szabadságok, egyenlőség, szolidaritás, polgárok jogai és igazságszolgáltatás.

Eredetileg a Charta csupán politikai dokumentum volt, a Lisszaboni Szerződés 2009. december 1-jei hatálybalépésével elsődleges uniós joganyagként (lásd az EUSZ 6. cikk (1) bekezdését) jogilag kötelező[27] erejűvé vált.[28] A Charta rendelkezéseinek címzettjei az uniós intézmények és szervek, és kötelezik ezeket az ott felsorolt jogok tiszteletben tartására feladataik ellátása során. A Charta rendelkezései a tagállamokra nézve is kötelezők az uniós jog végrehajtása során.

27 EU (2012), Az Európai Unió Alapjogi Chartája, HL C 326., 2012.10.26.

28 Lásd az Európai Közösségeknek (2012) az Európai Unióról szóló szerződése (HL C 326., 2012.10.26.) és az Európai Unió Működéséről szóló szerződése (HL C 326., 2012.10.26.) egységes szerkezetbe foglalt változatát.

A Charta nemcsak garantálja a magán- és családi élet tiszteletben tartását (7. cikk), hanem megállapítja az adatvédelemhez való jogot (8. cikk), kifejezetten alapjogi szintre emelve e védelem szintjét az uniós jogban. Az uniós intézmények és szervek – valamint a tagállamok annyiban, amennyiben az Unió jogát hajtják végre – kötelesek garantálni és tiszteletben tartani ezt a jogot. A Charta 8. cikkét, amely sok évvel az adatvédelmi irányelv után keletkezett, úgy kell értelmezni, hogy az a korábban már létezett uniós adatvédelmi jogot is magában foglalja. A Charta ezért a 8. cikk (1) bekezdésében nemcsak kifejezetten megemlíti az adatvédelemhez való jogot, hanem a 8. cikk (2) bekezdésében a legfontosabb adatvédelmi elvekre is kitér. Végül a Charta 8. cikkének (3) bekezdése előírja, hogy a szóban forgó elvek végrehajtását független hatóság ellenőrizze.

A Lisszaboni Szerződés elfogadása mérföldkő az adatvédelmi szabályozás fejlődésében, nemcsak azért, mert a Chartát az elsődleges joganyag szintjén kötelező erejű jogi dokumentum szintjére emelte, hanem azért is, mert rendelkezik a személyes adatok védelméről. Erről a jogról kifejezetten az EUMSZ 16. cikk rendelkezik a szerződésnek az EU általános elveinek szentelt részében. A 16. cikk továbbá egy új jogalapot is létrehoz, amely biztosítja az EU számára az arra vonatkozó hatáskört, hogy adatvédelmi kérdésekben jogszabályokat alkosson. Ez egy fontos fejlemény, mert az uniós adatvédelmi szabályok – nevezetesen az adatvédelmi irányelv – eredetileg a belső piacra vonatkozó jogalapon, valamint a nemzeti jogok közelítésének szükségességén alapult, hogy ne legyen akadálya az adatok szabad áramlásának az Unión belül. Az EUMSZ 16. cikk viszont egy független jogalapot biztosít egy korszerű, átfogó adatvédelmi megközelítéshez, amely kiterjed az uniós hatáskörbe tartozó valamennyi területre, beleértve a rendőrségi és igazságügyi együttműködést a büntetőügyekben. Az EUMSZ megerősíti továbbá, hogy az adatvédelmi szabályok betartását független felügyeleti hatóságoknak kell ellenőrizniük. A 16. cikk jogalapként szolgált az adatvédelmi szabályok 2016-os átfogó reformjához, vagyis az általános adatvédelmi rendelet és a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv elfogadásához (lásd alább).

Az általános adatvédelmi rendelet

1995-től 2018 májusáig az adatvédelemmel kapcsolatos legfőbb uniós jogi aktus a személyes adatok kezelése vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról szóló, 1995. október 24-i 95/46/EK európai parlamenti

és tanácsi irányelv (adatvédelmi irányelv) volt.[29] Az adatvédelmi irányelvet 1995-ben fogadták el – akkor, amikor már számos tagállam rendelkezett nemzeti adatvédelmi törvénnyel,[30] – és az indokolta, hogy harmonizálni kellett ezeket a jogszabályokat a magas szintű védelem, valamint a személyes adatok különböző tagállamok közötti szabad áramlásának biztosítása érdekében. A belső piacon az áruk, a tőke, a szolgáltatások és a személyek szabad mozgásához szabad adatáramlás szükséges, ami csak akkor valósítható meg, ha a tagállamok egységes, magas szintű adatvédelemre hagyatkozhatnak.

Az adatvédelmi irányelv tükrözte a nemzeti jogokban és a 108. Egyezményben már szereplő adatvédelmi elveket, miközben számos esetben kiterjesztette azokat. Azzal a 108. Egyezmény 11. cikkében foglalt lehetőséggel is számolt, hogy a védelmet biztosító további jogi aktusokkal is kiegészülhet. Különösen a független felügyelet mint az adatvédelmi szabályok jobb betartatását szolgáló eszköz bevezetése az irányelvben fontosnak bizonyult az európai adatvédelmi jog tényleges érvényesüléséhez. Ezért ez 2001-ben a 108. Egyezményhez fűzött kiegészítő jegyzőkönyvvel bekerült az Európa Tanács jogába. Ez tükrözi a két eszköz közötti szoros kapcsolatot, és az évek során egymásra gyakorolt kedvező hatást.

Az adatvédelmi irányelv egy részletes és átfogó adatvédelmi rendszert dolgozott ki az EU-ban. Az Unió jogrendszerével összhangban azonban az irányelvek nem érvényesek közvetlenül, és azokat át kell ültetni a tagállamok nemzeti jogába. A tagállamoknak szükségszerűen van mérlegelési mozgásterük az irányelv rendelkezéseinek átültetésében. Bár az irányelv célja az volt, hogy teljes harmonizációt[31] (és teljes körű védelmet) biztosítson, a gyakorlatban a tagállamok eltérően ültették azt át. Ez Unió-szerte különféle adatvédelmi szabályokat eredményezett, és a fogalommeghatározásokat, valamint a szabályokat a nemzeti jogokban eltérően értelmezték. A jogérvényesítés szintjei és a szankciók súlyossága is eltérő volt az egyes tagállamokban. Végezetül, az irányelv 1990-es évek közepén történt kidolgozása óta

29 Az Európai Parlament és a Tanács 1995. október 24-i 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, HL L 281., 1995.11.23.

30 A német Hessen tartomány fogadta el az első adatvédelmi törvényt 1970-ben, amely csak abban a tartományban volt érvényes. Svédország 1973-ban elfogadta a *Datalagent,* Németország 1976-ban a *Bundesdatenschutzgestezt,* Franciaország pedig 1977-ben a *Loi relatif à l'informatique, aux fichiers et aux libertés-t*. Az Egyesült Királyságban az adatvédelmi törvényt 1984-ben fogadták el. Végezetül pedig Hollandia 1989-ben elfogadta a *Wet Persoonregistratiest*.

31 EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24., 29. pont.

komoly változások következtek be az információs technológiában. Mindezen okok együttesen szükségessé tették az EU adatvédelmi jogszabályainak reformját.

A reform eredményeképp, több évig tartó élénk vitát követően, 2016 áprilisában elfogadták az általános adatvédelmi rendeletet. Az uniós adatvédelmi szabályok korszerűsítésének szükségességéről szóló viták 2009-ben kezdődtek, amikor a Bizottság nyilvános konzultációt kezdeményezett a személyes adatok védelméhez fűződő alapjog jövőbeli jogi keretéről. A rendeletre irányuló javaslatot a Bizottság 2012 januárjában tette közzé, amellyel kezdetét vette egy hosszadalmas jogalkotási tárgyalás az Európai Parlament és az EU Tanácsa között. Elfogadását követően az általános adatvédelmi rendelet egy kétéves átmeneti időszakról rendelkezik. 2018. május 25-én válik teljeskörűen alkalmazandóvá, amikor az adatvédelmi irányelv hatályát veszti.

Az általános adatvédelmi rendelet 2006-os elfogadása korszerűsítette az EU adatvédelmi jogszabályait, és ezzel alkalmassá tette azokat az alapvető jogok védelmére a digitális korszak gazdasági és társadalmi kihívásaival összefüggésben. Az általános adatvédelmi rendelet megtartja és továbbfejleszti az adatvédelmi irányelvben biztosított alapelveket és az érintettek jogait. Ezenkívül új kötelezettségeket vezetett be, amely előírja a szervezetek számára, hogy az adatvédelmet beépített és alapértelmezett módon hajtsák végre; bizonyos körülmények között nevezzenek ki egy adatvédelmi tisztviselőt; tartsák tiszteletben az adathordozhatósághoz való új jogot; és tartsák tiszteletben az elszámoltathatóság elvét. Az uniós jog értelmében a rendeletek közvetlenül alkalmazandók: nincs szükség nemzeti szintű végrehajtásra. Az általános adatvédelmi rendelet ezért az egész Unióban egységes adatvédelmi szabályrendszert biztosít. Ez az egész EU-ban következetes adatvédelmi szabályozást hoz létre, és egy olyan jogbiztonságot nyújtó környezetet teremt, amely a gazdasági szereplők és magánszemélyek, mint „érintettek" javát szolgálhatja.

Ugyanakkor az általános adatvédelmi rendelet közvetlen alkalmazhatósága ellenére a tagállamok várhatóan aktualizálni fogják meglévő nemzeti adatvédelmi jogszabályaikat annak érdekében, hogy teljes mértékben összehangolják azokat a rendelettel, ugyanakkor tükrözzék a (10) preambulumbekezdésben foglalt konkrét rendelkezések tekintetében a mérlegelési mozgásteret is. A rendeletben létrehozott fő szabályok és elvek, valamint az egyének számára biztosított erős jogok a kézikönyv jelentős részét képezik, és ezeket a következő fejezetekben mutatjuk be. A rendelet átfogó szabályokat tartalmaz a területi hatályra vonatkozóan. Hatálya alá tartoznak az EU-ban székhellyel rendelkező vállalkozások, és azok az EU-ban székhellyel nem rendelkező adatkezelők és adatfeldolgozók, amelyek uniós érintettek számára

kínálnak árukat és szolgáltatásokat, vagy uniós érintettek viselkedését figyelik meg. Mivel számos tengerentúli technológiai vállalkozás meghatározó részesedéssel rendelkezik az európai piacon, és több millió uniós vásárlója van, az egyének védelme, valamint az egyenlő versenyfeltételek biztosítása érdekében fontos, hogy e szervezetek az uniós adatvédelmi szabályok hatálya alá tartozzanak.

Adatvédelem a bűnüldözésben – 2016/680 irányelv

A hatályát vesztő adatvédelmi irányelv egy átfogó adatvédelmi rendszert biztosított. Ezt a rendszert továbbfejlesztették az általános adatvédelmi rendelet elfogadásával. Átfogó jellege ellenére a hatályon kívül helyezett adatvédelmi irányelv hatálya a belső piacon belüli tevékenységekre, valamint a közjogi hatóságok tevékenységére korlátozódott, amelybe a bűnüldözés nem tartozott bele. Ezért a szükséges egyértelműség és az adatvédelem, illetve egyéb jogos érdekek közötti egyensúly megteremtése, továbbá konkrét ágazatokban különösen releváns kihívások kezelése érdekében szükség volt speciális eszközök elfogadására. Erről van szó a személyes adatok bűnüldöző hatóságok általi kezelésére vonatkozó szabályok esetében.

A kérdést szabályozó első uniós jogi eszköz a Tanács 2008/977/IB kerethatározata a büntetőügyekben folytatott rendőrségi és igazságszolgáltatási együttműködés keretében feldolgozott személyes adatok védelméről. Az ebben megfogalmazott szabályok kizárólag a rendőrségi és igazságszolgáltatási adatokra vonatkoztak azok tagállamok közötti cseréje esetében. A személyes adatok bűnüldöző hatóságok általi belföldi kezelése nem tartozott a hatálya alá.

A 2016/680 irányelv a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról[32] (a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv) orvosolta ezt a helyzetet. Az általános adatvédelmi rendelettel párhuzamosan elfogadott irányelv hatályon kívül helyezte a 2008/977/IB tanácsi kerethatározatot, és a bűnüldözéssel összefüggésben létrehozta a személyes adatok védelmének átfogó

32 Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4.

rendszerét, miközben elismeri a közbiztonsággal kapcsolatos adatkezelés sajátosságait. Míg az általános adatvédelmi rendelet a személyes adatok kezelésére vonatkozóan általános szabályokat állapít meg az egyének védelme és az ilyen adatok Unión belüli szabad mozgásának biztosítása érdekében, az irányelv konkrét adatvédelmi szabályokat rögzít a büntetőügyekben folytatott rendőrségi és igazságszolgáltatási együttműködés terén. Azokban az esetekben, amikor egy illetékes hatóság személyes adatokat kezel bűncselekmények megelőzése, nyomozása, felderítése, büntetőeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából, a 2016/680 irányelvet kell alkalmazni. A személyes adatoknak az illetékes hatóságok általi fenti céloktól eltérő kezelése esetén az általános adatvédelmi rendelet szerinti általános rendszert kell alkalmazni. Elődjétől (2008/977/IB tanácsi kerethatározat) eltérően a 2016/680 irányelv hatálya kiterjed a személyes adatok bűnüldöző hatóságok általi belföldi kezelésére, és nem korlátozódik az ilyen adatok tagállamok közötti cseréjére. Ezenkívül az irányelv igyekszik egyensúlyt teremteni az egyének jogai és a biztonsággal kapcsolatos adatkezelés jogos céljai között.

Az irányelv e célból megerősíti a személyes adatok védelméhez való jogot és az adatkezelésre alkalmazandó alapelveket, szorosan követve az általános adatvédelmi rendeletben rögzített szabályokat és elveket. Az egyének jogai és az adatkezelőkre rótt kötelezettségek – például az adatbiztonsággal, a beépített és alapértelmezett adatvédelemmel és az adatvédelmi incidens bejelentésével kapcsolatban – hasonlóak az általános adatvédelmi rendeletben megállapított jogokhoz és kötelezettségekhez. Az irányelv figyelembe veszi, és igyekszik kezelni azon komoly technológiai kihívásokat, amelyek különösen komoly hatást gyakorolhatnak az egyénekre, mint például a bűnüldöző hatóságok általi profilalkotási technikák. Elvben meg kell tiltani a kizárólag automatizált adatkezelésen alapuló döntéseket, ideértve a profilalkotást.[33] Emellett a döntéseket tilos különleges adatokra alapozni. A szóban forgó elvekre az irányelvben biztosított bizonyos kivételek vonatkoznak. Ezenkívül az ilyen adatkezelés nem eredményezhet senkivel szemben sem megkülönböztetést.[34]

Az irányelv tartalmaz továbbá szabályokat az adatkezelők elszámoltathatóságának biztosítására. Az adatkezelőknek ki kell jelölniük egy adatvédelmi tisztviselőt, akinek feladata, hogy ellenőrizze az adatvédelmi szabályok betartását, tájékoztassa a szervezetet és az adatkezelést végző alkalmazottakat kötelezettségeikről,

33 A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv, 11. cikk (1) bekezdés.

34 *Uo.*, 11. cikk (2) és (3) bekezdés.

és hogy együttműködjön a felügyeleti hatósággal. A személyes adatok kezelése a rendőrségi és büntető igazságszolgáltatási ágazatban mára független felügyeleti hatóságok felügyelete alá tartozik. Az általános adatvédelmi rendszernek, valamint a bűnüldözésben és büntetőügyeknél alkalmazott különös adatvédelmi rendszernek egyaránt tiszteletben kell tartania az Európai Unió Alapjogi Chartájának előírásait.

Az adatkezelés – a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv által létrehozott – különös rendszerét a rendőrségi és igazságszolgáltatási együttműködés összefüggésében részletesen a 8. fejezet ismerteti.

Elektronikus hírközlési adatvédelmi irányelv

Az elektronikus kommunikációs ágazatban is szükség volt különös adatvédelmi szabályok megalkotására. Az internet, a vezetékes és mobiltelefonok fejlődésével fontos volt biztosítani, hogy tiszteletben tartsák a felhasználók magánélethez és a bizalmas adatkezeléshez való jogát. Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv[35] (Elektronikus hírközlési adatvédelmi irányelv) megállapítja az adatok biztonságára, a személyes adatok megsértésének bejelentésére és a közlések titkosságára vonatkozó szabályokat.

A biztonságot illetően az elektronikus hírközlési szolgáltatásokat nyújtók kötelesek többek között biztosítani, hogy a személyes adatokhoz való hozzáférés kizárólag arra feljogosított személyekre korlátozódjon, és kötelesek megtenni minden szükséges intézkedést az adatok megsemmisülésének, elvesztésének vagy részleges sérülésének megelőzése érdekében.[36] A hálózati biztonság megsértésének konkrét kockázata esetén a nyilvánosan elérhető elektronikus hírközlési szolgáltatást nyújtó szolgáltatónak tájékoztatnia kell az előfizetőket az ilyen kockázatról.[37] Ha a végrehajtott biztonsági intézkedések ellenére biztonság megsértése következik be, a szolgáltatók kötelesek értesíteni az irányelvben foglaltak végrehajtásával és érvényesítésével megbízott illetékes nemzeti hatóságot a személyes adatok megsértéséről. A szolgáltatóknak néha értesíteniük kell az egyéneket is a személyes adatok megsértéséről, mégpedig azokban az esetekben, amikor a jogsértés valószínűleg

35 Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről, HL L 201., 2002.7.31. („Elektronikus hírközlési adatvédelmi irányelv”).

36 Elektronikus hírközlési adatvédelmi irányelv, 4. cikk (1) bekezdés.

37 *Uo.*, 4. cikk (2) bekezdés.

hátrányosan befolyásolja személyes adataikat vagy magánéletüket.[38] A közlések bizalmassága előírja, hogy elvben tilos a közlések és a metaadatok meghallgatása, lehallgatása, tárolása vagy bármilyen módon történő elfogása vagy megfigyelése. Az irányelv továbbá tiltja a nem kívánt tájékoztatást („spameket" vagy „levélszemetet"), kivéve, ha a felhasználók ehhez hozzájárultak, és szabályokat tartalmaz a számítógépeken és más eszközökön tárolt sütikre vonatkozóan. Ezek az alapvető negatív kötelezettségek egyértelműen jelzik, hogy a közlések titkossága jelentős mértékben kapcsolódik a Charta 7. cikkében biztosított magánélet tiszteletben tartásához való jog és a Charta 8. cikkében biztosított személyes adatok védelméhez való jog védelméhez.

2017 januárjában a Bizottság rendeletre irányuló javaslatot tett közzé a magánélet tiszteletben tartását és a személyes adatok védelmét illetően az elektronikus hírközlésekben, amelynek célja az elektronikus hírközlési adatvédelmi irányelv felváltása. A reform célja, hogy összehangolja az elektronikus közlésekre vonatkozó szabályokat az általános adatvédelmi rendelet értelmében létrehozott új adatvédelmi rendszerrel. Az új szabályozás az egész EU-ban közvetlenül alkalmazandó lesz. Valamennyi egyén azonos szintű védelmet fog élvezni elektronikus közlései tekintetében, miközben a távközlési szolgáltatók és vállalkozások az egyértelműség, a jogbiztonság és az egész Unióban egységes szabályrendszer meglétének haszonélvezői lesznek. Az elektronikus közlések titkosságára vonatkozó javasolt szabályok azokra az elektronikus kommunikációs szolgáltatásokat nyújtó új szereplőkre is kiterjednek, akik nem tartoznak az elektronikus hírközlési adatvédelmi irányelv hatálya alá. Ez utóbbi csak a hagyományos távközlési szolgáltatásokat nyújtókra terjed ki. Az olyan szolgáltatások üzenetküldésre vagy hívásra való használatának erőteljes elterjedésével, mint a Skype, WhatsApp, Facebook Messenger és Viber, ezek az „over the top" szolgáltatások („OTT-szolgáltatások") is a rendelet hatálya alá fognak tartozni, és be kell tartaniuk annak adatvédelemre, titoktartásra és adatbiztonságra vonatkozó előírásait. E kézikönyv közzétételének idején még nem zárult le az elektronikus hírközlési adatvédelem szabályaira vonatkozó jogalkotási folyamat.

45/2001 rendelet

Mivel az adatvédelmi irányelv csak uniós tagállamokra vonatkozhat, további jogi eszközre volt szükség az uniós intézmények és szervek általi személyesadat-kezelésre vonatkozó adatvédelem megteremtéséhez. A személyes adatok közösségi intézmények és szervek által történő kezelése tekintetében az egyének védelméről,

38 *Uo.*, 4. cikk (3) bekezdés.

valamint az ilyen adatok szabad áramlásáról szóló 45/2001/EK rendelet (uniós intézmények adatvédelmi rendelete) tölti be ezt a funkciót.[39]

A 45/2001 rendelet szorosan követi az általános uniós adatvédelmi rendszer elveit, és az érintett elveket az uniós intézmények és szervek által feladataik ellátása során végzett adatkezelésre alkalmazza. Ezenkívül létrehoz egy független felügyeleti hatóságot rendelkezései alkalmazásának ellenőrzésére. Ez a hatóság az európai adatvédelmi biztos (EDPS). Az EDPS felügyeleti hatáskörrel rendelkezik, és feladata ellenőrizni a személyes adatok kezelését az uniós intézményeknél és testületeknél, meghallgatni és kivizsgálni az adatvédelmi szabályok feltételezett megsértését érintő panaszokat. A biztos továbbá tanáccsal látja el az uniós intézményeket és szerveket a személyes adatok védelmét érintő minden kérdésben, az új jogszabályra irányuló javaslatoktól az adatkezelésre vonatkozó belső szabályok kidolgozásáig.

2017 januárjában az Európai Bizottság az uniós intézmények általi adatkezelésre vonatkozó új rendeletre irányuló javaslatot terjesztett elő, amely hatálytalanítja majd a jelenlegi rendeletet. Akárcsak az elektronikus hírközlési adatvédelmi irányelv reformja, a 45/2001 rendelet reformja is korszerűsíti és összehangolja szabályait az általános adatvédelmi rendelet értelmében létrehozott új adatvédelmi rendszerrel.

Az EUB szerepe

Az EUB hatáskörébe tartozik annak megállapítása, hogy egy tagállam teljesítette-e az uniós adatvédelmi törvény értelmében fennálló kötelezettségeit, illetve az uniós jogszabályok értelmezése azok hatékony és egységes alkalmazásának biztosítása érdekében a tagállamokban. Az adatvédelmi irányelv 1995-ös elfogadása óta széles körű ítélkezési gyakorlat halmozódott fel, amely tisztázza az adatvédelmi elvek hatályát és jelentését, valamint a személyes adatok védelméhez fűződő alapjogot a Charta 8. cikkében megállapítottak szerint. Annak ellenére, hogy az irányelv hatályát veszítette és mára egy új jogi eszköz – az általános adatvédelmi rendelet – van érvényben, az előzetesen meglévő ítélkezési gyakorlat továbbra is releváns és érvényes marad az uniós adatvédelmi elvek értelmezése és alkalmazása tekintetében.

39 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

1.2 A személyes adatok védelméhez való jog korlátozása

Főbb pontok

- A személyes adatok védelméhez való jog nem abszolút jog. Ez a jog korlátozható, ha az szükséges általános érdekű célkitűzés megvalósítása vagy mások jogainak és szabadságainak védelme érdekében.
- A magánélethez és a személyes adatok védelméhez való jog korlátozásának feltételeit az EJEE 8. cikke és a Charta 52. cikkének (1) bekezdése ismerteti. Ezek az EJEB és az EUB ítélkezési gyakorlatán keresztül öltöttek testet és értelmeződtek.
- Az Európa Tanács adatvédelmi szabályozása értelmében a személyes adatok kezelése csak akkor minősül a magánélet tiszteletben tartásához való jogba történő jogszerű beavatkozásnak, ha az:
  - megfelel a jogszabályoknak;
  - törvényes célt szolgál;
  - tiszteletben tartja az alapvető jogok és szabadságok lényeges tartalmát;
  - szükséges és arányos egy demokratikus társadalomban valamely törvényes cél eléréséhez.
- Az EU jogrendje hasonló feltételekhez köti a Charta által védett alapjogok gyakorlásának korlátozását. Valamely alapjog, beleértve a személyes adatok védelméhez való jogot, korlátozása kizárólag akkor lehet törvényes, ha az:
  - megfelel a jogszabályoknak;
  - tiszteletben tartja az érintett jog lényeges tartalmát;
  - az arányosság függvényében szükséges; és
  - az Unió által elismert általános érdekű célkitűzéseket követ, vagy mások jogainak védelmét szolgálja.

A Charta 8. cikke szerinti, a személyes adatok védelméhez való alapjog „nem abszolút jog, hanem a társadalomban betöltött szerepének függvényében kell figyelembe venni”.[40] A Charta 52. cikkének (1) bekezdése elfogadja tehát, hogy lehetséges

40 Lásd például: EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9., 48. pont.

a Charta 7. és 8. cikkében említett jogok gyakorlásának korlátozása, feltéve, hogy a korlátozásra a törvény által, a jogok és szabadságok lényeges tartalmának, valamint az arányosság elvének tiszteletben tartásával kerül sor, továbbá a korlátozás elengedhetetlen és ténylegesen az Európai Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.[41] Hasonlóképp, az EJEE rendszerében az adatvédelmet a 8. cikk garantálja, és e jog gyakorlása korlátozható, amennyiben törvényes cél elérése érdekében az szükséges. Ez a szakasz kitér az EJEE értelmében történő beavatkozás feltételeire az EJEB ítélkezési gyakorlata általi értelmezés szerint, valamint a Charta 52. cikke szerinti törvényes korlátozás feltételeire.

1.2.1 Az igazolható beavatkozás EJEE szerinti követelményei

A személyes adatok kezelése az érintett magánéletének tiszteletben tartásához való jogába történő beavatkozásnak minősülhet, amely jog az EJEE 8. cikke szerint védelmet élvez.[42] A fentebb ismertetettek szerint (lásd az 1.1.1 és 1.1.4 szakaszt), az Unió jogrendjével ellentétben, az EJEE nem fogalmazza meg különálló jogként az adatvédelmet. A személyes adatok védelme a magánélet tiszteletben tartásához való jog értelmében védett jogok részét képezi. Így tehát a személyes adatok kezelésével járó bármely tevékenység nem tartozhat az EJEE 8. cikkének hatálya alá. Ahhoz, hogy a 8. cikk életbe lépjen, először azt kell megállapítani, hogy sérült-e magánérdek, vagy valamely személy magánélete. Ítélkezési gyakorlatán keresztül az EJEB a „magánélet" fogalmát tág fogalomként kezeli, amelybe még a szakmai élet és nyilvános viselkedés is beletartozik. Hozott olyan ítéletet is, hogy a személyes adatok védelme a magánélet tiszteletben tartásához való jog fontos része. A magánélet tág értelmezése ellenére azonban nem minden adatkezelés sérti önmagában a 8. cikk értelmében védett jogokat.

Amennyiben az EJEB úgy véli, hogy a szóban forgó adatkezelési művelet érinti az egyén magánélet tiszteletben tartásához való jogát, kivizsgálja, hogy jogos-e a beavatkozás. A magánélet tiszteletben tartásához való jog nem abszolút jog, hanem egyensúlyt kell teremteni közte és más törvényes érdekek és jogok között, és ezekkel össze kell egyeztetni – legyenek azok más személyek (magánérdek) vagy a társadalom érdekei (közérdek).

41 *Uo.*, 50. pont.

42 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4., 67. pont.

A beavatkozás a következő együttes feltételek fennállása mellett lehet indokolt:

A jogszabályokkal összhangban

Az EJEB ítélkezési gyakorlat szerint a beavatkozás akkor áll összhangban a jogszabályokkal, ha bizonyos jellemzőkkel rendelkező hazai jogszabályi rendelkezésen alapszik. A jogszabálynak „hozzáférhetőnek kell lennie az érintett személyek számára, és hatásainak előre láthatónak kell lennie".[43] Egy szabály akkor előre látható, ha „kellő pontossággal van meghatározva ahhoz, hogy egy személy – szükség esetén a megfelelő tanácsokat követve – magatartását ennek megfelelően kiigazítsa".[44] Továbbá, „[a] »jogszabálytól« e tekintetben megkövetelt pontosság mértéke a konkrét tárgytól függ".[45]

Példák: A *Rotaru kontra Románia* ügyben[46] a felperes azt állította, hogy megsértették a magánélet tiszteletben tartásához való jogát azzal, hogy a román titkosszolgálat az ő személyes adatait tartalmazó fájlt vezetett és használt. Az EJEB megállapította, hogy miközben a nemzeti jog megengedte a nemzetbiztonságot érintő információk gyűjtését, rögzítését és titkos fájlokban való archiválását, nem határozta meg e jogkörök gyakorlásának korlátait, amit így a hatóságok mérlegelésére bízott. A hazai jog nem határozta meg például a feldolgozható információk típusát, azon személyek kategóriáit, akikkel szemben megfigyelés foganatosítható, a körülményeket, amelyek fennállása esetén ezen intézkedések meghozhatók, illetve a követendő eljárást. A Bíróság ezért megállapította, hogy a hazai jogszabály nem felel meg az EJEE 8. cikke szerinti előreláthatóság követelményének, és hogy e cikket megsértették.

43 EJEB, *Amann kontra Svájc* [Nagykamara], 27798/95. sz. ügy, 2000. február 16., 50. pont; lásd még: EJEB, *Kopp kontra Svájc*, 23224/94. sz. ügy, 1998. március 25., 55. pont; és EJEB, *Iordachi és társai kontra Moldova*, 25198/02. sz. ügy, 2009. február 10., 50. pont.

44 EJEB, *Amann kontra Svájc* [Nagykamara], 27798/95. sz. ügy, 2000. február 16., 56. pont; lásd még: EJEB, *Malone kontra Egyesült Királyság*, 8691/79. sz. ügy, 1984. augusztus 2., 66. pont; EJEB, *Silver és társai kontra Egyesült Királyság*, 5947/72., 6205/73., 7052/75., 7061/75., 7107/75., 7113/75. sz. ügyek, 1983. március 25., 88. pont.

45 EJEB, *The Sunday Times kontra Egyesült Királyság*, 6538/74. sz. ügy, 1979. április 26., 49. pont.; lásd még: EJEB, *Silver és társai kontra Egyesült Királyság*, 5947/72., 6205/73., 7052/75., 7061/75., 7107/75., 7113/75. sz. ügyek, 1983. március 25., 88. pont.

46 EJEB, *Rotaru kontra Románia* [Nagykamara], 28341/95. sz. ügy, 2000. május 4., 57. pont; lásd még: EJEB, *Association for European Integration and Human Rights és Ekimdzhiev kontra Bulgária*, 62540/00. sz. ügy, 2007. június 28.; EJEB, *Shimovolos kontra Oroszország*, 30194/09. sz. ügy, 2011. június 21.; és EJEB, *Vetter kontra Franciaország*, 59842/00. sz. ügy, 2005. május 31.

A *Taylor-Sabori kontra Egyesült Királyság* ügyben[47] a felperes egy rendőrségi megfigyelés célpontja volt. A felperes személyhívójának „klónozásával" a rendőrség el tudta fogni a neki küldött üzeneteket. A felperest letartóztatták, és megvádolták ellenőrzött gyógyszer átadásában való közreműködéssel. Az ellene emelt vád részben a személyhívóra beérkezett írásos üzenetek rendőrség általi átiratán alapult. A felperes tárgyalásának idején azonban a brit jogban nem volt a magán távközlési rendszeren keresztül továbbított közlések lehallgatását szabályozó rendelkezés. Ezért a felperes jogainak sérelme nem állt „összhangban a jogszabályokkal". Az EJEB arra a következtetésre jutott, hogy ez megsértette az EJEE 8. cikkét.

A *Vukota-Bojić kontra Svájc* ügy[48] egy társadalombiztosítási ellátást igénylő személynek a biztosítója által megbízott magándetektív általi titkos megfigyelésével foglalkozott. Az EJEB úgy vélte, hogy noha a keresetben szereplő megfigyelési intézkedést egy magán biztosítótársaság rendelte meg, e vállalat számára az állam biztosította a jogot arra, hogy a kötelező egészségbiztosításból eredő ellátásokat nyújtson és beszedje a biztosítási díjakat. Az állam nem mentesülhet az egyezmény értelmében fennálló felelőssége alól azzal, hogy kötelezettségeit magánszervezetekre vagy magánszemélyekre ruházza át. A nemzeti jognak megfelelő biztosítékokat kell nyújtania az EJEE 8. cikke szerinti jogokba való beavatkozással való visszaéléssel szemben ahhoz, hogy az a „jogszabályokkal összhangban" lévő legyen. A szóban forgó ügyben az EJEB arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét, mivel a nemzeti jog nem jelezte kellően egyértelműen a biztosítási vitákban hatóságként eljáró biztosítótársaságra átruházott mérlegelési jogkör gyakorlásának alkalmazási körét és módját a biztosítottak titkos megfigyelését illetően. Különösen pedig nem tartalmazott megfelelő biztosítékokat a visszaéléssel szemben.

Törvényes cél előmozdítása

A törvényes cél lehet bármely nevesített közérdek, vagy mások jogainak és szabadságainak védelme. Az EJEE 8. cikkének (2) bekezdése értelmében beavatkozást indokolható törvényes célok lehetnek nemzetbiztonsági, közbiztonsági érdekek, vagy az ország gazdasági jólétének érdeke, zavargás vagy bűncselekmény

47 EJEB, *Taylor-Sabori kontra Egyesült Királyság*, 47114/99. sz. ügy, 2002. október 22.

48 EJEB, *Vukota-Bojić kontra Svájc*, 61838/10. sz. ügy, 2016. október 18., 77. pont.

megelőzése, a közegészség vagy az erkölcsök védelme, vagy mások jogainak és szabadságainak védelme.

Példa: A *Peck kontra Egyesült Királyság* ügyben[49] a felperes csuklójának elvágásával öngyilkosságot kísérelt meg az utcán, nem tudva arról, hogy egy zárt láncú televíziós rendszerhez (CCTV) tartozó kamera filmre veszi őt. A rendőrség, aki figyelte a CCTV-kamerákat, megmentette őt, majd elküldte a videofelvételt a médiának, amely a felperes arcának kitakarása nélkül közzétette azt. Az EJEB megállapította, hogy nincs olyan lényeges vagy elégséges ok, amely indokolná a felvétel hatóságok általi közvetlen nyilvánosságra hozatalát anélkül, hogy megszereznék a felperes hozzájárulását, vagy elfednék személyazonosságát. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Szükséges egy demokratikus társadalomban

Az EJEB kimondta, hogy „a szükségesség fogalma magában foglalja, hogy a beavatkozás kényszerítő társadalmi igénynek felel meg, és azt is, hogy arányos a kitűzött jogszerű céllal".[50] Annak vizsgálatakor, hogy egy intézkedés szükséges-e egy kényszerítő társadalmi igény kezeléséhez, az EJEB azt vizsgálja, hogy az mennyire releváns és megfelelő az elérendő cél szempontjából. E célból mérlegelheti, hogy a beavatkozás egy olyan problémát kísérel-e meg kezelni, amely – ha nem kezelik – káros hatást gyakorolhat a társadalomra, hogy van-e bizonyíték arra vonatkozóan, hogy a beavatkozás mérsékelheti ezt a káros hatást, és hogy a szóban forgó problémára vonatkozóan milyen tágabb társadalmi nézetek léteznek.[51] Például, olyan személyek személyes adatainak biztonsági szolgálatok általi gyűjtése és tárolása, akikről megállapították, hogy rendelkeznek terrorista mozgalmakhoz köthető kapcsolatokkal, az egyén magánélet tiszteletben tartásához való jogába történő beavatkozás, mindazonáltal komoly, nyomós társadalmi szükségletet szolgál, ez pedig a nemzetbiztonság, illetve a terrorizmus elleni küzdelem. Ahhoz, hogy átmenjen a szükségességi vizsgálaton, a beavatkozásnak arányosnak is kell lennie. Az EJEB ítélkezési gyakorlatában az arányosságot a szükségesség fogalmán belül vizsgálja. Az arányossághoz az szükséges, hogy az EJEE alapján védett jogokba való

49 EJEB, *Peck kontra Egyesült Királyság*, 44647/98. sz. ügy, 2003. január 28., 85. pont.

50 EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987. március 26., 58. pont.

51 A 29. cikk alapján létrehozott adatvédelmi munkacsoport (a 29. cikk szerinti munkacsoport) (2014), *Vélemény a szükségesség és arányosság fogalmának alkalmazásáról és az adatvédelemről a bűnüldözési ágazatban*, WP 211, Brüsszel, 2014. február 27, 7–8 o.

beavatkozás ne mutasson túl azon a mértéken, amely a törvényes cél előmozdítása érdekében szükséges. Az arányosság vizsgálatakor fontos és figyelembe veendő tényező a beavatkozás köre, vagyis az érintett személyek száma, valamint az alkalmazott biztosítékok vagy korlátozások figyelembe vétele a beavatkozás körének, illetve az egyének jogaira gyakorolt káros hatások korlátozása érdekében.[52]

Példa: A *Khelili kontra Svájc* ügyben[53] a rendőrség egy rendőri ellenőrzés során a következő szövegű névjegyeket találta a felperesnél: „Kedves, csinos, harmincas évei második felében járó nő megismerkedne egy férfival rendszeres találkozás vagy szabadidős programok céljából. Tel. szám [...]". A felperes állítása szerint ezt követően a rendőrség prostituáltként felvette őt a nyilvántartásába, mely tevékenység folytatását a felperes folyamatosan tagadta. A felperes a „prostituált" szó törlését kérte a számítógépes rendőrségi nyilvántartásból. Az EJEB főszabályként elismerte, hogy az egyén személyes adatainak azon a címen való őrzése, hogy a szóban forgó egyén más bűncselekményt is elkövethet, bizonyos körülmények között arányos lehet. A felperes esetében azonban az illegális prostitúció vádja túl tágnak és általánosnak tűnik, és konkrét tények nem is támasztják alá, mivel a felperest soha nem ítélték el illegális prostitúcióért, ezért a vád nem tekinthető olyannak, amely megfelel az EJEE 8. cikkének értelemben vett „kényszerítő társadalmi szükségletnek". Figyelemmel arra, hogy a hatóságoknak kell bizonyítaniuk a felperesről tárolt adatok pontosságát, figyelemmel továbbá a felperes jogaiba való beavatkozás súlyosságára, a Bíróság úgy ítélte meg, hogy a „prostituált" szó évekig való fenntartása a rendőrségi adatállományban nem szükséges egy demokratikus társadalomban. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: Az *S. és Marper kontra Egyesült Királyság* ügyekben[54] a két felperest letartóztatták, és bűncselekmények elkövetésével vádolták meg. A rendőrség ujjlenyomatot és DNS-mintát vett tőlük a büntetőeljárási törvény rendelkezéseinek megfelelően. A felpereseket soha nem ítélték el a bűncselekmények miatt: az egyiket a bíróság felmentette, a másik ellen folytatott büntetőeljárást pedig megszüntették. Ennek ellenére a rendőrség adatbázisában megtartotta és tárolta ujjlenyomataikat, DNS-profiljukat

52 *Uo.*, 9–11. oldal.

53 EJEB, *Khelili kontra Svájc*, 16188/07. sz. ügy, 2011. október 18.

54 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4.

és sejtmintáikat, és a nemzeti jogszabályok engedélyezték ezek időbeli korlátozás nélküli megőrzését. Miközben az Egyesült Királyság azzal érvelt, hogy az adatok megőrzése segíti a jövőbeli elkövetők azonosítását, és ezért a bűncselekmények megelőzésének és felderítésének törvényes célját szolgálja, az EJEB úgy vélte, hogy indokolatlan a beavatkozás a felperes magánéletének tiszteletben tartásához való jogába. Emlékeztetett arra, hogy az adatvédelem alapelvei előírják, hogy a személyes adatok megőrzése a gyűjtés céljával arányos legyen, és hogy a megőrzési időt korlátozni kell. A Bíróság elfogadta, hogy az adatbázis nemcsak az elítéltek, hanem minden gyanúsított, de el nem ítélt személy DNS-profiljával való bővítése hozzájárulhatott volna a bűncselekmények megelőzéséhez és felderítéséhez az Egyesült Királyságban. Ugyanakkor „az adatmegőrzés válogatás nélküli, általános jellege ezt ellehetetlenítette”.[55]

Figyelemmel a sejtmintákban található hatalmas mennyiségű genetikai és egészségügyi adatra, a felperesek magánélethez való jogába való beavatkozás különösen tolakodó volt. Ujjlenyomatot és DNS-mintát lehetett venni letartóztatott személyektől, és azokat korlátlan ideig meg lehetett tartani a rendőrség adatbázisában függetlenül a bűncselekmény jellegétől vagy súlyától, még börtönbüntetéssel nem sújtható kisebb súlyú bűncselekmények esetében is. Ráadásul korlátozott volt annak lehetősége, hogy a felmentett személyek adatait töröljék az adatbázisból. Végezetül az EJEB különös figyelemben részesítette azt a tényt, hogy az egyik felperes letartóztatása idején mindössze tizenegy éves volt. Egy olyan kiskorú személyes adatainak megőrzése, akit nem ítéltek el, különösen káros, figyelemmel a kiskorú sérülékenységére, valamint fejlődésének és társadalmi integrációjának jelentőségére.[56] A Bíróság egyhangúlag megállapította, hogy az adatok megőrzése a magánélethez való jogba történő aránytalan beavatkozásnak minősül, ami nem tekinthető szükségesnek egy demokratikus társadalomban.

Példa: A *Leander kontra Svédország* ügyben[57] az EJEB megállapította, hogy nemzetbiztonsági szempontból fontos állásra pályázó személyek titkos ellenőrzése önmagában nem ellentétes a demokratikus társadalomban való szükségesség követelményével. Az érintettek érdekeinek védelmére

55 *Uo.*, 119. pont.

56 *Uo.*, 124. pont.

57 EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987. március 26., 59. és 67. pont.

a nemzeti jogban megállapított külön biztosítékok – például a parlament és az igazságügyi miniszter által gyakorolt ellenőrzés – eredményeként az EJEB arra a következtetésre jutott, hogy a svéd személyzeti ellenőrzési rendszer megfelel az EJEE 8. cikkének (2) bekezdésében szereplő követelményeknek. Tekintettel a rendelkezésére álló tág mérlegelési mozgástérre, az alperes állam megfontolhatta, hogy a felperes esetében a nemzetbiztonsági érdek elsőbbséget élvez-e az egyéni érdekkel szemben. A Bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

1.2.2 A jogok törvényes korlátozásának feltételei az EU Alapjogi Chartája értelmében

A Charta szerkezete és szóhasználata is eltér az EJEE-étől. A Charta nem használja a garantált jogokkal való ütközések fogalmát, de tartalmaz egy rendelkezést a Charta által elismert jogok és szabadságok gyakorlásának korlátozásáról.

Az 52. cikk (1) bekezdése szerint a Charta által elismert jogok és szabadságok gyakorlására, és ennek megfelelően a személyes adatok védelméhez való jog gyakorlására vonatkozó korlátozások csak akkor elfogadhatók, ha:

- jogszabály rendelkezik róluk; és
- tiszteletben tartják az adatvédelemhez való jog lényegét; és
- az arányosság függvényében szükségesek;[58] és
- ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálják.

Mivel a személyes adatok védelme a Charta 8. cikkében védett külön és önálló alapjog az uniós jogrendben, bármilyen adatkezelés önmagában is e jogba való beavatkozást jelent. Lényegtelen az, hogy a kérdéses személyes adatok egy egyén magánéletéhez kapcsolódnak, különlegesek, vagy hogy az érintetteknek okoztak-e bármilyen kellemetlenséget. Ahhoz, hogy törvényes legyen, a beavatkozásnak teljesítenie kell a Charta 52. cikkének (1) bekezdésében foglalt valamennyi feltételt.

58 A személyes adatok védelméhez fűződő alapvető jogok korlátozására irányuló intézkedések szükségességének értékelésével kapcsolatban lásd: EDPS (2017), *Necessity Toolkit*, Brüsszel, 2017. április 11.

Jogszabály rendelkezik róluk

A személyes adatok védelméhez való jog korlátozásáról jogszabálynak kell rendelkeznie. Ez a követelmény arra utal, hogy a jog korlátozásának egy olyan jogalapon kell alapulnia, amely kellőképpen hozzáférhető és előre látható, és megfelelő pontossággal kell megfogalmazni ahhoz, hogy lehetővé tegye az egyén számára kötelezettségeinek megértését és magatartásának kiigazítását. A jogalapnak továbbá kellő világossággal kell meghatároznia az illetékes hatóságok hatásköre gyakorlásának terjedelmét és módját, hogy az egyén számára védelmet biztosítson a visszaélésekkel szemben. Ez az értelmezés hasonlít az EJEB ítélkezési gyakorlata szerinti „jogos beavatkozás" követelményére,[59] és felmerült, hogy a Chartában használt „a törvényben rögzített" kifejezés jelentésének meg kellene egyeznie az EJEE-vel összefüggésben ennek tulajdonított jelentésnek.[60] Az EJEB ítélkezési gyakorlata, és különösen az általa az évek során kialakult „törvényi minőség" fogalma egy lényeges szempont, amelyet az EUB-nek figyelembe kell vennie a Charta 52. cikke (1) bekezdése hatályának értelmezésekor.[61]

Tiszteletben tartják a jog lényegét

Az EU jogrendjében a Chartában védett alapjogok minden korlátozásának tiszteletben kell tartania az érintett jogok lényegét. Ezt azt jelenti, hogy nem indokolható a jogok olyan korlátozása, amely olyan széles körű és betolakodó, hogy megfosztja valamely alapjogot annak alapvető tartalmától. Ha a jog lényege sérül, a korlátozást törvénytelennek kell tekinteni arra vonatkozó további vizsgálat szükségessége nélkül, hogy az általános érdekű célkitűzéseket szolgál-e, és kielégíti-e a szükségességre és arányosságra vonatkozó kritériumokat.

> Példa: A *Schrems* ügy[62] az egyének védelmével foglalkozott személyes adataik harmadik országba – az adott esetben az Egyesül Államokba – továbbítását illetően. Schrems, egy osztrák állampolgár, aki éveken keresztül Facebook-felhasználó volt, panaszt nyújtott be az ír adatvédelmi felügyeleti

59 *Uo.*, 4. o.; lásd még: EUB, *A Bíróság 1/15. sz. véleménye* [nagytanács], 2017. július 26.

60 EUB, *Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Tom Watson, Peter Brice, Geoffrey Lewis*, Saugmandsgaard Øe főtanácsnok indítványa, C-203/15. és C-698/15. sz. egyesített ügyek, 2016. július 19., 140. pont.

61 EUB, *Scarlet Extended SA kontra Société belge des auteurs compositeurs et éditeurs (SABAM)*, Cruz Villalón főtanácsnok indítványa, C-70/10. sz. ügy, 2011. április 14., 100. pont.

62 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

hatóságnál, amelyben kifogásolta személyes adatainak továbbítását a Facebook ír leányvállalatától a Facebook Inc. vállalat részére, és az USA-ban lévő szerverekre, ahol azokat kezelték. Azzal érvelt, hogy figyelemmel Edward Snowden, egy visszaélést bejelentő amerikai személy által 2013-ban az Egyesült Államok hírszerző szolgálatainak a tevékenységeire vonatkozóan kiszivárogtatott információkra, az Egyesült Államok joga és gyakorlata nem biztosít elégséges védelmet az amerikai területre továbbított személyes adatok tekintetében. Snowden feltárta, hogy a National Security Agency (Nemzetbiztonsági Ügynökség) közvetlenül rákapcsolódik cégek, például a Facebook szervereire, és elolvashatja a csevegések és privát üzenetek tartalmát.

Az adatok USA-ba történő továbbítása egy 2000-ben elfogadott bizottsági megfelelőségi határozaton alapult, amely lehetővé teszi az adattovábbítást azon amerikai vállalatok számára, amelyek nyilatkoztak arról, hogy az EU-ból továbbított személyes adatokat védik, és megfelelnek az ún. „biztonságos kikötő" adatvédelmi elveknek. Amikor az ügyet az EUB elé vitték, a Bíróság a Charta alapján vizsgálta meg a bizottsági határozatot. Emlékeztetett arra, hogy az EU-ban az alapjogok védelmével szemben támasztott követelmény, hogy az érintett jogokra vonatkozó eltérések és korlátozások a feltétlen szükségesre korlátozódjanak. Az EUB az olyan szabályozást, amely lehetővé teszi a közjogi hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához, úgy tekintette, hogy az „a magánélet tiszteletben tartásához való, a Charta 7. cikkében biztosított alapvető jog lényegét sérti". A jogot a lényegétől fosztaná meg, ha az amerikai hatóságok válogatás nélkül hozzáférhetnének az elektronikus kommunikációhoz, anélkül hogy szükség lenne az érintett egyénekkel konkrét kapcsolatban nemzetbiztonsági vagy bűnmegelőzési megfontolásokra alapított objektív igazolásra, és anélkül hogy e megfigyelési gyakorlatokhoz megfelelő visszaélésekkel szembeni garanciák társulnának.

Ráadásul az EUB megállapította, hogy „az olyan szabályozás, amely nem biztosítja a jogalany számára a jogorvoslat lehetőségét abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse", összeegyeztethetetlen a hatékony bírói jogvédelemhez való alapjoggal (Charta 47. cikk). Ezért a biztonságos kikötőről szóló határozat lényegét tekintve nem biztosította az alapjogoknak

a Charta fényében értelmezett irányelv alapján az EU-ban garantált védelmi szinttel egyenértékű védelmét. Az EUB következésképp érvénytelenítette a határozatot.[63]

Példa: A *Digital Rights Ireland* ügyben[64] az EUB megvizsgálta a 2006/24/EK irányelv (adatmegőrzési irányelv) összeegyeztethetőségét a Charta 7. és 8. cikkével. Az irányelv kötelezte az elektronikus hírközlési szolgáltatókat, hogy a forgalommal és a helymeghatározással kapcsolatos adatokat legalább hat és legfeljebb 24 hónapig megőrizzék, és hogy az illetékes nemzeti hatóságok számára hozzáférést biztosítsanak ezen adatokhoz súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében. Az irányelv nem engedélyezte az elektronikus kommunikáció tartalmának megőrzését. Az EUB megjegyezte, hogy az irányelv alapján a szolgáltatók által megőrizendő adatok tartalmazzák a közlés forrásának és címzettjének megtalálásához és azonosításához, továbbá valamely közlés napjának, időpontjának, időtartamának meghatározásához szükséges adatokat, a hívó telefonszámát és a hívott számot, valamint az IP-címet. Ezek az adatok „együttesen véve, igen pontos következtetések levonását tehetik lehetővé azon személyek magánélete vonatkozásában, akiknek az adatait megőrizték, így például a napi szokások, az állandó vagy ideiglenes tartózkodási helyek, a napi vagy egyéb helyváltoztatások, a gyakorolt tevékenységek, az e személyek társadalmi kapcsolatai és az általuk látogatott társadalmi közegek tekintetében."

Ezért a személyes adatok irányelv szerinti megőrzése a magánélet és a személyes adatok védelméhez való jogba történő különösen súlyos beavatkozásnak minősült. Az EUB azonban úgy vélte, hogy a beavatkozás nem befolyásolta hátrányosan e jogok lényegét. A magánélethez való jogot illetően, nem sérült a jog lényeges tartalma, mivel az irányelv nem tette lehetővé magának az elektronikus közlések tartalmának a megismerését. Hasonlóképpen, a személyes adatok védelméhez való jog lényege sem

63 Az EUB 520/2000/EK bizottsági határozat érvénytelenné nyilvánítására irányuló ítélete egyéb okokon is alapult, amelyeket e kézikönyv más fejezeteiben fogunk megvizsgálni. Nevezetesen, az EUB úgy vélte, hogy a határozat törvénytelenül korlátozta a nemzeti adatvédelmi felügyeleti hatóságok hatáskörét. Ezenkívül a „biztonságos kikötő" rendszere keretében nem állt rendelkezésre jogorvoslati lehetőség az egyének számára arra az esetre, ha be kívántak volna tekinteni a rájuk vonatkozó személyes adatokba, és/vagy azok helyesbítését vagy törlését kérték volna. Ezért sérült a Charta 47. cikkében rögzített hatékony hatékony bírói jogvédelemhez való alapjog is.

64 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

sérült, mivel az irányelv előírta az elektronikus hírközlési szolgáltatók számára bizonyos adatvédelmi és adatbiztonsági elvek betartását, illetve e célból megfelelő technikai és szervezési intézkedések megvalósítását.

Szükségesség és arányosság

A Charta 52. cikkének (1) bekezdése kimondja, hogy az arányosság elvére figyelemmel, a Chartában elismert alapjogok és szabadságok gyakorlásának korlátozására csak akkor kerülhet sor, ha az szükséges.

A korlátozás akkor lehet **szükséges**, ha a követett közérdekű cél érdekében szükség van intézkedések elfogadására, azonban a szükségesség EUB általi értelmezése magában foglalja azt is, hogy az elfogadott intézkedéseknek kevésbé beavatkozó jellegűnek kell lenniük az ugyanazon cél elérésének egyéb lehetőségeihez viszonyítva. A magánélet tiszteletben tartásához és a személyes adatok védelméhez való jogok korlátozására az EUB szigorú szükségességi vizsgálatot alkalmaz, mivel úgy véli, hogy „a kivételeknek és korlátozásoknak a feltétlenül szükséges határokon belül kell maradniuk". Ha egy korlátozás feltétlenül szükségesnek minősül, azt is meg kell vizsgálni, hogy az arányos-e.

Az **arányosság** az jelenti, hogy a jog korlátozásából származó előnyök meghaladják a korlátozás által érintett alapjog gyakorlása tekintetében okozott hátrányokat.[65] A magánélethez és az adatvédelemhez való jog élvezetét befolyásoló hátrányok és kockázatok csökkentése érdekében fontos, hogy a korlátozások megfelelő garanciákat tartalmazzanak.

Példa: A *Volker und Markus Schecke* ügyben[66] az EUB arra a következtetésre jutott, hogy a Tanács és a Bizottság azzal, hogy kötelezővé tette bizonyos mezőgazdasági alapokból nyújtott támogatások valamennyi természetes személy kedvezményezettjeire vonatkozó személyes adatoknak a közzétételét – anélkül, hogy különbséget tett volna lényeges kritériumok alapján (ilyenek például az időszak, amelyen keresztül a szóban forgó személyek a támogatást kapták, a támogatás gyakorisága, jellege vagy összege) –, túllépett az arányosság elve tiszteletben tartása által megkövetelt határokon.

65 EDPS (2017), *Necessity Toolkit*, 5. o.

66 EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9., 89. és 86. pont.

Ezért az EUB szükségesnek találta az 1290/2005/EK tanácsi rendelet bizonyos rendelkezéseinek érvénytelenítését, továbbá a 259/2008/EK rendeletet teljes egészében érvénytelennek nyilvánította.[67]

Példa: A *Digital Rights Ireland* ügyben[68] az EUB úgy vélte, hogy az adatmegőrzési irányelv által okozott beavatkozás a magánélethez való jogba nem sértette a szóban forgó jog lényegét, mivel tiltotta az elektronikus közlések tartalmának megőrzését. Ugyanakkor arra a következtetésre jutott, hogy az irányelv összeegyeztethetetlen a Charta 7. és 8. cikkével, és érvénytelennek nyilvánította azt. Mivel a forgalommal és a helymeghatározással kapcsolatos adatokat összesítve és egészébe véve lehetne elemezni, és részletes képet lehetne alkotni az egyének magánéletéről, e jogokba való súlyos beavatkozásnak minősült. Az EUB figyelembe vette, hogy az irányelv előírta a vezetékestelefon-szolgáltatásokra, a mobiltelefon-szolgáltatásokra, az internet-hozzáférésre, az internetes telefonálásra és az internetes elektronikus levelekre vonatkozó összes metaadat megőrzését, így valamennyi olyan elektronikus hírközlési eszközt érinti, amelynek a használata a mindennapi élet során igen elterjedt. Gyakorlatilag az érintett jogba való olyan mértékű beavatkozást jelentett, amely Európa teljes népességét érintette. Figyelemmel a beavatkozás mértékére és súlyosságára, a forgalommal és a helymeghatározással kapcsolatos adatok megőrzése az EUB szerint kizárólag súlyos bűncselekmények elleni küzdelem céljából lehet indokolt. Ezenkívül az irányelv nem állapít meg olyan objektív kritériumokat, amelyek biztosítanák, hogy az illetékes hatóságok által a megőrzött adatokhoz való hozzáférés szigorúan a feltétlenül szükséges mértékre korlátozódjon. Ráadásul nem tartalmazott a megőrzött adatokhoz való nemzeti hatóságok általi hozzáférést és azok felhasználását szabályozó anyagi jogi és eljárásjogi feltételeket, és a hozzáférést, illetve felhasználást nem tette függővé bíróság vagy egyéb független testület előzetes felülvizsgálatától.

67 A Tanács 1290/2005/EK rendelete (2005. június 21.) a közös agrárpolitika finanszírozásáról, HL L 209., 2005.8.11.; a Bizottság 259/2008/EK rendelete (2008. március 18.) az 1290/2005/EK tanácsi rendeletnek az Európai Mezőgazdasági Garanciaalapból (EMGA) és az Európai Mezőgazdasági Vidékfejlesztési Alapból (EMVA) származó pénzeszközök kedvezményezettjeire vonatkozó információk nyilvánosságra hozatalának tekintetében történő alkalmazása részletes szabályainak megállapításáról, HL L 76., 2008.3.19.

68 EUB, *Digital Rights Ireland Ltd kontra v Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8., 39. pont.

Az EUB hasonló következtetésre jutott a *Tele2 Sverige AB kontra Post- och telestyrelsen* és *Secretary of State for the Home Department kontra Tom Watson és társai* egyesített ügyeknél.[69] Ezek az ügyek „minden elektronikus hírközlési berendezés tekintetében valamennyi előfizető és nyilvántartott felhasználó" összes forgalmi és helymeghatározó adatának „a követett cél szerinti különbségtétel, korlátozás vagy kivétel nélküli" megőrzésével foglalkoztak.[70] A szóban forgó esetben az adatok megőrzése tekintetében nem volt feltétel, hogy az érintett személy közvetlenül vagy közvetetten súlyos bűncselekménnyel álljon kapcsolatban, vagy hogy az illető közleményei nemzetbiztonsági szempontból relevánsak legyenek. Figyelemmel arra, hogy hiányzott a szükséges kapcsolat a megőrzött adatok és a közbiztonság elleni fenyegetés között, az EUB arra a következtetésre jutott, hogy a nemzeti szabályozás túllépett a súlyos bűncselekmények elleni küzdelem céljából feltétlenül szükséges mértéken.[71]

A szükségességet tekintve hasonló megközelítést alkalmazott az európai adatvédelmi biztos a *Necessity Toolkitben (szükségességi eszköztár)*.[72] Az eszköztár célja, hogy segítsen megállapítani a javasolt intézkedések uniós adatvédelmi joggal való összeegyeztethetőségét. Kidolgozását az vezérelte, hogy a személyes adatok kezeléséért, valamint a személyes adatok védelmét, illetve a Chartában rögzített egyéb jogok és szabadságok korlátozását érintő intézkedések előkészítéséért és ellenőrzéséért felelős uniós politikai döntéshozókat jobb eszköztárral lássák el.

Általános érdekű célkitűzések

Ahhoz, hogy a Chartában elismert jogok gyakorlásának korlátozása indokolt legyen, annak az Unió által elismert közérdekű célokhoz, illetve a másokat megillető jogok és szabadságok védelméhez szükségesnek kell lennie, és azoknak ténylegesen meg kell felelnie. A másokat megillető jogok és szabadságok védelméhez szükséges jelleget illetően a személyes adatok védelméhez való jog gyakran kölcsönhatásban van más alapjogokkal. Az 1.3 szakasz részletesen elemzi az ilyen kölcsönhatásokat. A közérdekű célokat tekintve ide tartoznak az EU-nak az Európai Unió Működéséről

69 EUB, *Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016. december 21., 105–106. pont.

70 *Uo.*, 105. pont.

71 *Uo.*, 107. pont.

72 EDPS (2017), *Necessity Toolkit*, Brüsszel, 2017. április 11.

szóló szerződés (EUMSZ) 3. cikkében rögzített általános céljai, például a béke és az Unió népei jólétének előmozdítása, társadalmi igazságosság és védelem, a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség létrehozása, ahol a személyek szabad mozgásának biztosítása a bűnmegelőzésre és bűnüldözésre irányuló megfelelő intézkedésekkel párosul, valamint a Szerződések konkrét rendelkezései által védett egyéb célkitűzések és érdekek.[73] Az általános adatvédelmi rendelet e tekintetben tovább konkretizálja a Charta 52. cikkének (1) bekezdését: A 23. cikk (1) bekezdése egy sor olyan közérdekű célt sorol fel, amelyek jogszerűnek tekinthetők az egyének jogainak korlátozására, feltéve, hogy a korlátozás tiszteletben tartja a személyes adatok védelméhez való jog lényegét, valamint szükséges és arányos. Az említett közérdekű célok között szerepel a nemzetbiztonság és védelem, bűnmegelőzés, az EU vagy a tagállamok fontos gazdasági és pénzügyi érdekeinek védelme, illetve a közegészség és szociális biztonság.

Fontos kellő részletességgel meghatározni és magyarázni a korlátozással követett közérdekű célt, mivel a korlátozás szükségességét e körülményekre tekintettel kell megítélni. A korlátozás és a javasolt intézkedések céljának egyértelmű és részletes leírása elengedhetetlen annak megállapításához, hogy az szükséges-e.[74] A követett cél, valamint a korlátozás szükségessége és arányossága szorosan kapcsolódik egymáshoz.

Példa: A *Schwarz kontra Stadt Bochum* ügy[75] a magánélet tiszteletben tartásához való jognak és a személyes adatok védelméhez való jognak az útlevél-kibocsátáskor a tagállami hatóságok által vett és tárolt ujjlenyomatok kapcsán felmerült korlátozásával foglalkozott.[76] A felperes Bochumban igényelt útlevelet, de nem engedte meg, hogy ujjlenyomatot vegyenek tőle. Ezt követően Bochum városa elutasította az útlevél iránti kérelmét. Ezután eljárást indított a német bíróság előtt annak érdekében, hogy útlevelét ujjlenyomat nélkül adják ki. A német bíróság az ügyet az EUB elé vitte azt kérdezve, hogy a tagállamok által kiállított útlevelek és úti okmányok biztonsági jellemzőire és biometrikus elemeire vonatkozó előírásokról szóló 2252/2004 rendelet 1. cikkének (2) bekezdése érvényesnek minősül-e.

73 Magyarázatok az Alapjogi Chartához, HL C 303., 2007.12.14.

74 EDPS (2017), *Necessity Toolkit*, Brüsszel, 2017. április 11., 4. o.

75 EUB, *Michael Schwarz kontra Stadt Bochum*, C-291/12. sz. ügy, 2013. október 17.

76 *Uo.*, 33–36. pont.

Az EUB rámutatott arra, hogy az ujjlenyomatok **személyes adatnak minősülnek**, mivel azok objektíven olyan egyedi információt tartalmaznak egy egyénről, amely lehetővé teszi az illető pontos azonosítását, míg az ujjlenyomat vétele és tárolása adatkezelésnek minősül. Ez utóbbi adatkezelés, amelyet a 2252/2004 rendelet 1. cikkének (2) bekezdése szabályoz, a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő jogok megsértésének minősül.[77] A Charta 52. cikkének (1) bekezdése ugyanakkor lehetővé teszi e jogok gyakorlásának korlátozását, amennyiben a korlátozást törvény írja elő, tiszteletben tartja az érintett jogok lényegét, és összhangban van az arányosság elvével, szükséges, és ténylegesen az Unió által elismert általános érdekű célkitűzéseket vagy mások jogainak és szabadságainak védelmét szolgálja.

A jelen ügynél az EUB először megjegyezte, hogy az útlevél-kibocsátáskor vett és tárolt ujjlenyomatok kapcsán felmerült korlátozást **törvényben előírtnak** kell tekinteni, mivel ezekről a 2252/2004 rendelet 1. cikkének (2) bekezdése rendelkezik. Másodszor, ez utóbbi rendelet célja az útlevelek hamisításának és csalárd használatának megelőzése. Az 1. cikk (2) bekezdése tehát többek között azt a célt szolgálja, hogy megakadályozza az illegális belépést az EU-ba, és ezért az Unió által elismert általános érdekű célkitűzést szolgál. Harmadszor, az EUB rendelkezésére álló bizonyítékokból nem derült ki, és nem is állították, hogy e jogok korlátozása a jelen ügyben nem tartotta volna tiszteletben e jogok lényeges tartalmát. Negyedszer, az ujjlenyomatok felettébb biztonságos tárolóelemen való, a szóban forgó rendelkezésben előírt megőrzése technikai kifinomultsággal jár. Az ilyen tárolás alkalmas az útlevél-hamisítás kockázatának csökkentésére, valamint az útlevelek valódiságának a határokon történő ellenőrzésével megbízott hatóságok feladatának megkönnyítésére. Az a tény, hogy a módszer nem teljesen megbízható, nem döntő. Jóllehet a módszer nem zárja ki teljes mértékben a jogosulatlan személyek számára a beengedést, elegendő, ha jelentős mértékben csökkenti az ilyen beengedések valószínűségét. Figyelemmel az előzőekre az EUB azt állapította meg, hogy az ujjlenyomatok 2252/2004 rendelet 1. cikkének (2) bekezdésében említett gyűjtése és tárolása megfelelő a szóban forgó rendelet által követett cél és tágabb értelemben az Unió területére való illegális belépés megakadályozására irányuló cél eléréséhez.[78]

77 *Uo.*, 27–30. pont.

78 *Uo.*, 35–45. pont.

Az EUB ezt követően megvizsgálta, hogy ez az adatkezelés **szükséges**-e, megjegyezve, hogy a kérdéses intézkedés pusztán két ujj lenyomatának levételéből áll, amelyeket egyébként rendszerint mások is láthatnak, tehát nem intim jellegű műveletről van szó**.** Ez a művelet nem okoz különösebb testi vagy lelki kellemetlenséget sem az érdekelt számára, mint ahogyan az arckép készítése sem. Meg kell állapítani azt is, hogy az ujjlenyomatvételnek az EUB előtti eljárás során hivatkozott egyetlen valódi alternatívája az íriszfelismerés. Márpedig az EUB-hez benyújtott iratokból egyáltalán nem következik az, hogy ez utóbbi eljárás az ujjlenyomatvételnél kevésbé sértené a Charta 7. és 8. cikkében elismert jogokat. Ezen túlmenően e két módszer hatékonyságát illetően nem vitatott, hogy az íriszfelismerésen alapuló módszer technikai fejlettségének szintje még nem éri el az ujjlenyomatokon alapuló módszer technikai fejlettségének szintjét. Az íriszfelismerés egyébként jelenleg érezhetően költségesebb, mint az ujjlenyomatok összehasonlítása, ekként pedig kevésbé alkalmas arra, hogy általános körűen alkalmazzák. Következésképpen az EUB nem szerzett tudomást olyan intézkedések meglétéről, amelyek eléggé hatékonyan tudnának hozzájárulni az útlevelek csalárd felhasználással szembeni védelmére irányuló célhoz, és amelyek ugyanakkor az ujjlenyomatokon alapuló módszernél kevésbé sértenék a Charta 7. és 8. cikkében elismert jogokat.[79]

Az EUB megjegyezte, hogy a 2252/2004 rendelet 4. cikkének (3) bekezdése kifejezetten pontosítja, hogy az ujjlenyomatok kizárólag az okmány valódiságának, valamint birtokosa személyazonosságának ellenőrzése céljából használhatók fel, míg a rendelet 1. cikkének (2) bekezdése az ujjlenyomatok megőrzését csupán maga az útlevél tekintetében írja elő, amely továbbra is jogosultjának kizárólagos birtokában marad. A rendelet tehát nem biztosított jogalapot az értelmében gyűjtött adatok központi tárolásához, vagy az ilyen adatoknak az EU területére való jogellenes belépés megakadályozására irányulótól eltérő célokra történő felhasználásához.[80] A fenti megfontolások összességére tekintettel az EUB megállapította, hogy az említett kérdés megvizsgálása során nem tárt fel olyan tényezőket, amelyek érintenék a 2252/2004 rendelet 1. cikke (2) bekezdésének érvényességét.

79 *Uo.*, 46–53. pont.

80 *Uo.*, 56–61. pont.

A Charta és az EJEE közötti kapcsolat

Az eltérő megszövegezés ellenére a jogok Charta 52. cikkének (1) bekezdésében foglalt törvényes korlátozásának feltételei a magánélet tiszteletben tartásához való jog tekintetében emlékeztetnek az EJEE 8. cikke (2) bekezdésére. Ítélkezési gyakorlatukban az EUB és az EJEB gyakran hivatkozik egymás ítéleteire a két bíróság arra irányuló folyamatos párbeszéde részeként, hogy harmonizált módon értelmezzék az adatvédelmi szabályokat. A Charta 52. cikkének (3) bekezdése kimondja, hogy „amennyiben e Charta olyan jogokat tartalmaz, amelyek megfelelnek az emberi jogok és alapvető szabadságok védelméről szóló európai egyezményben biztosított jogoknak, akkor e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek.”. A Charta 8. cikke azonban közvetlenül nem egyezik meg az EJEE egyik cikkével sem.[81] A Charta 52. cikkének (3) bekezdése az egyes jogrendek által védett jogok tartalmával és terjedelmével foglalkozik, nem pedig azok korlátozásával. A két bíróság közötti párbeszéd és együttműködés szélesebb összefüggését tekintve az EUB elemzései során figyelembe veheti a törvényes korlátozás EJEE 8. cikke szerinti feltételeit az EJEB értelmezésének megfelelően. De létezik egy ezzel ellentétes forgatókönyv is, amikor az EJEB hivatkozik a Charta szerinti törvényes korlátozás feltételeire. Bármelyik eset is álljon fenn, figyelembe kell venni, hogy az EJEE nem tartalmaz a Charta 8. cikkével tökéletesen egyenértékű rendelkezést, amely a személyes adatok védelmére, nevezetesen pedig az érintett jogaira, az adatkezelés jogszerű okára és független hatóság általi felügyeletre hivatkozna. A Charta 8. cikkének egyes elemei megtalálhatók az EJEB-nek az EJEE 8. cikke alapján és a 108. Egyezményhez kapcsolódóan kialakított ítélkezési gyakorlatában.[82] Ez a kapcsolat biztosítja az EUB és az EJEB közötti kölcsönös ösztönzés meglétét az adatvédelemhez kapcsolódó ügyekben.

1.3 Kölcsönhatás egyéb jogokkal és jogos érdekekkel

Főbb pontok

- Az adatvédelemhez való jog gyakran kölcsönhatásban van más jogokkal, például a véleménynyilvánítás szabadságával és az információk megismerésének és közlésének jogával.

81 EDPS (2017), *Necessity Toolkit*, Brüsszel, 2017. április 11., 6. o.

82 Magyarázatok az Alapjogi Chartához, 8. cikk.

- Ez a kölcsönhatás gyakran ambivalens: miközben léteznek szituációk, ahol feszültség van a személyes adatok védelméhez való jog és egy konkrét jog között, addig léteznek olyan szituációk is, ahol a személyes adatok védelméhez való jog hatékonyan biztosítja ugyanazon konkrét jog tiszteletben tartását. Például ez áll fenn a véleménynyilvánítás szabadságának esetében, figyelemmel arra, hogy a szakmai titoktartás a magánélet tiszteletben tartásához való jog eleme.
- A mások jogai és szabadságai védelmének szükségessége egyike azon kritériumoknak, amelyek alapján a személyes adatok védelméhez való jog korlátozását rendszerint megvizsgálják.
- Amikor eltérő jogok érintettek, a bíróságoknak mérlegelniük kell, hogy összeegyeztessék azokat.
- Az általános adatvédelmi rendelet előírja a tagállamok számára, hogy egyeztessék össze a személyes adatok védelméhez való jogot a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal.
- A tagállamoknak továbbá konkrét szabályokat kell elfogadniuk nemzeti jogukban annak érdekében, hogy a személyes adatok védelméhez való jogot össze lehessen egyeztetni a hivatalos dokumentumokhoz való hozzáféréssel és a szakmai titoktartási kötelezettségekkel.

A személyes adatok védelméhez való jog nem abszolút jog; e jog jogos korlátozásának feltételeit fentebb részleteztük. A jogok jogos korlátozásának egyik feltétele, amelyet az Európa Tanács és az EU joga egyaránt elismer, az az, hogy az adatvédelembe való beavatkozás mások jogainak és szabadságainak védelme érdekében szükséges. Azokban az esetekben, amikor az adatvédelem más jogokkal kerül kölcsönhatásba, az EJEB és az EUB egyaránt ismételten kijelentette, hogy megfelelő egyensúlyt kell teremteni az egyéb jogokkal az EJEE 8. cikkének és a Charta 8. cikkének alkalmazása és értelmezése során.[83] Számos fontos példa szemlélteti e mérlegelés folyamatát.

E bíróságok által végzett mérlegelés mellett az államok, amennyiben szükséges, jogszabályt fogadhatnak el a személyes adatok védelméhez való jog más jogokkal való összeegyeztetése érdekében. Ez okból az általános adatvédelmi rendelet

83 EJEB, *Von Hannover kontra Németország (no. 2)* [Nagykamara], 40660/08. és 60641/08. sz. ügyek, 2012. február 7.; EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24., 48. pont; EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008. január 29., 68. pont.

számos olyan területet határoz meg, ahol eltérést biztosító nemzeti rendelkezés hozható.

A véleménynyilvánítás szabadságát illetően az általános adatvédelmi rendelet kötelezi a tagállamokat, hogy jogszabályban egyeztessék össze „a személyes adatok e rendelet szerinti védelméhez való jogot a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal, ideértve a személyes adatok újságírási célból, illetve tudományos, művészi vagy irodalmi kifejezés céljából végzett kezelését is".[84] A tagállamok egyedi szabályokat is elfogadhatnak annak érdekében, hogy összeegyeztessék az adatvédelmet a hivatalos dokumentumokhoz való nyilvános hozzáféréssel és a magánélet tiszteletben tartásához való jog egy formájaként védett szakmai titoktartási kötelezettségekkel.[85]

1.3.1 A véleménynyilvánítás szabadsága

Az adatvédelemhez való joggal legkomolyabban ütköző egyik jog a véleménynyilvánításhoz való jog.

A véleménynyilvánítás szabadságát a Charta 11. cikke (A véleménynyilvánítás és a tájékozódás szabadsága) védi. Ez a jog magában foglalja „a véleményalkotás szabadságát, valamint az információk és eszmék megismerésének és közlésének szabadságát anélkül, hogy ebbe hatósági szerv beavatkozhatna, továbbá országhatárokra való tekintet nélkül". Mind a Charta 11. cikke, mind pedig az EJEE 10. cikke szerinti tájékozódási szabadság nemcsak az információk átadásához, hanem *átvételéhez* való jogot is védelemben részesíti.

A véleménynyilvánítás szabadsága korlátozásának összeegyeztethetőnek kell lennie a Charta 52. cikkének (1) bekezdésében foglalt, fentebb ismertetett feltételekkel. Ezenkívül a 11. cikk megfelel az EJEE 10. cikkének. A Charta 52. cikkének (3) bekezdése szerint: amennyiben a Charta olyan jogokat tartalmaz, amelyek megfelelnek az EJEE-ben biztosított jogoknak, akkor „e jogok tartalmát és terjedelmét azonosnak kell tekinteni azokéval, amelyek az említett egyezményben szerepelnek". A Charta 11. cikkében biztosított jog jogszerű korlátozása tehát nem terjedhet túl az EJEE 10. cikkének (2) bekezdésében említett korlátozásokon, azaz a korlátozást törvényben kell meghatározni, és „mások jó hírneve vagy jogai védelme [...] céljából" szükséges intézkedésnek kell minősülnie. Az ilyen jogok nevezetesen

84 Általános adatvédelmi rendelet, 85. cikk.

85 *Uo.*, 86. és 90. cikk.

magukban foglalják a magánélet tiszteletben tartásához való jogot és a személyes adatok védelméhez való jogot.

A személyes adatok védelme és a véleménynyilvánítás szabadsága közötti kapcsolatra az általános adatvédelmi rendeletnek „A személyes adatok kezelése és a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog" című 85. cikke az irányadó. E cikknek megfelelően a tagállamok összeegyeztetik a személyes adatok védelméhez való jogot a véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal. Az általános adatvédelmi rendelet konkrét fejezeteiből eredő mentességeket és eltéréseket különösen újságírási célból, valamint tudományos, művészi vagy irodalmi kifejezés céljából célszerű meghatározni, amennyiben ezek szükségesek a személyes adatok védelméhez való jog véleménynyilvánítás szabadságához és a tájékozódáshoz való joggal való összeegyeztetéséhez.

Példa: A *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy* ügyben[86] az EUB-t megkérték, hogy határozza meg az adatvédelem és a sajtószabadsághoz való jog közötti kapcsolatot.[87] 1,2 millió magánszemélynek a finn adóhatóságtól törvényesen beszerzett, adózásra vonatkozó adatainak egy vállalat által SMS-ben történő terjesztését kellett megvizsgálnia. A finn adatvédelmi felügyeleti hatóság egy határozatot adott ki, amelyben ezen adatok terjesztésének megszüntetésére kötelezi a vállalatot. A vállalat egy nemzeti bíróság előtt megtámadta ezt a határozatot, amely felkérte az EUB-t, hogy tisztázza az adatvédelmi irányelv értelmezését. Az EUB-nek különösen azt kellett értékelnie, hogy a személyesadat-kezelés, amit az adóhatóság azért tett lehetővé, hogy a mobiltelefon-használók más természetes személyekre vonatkozó adózási adatokat kaphassanak, kizárólag újságírás céljából végzett tevékenységnek minősül-e. Miután az EUB arra a következtetésre jutott, hogy a vállalat tevékenysége az adatvédelmi irányelv 3. cikkének (1) bekezdése értelmében „személyes adatok kezelésének" minősül, elemezte az irányelv (a személyes adatok feldolgozásáról és a szólásszabadságról szóló) 9. cikkét.

86 EUB, *Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy* [nagytanács], C-73/07. sz. ügy, 2008. december 16., 56., 61. és 62. pont.

87 A ügy az adatvédelmi irányelv 9. cikkének – amelyet felváltott az általános adatvédelmi rendelet 85. cikke – értelmezésével foglalkozott, amely a következőképpen szól: „A tagállamok e fejezet, a IV. és a VI. fejezet rendelkezései alóli felmentésről, illetve eltérésről kizárólag a személyes adatoknak újságírás, vagy irodalmi, illetve művészi kifejezés céljából történő feldolgozása esetén rendelkezhetnek, amennyiben azok a magánélet tiszteletben tartásához való jognak a szólásszabadságra vonatkozó szabályokkal való összeegyeztetéséhez szükségesek".

Először megállapította a véleménynyilvánítás szabadságához való jog fontosságát minden demokratikus társadalomban, és kijelentette, hogy az e szabadsággal kapcsolatos fogalmakat, például az újságírás fogalmát, tágan kell értelmezni. Ezután megállapította, hogy a két alapvető jog közötti egyensúly megteremtéséhez az adatvédelemhez való jog alóli kivételeket és korlátozásokat kizárólag a feltétlenül szükséges mértékben kell alkalmazni. Ilyen körülmények között az EUB megítélése szerint a szóban forgó vállalatok által a nemzeti jogszabályok szerint nyilvánosan hozzáférhető dokumentumokból származó adatokkal kapcsolatban végzett tevékenységek „újságírás céljából végzett tevékenységnek" minősíthetők, ha információk, vélemények vagy gondolatok nagyközönségnek történő közlésére irányulnak – függetlenül a továbbításukhoz használt médiumtól. Azt is megállapította, hogy e tevékenységek nem korlátozódnak csupán a médiavállalkozásokra, és jövedelemszerzés céljából is végezhetők. Az EUB annak eldöntését azonban a nemzeti bíróságra hagyta, hogy a konkrét esetben erről volt-e szó.

Ugyanezt az ügyet megvizsgálta az EJEB is, miután az EUB-től kapott iránymutatás alapján a nemzeti bíróság úgy határozott, hogy a felügyeleti hatóság valamennyi adóügyi információ közzétételének megszüntetésére irányuló határozata a vállalatot megillető véleménynyilvánítás szabadságába való jogos beavatkozásnak minősül. Az EJEB osztotta ezt az álláspontot.[88] Megállapította, hogy bár beavatkozás történt a vállalat közléshez való jogába, a beavatkozás a törvénnyel összhangban volt, jogos célt szolgált, és szükséges volt egy demokratikus társadalomban.

A Bíróság emlékeztetett az ítélkezési gyakorlat azon kritériumaira, amelyeknek iránymutatásként kellene szolgálniuk a nemzeti hatóságok és magának az EJEB számára, amikor egymással szemben mérlegelik a véleménynyilvánítás szabadságát és a magánélet tiszteletben tartásához való jogot. Amikor egy közérdekkel bíró ügyre vonatkozó politikai beszédről vagy vitáról van szó, kevés lehetőség van az információk megismerése és közlése jogának korlátozására, „és ez egy alapvető jog egy demokratikus társadalomban".[89] Azonban a kizárólag egy adott olvasóközönség valamely személy magánéletének részleteit illető kíváncsiságát kielégíteni szándékozó újságcikkek nem tekinthetők közérdekkel bíró ügyről szóló vitának.

88 EJEB, *Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország* [Nagykamara], 931/13. sz. ügy, 2017. június 27.

89 *Uo.*, 169. pont.

Az adatvédelmi szabályoktól újságírói célból való eltérés szándéka lehetővé tenni az újságírók számára, hogy újságírói tevékenységük végzése érdekében férhessenek hozzá, gyűjthessenek és kezeljenek személyes adatokat. Így tehát valóban fennállt közérdek a felperes vállalatok általi nagy mennyiségű adózási adatok gyűjtése és kezelése, illetve az azokhoz való hozzáférés biztosítása tekintetében. Ezzel szemben a Bíróság azt állapította meg, hogy nem fűződött közérdek az ilyen nyers adatok újságokban történő tömeges, változatlan formában történő és elemzés nélküli terjesztéséhez. Az adózásra vonatkozó adatok a nyilvánosság kíváncsi tagjai számára lehetővé tehették az egyének gazdasági helyzetük alapján történő kategorizálását, továbbá kielégíthették a nyilvánosság mások magánéletére vonatkozó információk iránti vágyát. Ez nem tekinthető közérdekű vita előmozdításának.

Példa: A *Google Spain* ügyben[90] az EUB azt vizsgálta, hogy a Google köteles-e törölni a felperes pénzügyi nehézségeire vonatkozó elavult információkat a keresés találati listájából. Amikor a felperes nevével a Google keresőmotorjával keresést indítottak, a keresés találati listája a felperest csődeljárással összefüggésben megemlítő régi újságcikkekre mutató hivatkozásokat tartalmazott. A felperes ezt a magánélet tiszteletben tartásához való jog és a személyes adatok védelméhez való jog megsértésének tekintette, mivel az eljárás évekkel korábban befejeződött, így az arra való hivatkozások irrelevánsak.

Az EUB először tisztázta, hogy az internetes keresőmotorok és a személyes adatokat szolgáltató találati listák lehetővé teszik, hogy létrehozzák az érintett részletes profilját. Figyelemmel a fokozottan digitalizált társadalomra, az a követelmény, hogy a személyes adatok pontosak legyenek, és közzétételük ne haladja meg a feltétlenül szükséges mértéket, vagyis a nyilvánosság tájékoztatását, alapvető az egyének számára történő magas szintű adatvédelem biztosítása érdekében. A „keresőmotor működtetőjének – adatkezelőként – felelősségi körén, hatáskörén és lehetőségein belül biztosítania kell, hogy az általa végzett adatkezelés megfelel" az uniós jognak annak érdekében, hogy a biztosított garanciák valamennyi joghatásukat kifejthessék. Ez azt jelenti, hogy a személyes

90 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 81–83. pont.

adatok törléséhez való jog, amennyiben az adatkezelés már nem szükséges vagy idejétmúlt, nemcsak az adatfeldolgozókra, hanem a keresőmotorokra is kiterjed, amelyek adatkezelőnek minősülnek (lásd a 2.3.1 szakaszt).

Annak vizsgálata során, hogy a Google köteles-e törölni a felperesre vonatkozó hivatkozásokat, az EUB úgy vélte, hogy bizonyos feltételek mellett az egyéneknek jogukban áll kérni személyes adataik internetes keresőmotorok találati listájából való törlését. E jogra akkor lehet hivatkozni, ha az egyénre vonatkozó információk pontatlanok, nem megfelelők, irrelevánsak vagy az adatkezelés céljához mérten túlzottak. Az EUB elismerte, hogy ez a jog nem abszolút. Egyéb jogokkal, különösen a nyilvánosság információhoz való hozzáféréséhez fűződő érdekével és jogával összevetve szükséges mérlegelni. Minden törlés iránti kérelmet eseti alapon kell megvizsgálni, hogy megfelelő egyensúlyt lehessen teremteni egyrészről az érintett személyes adatok védelméhez és a magánélethez való alapjogai, másrészről pedig valamennyi internethasználó jogos érdekei között. Az EUB iránymutatást adott azon tényekre vonatkozóan, amelyeket a mérlegelés során figyelembe kell venni. A kérdéses információ természete különösen fontos tényező. Ha az információ az egyén magánélete szempontjából érzékeny, és amennyiben nem fűződik közérdek az információ rendelkezésre állásához, az adatvédelem és a magánélet megelőzi a nyilvánosság tájékoztatáshoz való jogát. Ezzel szemben azonban, ha az érintett közszereplőnek tűnik, vagy az információ jellege indokolja, hogy ahhoz a nyilvánosság hozzáférhessen, az adatvédelemhez és magánélethez való jogba való beavatkozás jogosnak minősül.

Az ítéletet követően a 29. cikk szerinti munkacsoport iránymutatást fogadott el az EUB ítéletének végrehajtására. Az iránymutatás a felügyeleti hatóságok által az egyének adattörlés iránti kérelmeihez kapcsolódó panaszainak kezelése, valamint a jogok gyakorlásának mérlegelése során alkalmazandó közös kritériumok listáját tartalmazza.[91]

Az adatvédelemhez való jognak a véleménynyilvánítás szabadságával való összeegyeztetése tekintetében az EJEB számos iránymutató ítéletet adott ki.

91 29. cikk szerinti munkacsoport (2014), *Az EUB „Google Spain and Inc kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González" C-131/12. sz. ügyben hozott ítéletének végrehajtására vonatkozó iránymutatás*, WP 225, Brüsszel, 2014. november 26.

Példa: Az *Axel Springer AG kontra Németország* ügyben[92] az EJEB megállapította, hogy a felperes vállalat számára egy ismert színész letartóztatásáról és elítéléséről szóló cikk közzétételének bírósági úton történő korlátozása sérti az EJEE 10. cikkét. Az EJEB állandó ítélkezési gyakorlatában szereplőként ismételte meg a véleménynyilvánítás szabadságához és a magánélet tiszteletben tartásához való jogok mérlegelésekor figyelembe veendő kritériumokat:

- a szóban forgó cikk általános érdeket szolgált-e;
- az érintett személy közismert volt-e;
- az információszerzés módja és megbízhatósága.

Az EJEB megállapította, hogy a színész letartóztatása és elítélése egy nyilvános bírósági tény, és ezért közérdekű volt; a színész kellően ismert volt ahhoz, hogy közszereplőnek minősüljön; az információt az ügyészség hozta nyilvánosságra, és pontosságát a felek nem vitatták. Ezért a társasággal szemben megállapított közzétételi korlátozások nem álltak megfelelően arányban a felperes magánélethez való joga védelmének törvényes céljával. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 10. cikkét.

Példa: A *Couderc és Hachette Filipacchi Associés kontra Franciaország* ügy[93] egy francia hetilapban megjelent, N. Coste-val készített interjúval foglalkozott, aki azt állította, hogy fiának apja Albert monacói herceg. Az interjú ismertette N. Coste kapcsolatát a herceggel, és azokat a körülményeket, amelyek a gyermek megszületéséhez vezettek, és mindezt a hercegről és a gyermekről készült fotók illusztrálták. Albert herceg eljárást indított a kiadó ellen a magánélet védelméhez való jogának megsértése miatt. A francia bíróságok megállapították, hogy a cikk közzététele visszafordíthatatlan kárt okozott Albert herceg számára, és elrendelte, hogy a kiadó fizessen kártérítést, és a magazin címlapján tegye közzé az ítélet részleteit.

92 EJEB, *Axel Springer AG kontra Németország* [Nagykamara], 39954/08. sz. ügy, 2012. február 7., 90. és 91. pont.

93 EJEB, *Couderc és Hachette Filipacchi Associés kontra Franciaország* [Nagykamara], 40454/07. sz. ügy, 2015. november 10.

A magazin kiadói az ügyet az EJEB elé vitték, azt állítva, hogy a francia bíróságok ítélete jogszerűtlenül sérti a véleménynyilvánítás szabadságához való jogukat. Az EJEB-nek mérlegelnie kellett Albert herceg magánélet tiszteletben tartásához való jogát, szemben a kiadó véleménynyilvánítás szabadságához való jogával, valamint a nyilvánosság tájékoztatáshoz való jogával. Fontos szempont volt továbbá N. Coste történetének nyilvánossággal való megosztásához való joga, valamint a gyermek azon érdeke, hogy hivatalosan elismerjék az apa-gyermek kapcsolatot.

Az EJEB megállapította, hogy az interjú közzététele a herceg magánéletébe való beavatkozásnak minősül, és vizsgálatát annak vizsgálatával folytatta, hogy a beavatkozás szükséges volt-e. Mérlegelte, hogy a közzététel egy közszereplőt és egy közérdekű ügyet érintett, mivel Monaco állampolgárainak érdeke fűződik ahhoz, hogy tudjanak a herceg gyermekének létezéséről, mivel a monarchia jövőbeli megöröklése „szervesen kapcsolódik a leszármazottak létezéséhez", és ezért közérdekű ügyről van szó.[94] A bíróság azt is megjegyezte, hogy a cikk lehetővé tette N. Coste és gyermeke számára, hogy gyakorolják a véleménynyilvánítás szabadságához való jogukat. A hazai bíróságok nem vették kellően figyelembe az EJEB ítélkezési gyakorlatán keresztül a magánélet tiszteletben tartásához való jog és a véleménynyilvánítás szabadságához való jog mérlegelésével kapcsolatban kialakított elveket és kritériumokat. Megállapította, hogy Franciaország megsértette az EJEE véleménynyilvánítás szabadságáról szóló 10. cikkét.

Az EJEB ítélkezési gyakorlatában a szóban forgó jogok mérlegelésével kapcsolatos egyik legfontosabb kritérium az, hogy a kérdéses közlés hozzájárul-e közérdekű vitához.

Példa: A *Mosley kontra Egyesült Királyság* ügyben[95] egy nemzeti hetilap intim fényképeket közölt a felperesről, egy ismert személyről, aki később sikeresen indított polgári pert a kiadó ellen, és kártérítést ítéltek meg számára. A megítélt anyagi kártérítés ellenére arról panaszkodott, hogy továbbra is a magánélethez való joga megsértésének áldozata, mivel megtagadták tőle annak lehetőségét, hogy a kérdéses fényképek közzététele előtt a jogsértés

94 *Uo.*, 104–116. pont.

95 EJEB, *Mosley kontra Egyesült Királyság*, 48009/08. sz. ügy, 2011. május 10., 129. és 130. pont.

megszüntetésére irányuló eljárást indítson, mivel nincs olyan jogszabályi előírás, amely az újságot arra kötelezte volna, hogy a közzétételről őt előzetesen értesítse.

Az EJEB megjegyezte, hogy bár a szóban forgó anyag terjesztése általánosságban szórakoztatási, nem pedig oktatási célt szolgált, kétségtelenül részesült az EJEE 10. cikke szerinti védelemben, ami elvezethet az EJEE 8. cikkében foglalt követelményekhez, amennyiben magán- vagy intim jellegű információkról volt szó, és a terjesztéshez nem fűződött közérdek. Különös gondossággal kellett azonban vizsgálni azokat a korlátozásokat, amelyek a közzététel előtti cenzúraként működhettek. Figyelemmel az előzetes értesítési követelmény öncenzúraként működő hatására („chilling effect"), az e követelmény hatékonyságával kapcsolatos kételyekre és az e téren fennálló széles mérlegelési mozgástérre, az EJEB arra a következtetésre jutott, hogy a 8. cikk nem ír elő jogilag kötelező előzetes értesítést. Ennek megfelelően a Bíróság arra a következtetésre jutott, hogy nem sértették meg a 8. cikket.

Példa: A *Bohlen kontra Németország* ügyben[96] a felperes, egy ismert énekes és előadó producer önéletrajzi könyvet jelentetett meg, majd később egy bírósági ítélet nyomán néhány szövegrész törlésére kötelezték. A történettel széles körben foglalkozott a nemzeti média, és egy dohányipari vállalat humoros reklámkampányt indított erre az esetre hivatkozva, a felperes keresztnevének felhasználásával, anélkül hogy hozzájárulását kérték volna ahhoz. A felperes sikertelenül próbált meg kártérítést követelni a reklámcégtől arra hivatkozva, hogy megsértették az EJEE 8. cikke szerinti jogait. Az EJEB megismételte a magánélet tiszteletben tartásához való jog és a véleménynyilvánítás szabadságához való jog közötti egyensúly megteremtésére irányadó kritériumokat, és azt állapította meg, hogy nem sértették meg a 8. cikket. A felperes közszereplő volt, és a reklám nem magánéletének részleteire hivatkozott, hanem egy olyan nyilvános eseményre, amellyel már foglalkozott a média és közérdekű vita részét képezte. Ezenkívül a reklám humoros volt, és nem tartalmazott a felperest illetően semmilyen lekicsinylő vagy negatív állítást.

96 EJEB, *Bohlen kontra Németország*, 53495/09. sz. ügy, 2015. február 19., 45–60. pont.

Példa: A *Biriuk kontra Litvánia* ügyben[97] a felperes az EJEB előtt azzal érvelt, hogy Litvánia nem teljesítette azon kötelezettségét, hogy biztosítsa a magánélet tiszteletben tartásához való jogát, mivel noha magánéletét egy újság súlyosan megsértette, az ügyet vizsgáló nemzeti bíróságok egy nevetséges összegű vagyoni kártérítést ítéltek meg számára. A nem vagyoni kártérítés megítélésekor a nemzeti bíróságok a nyilvánosság tájékoztatásáról szóló nemzeti törvény rendelkezéseit alkalmazták, amely alacsony összegben maximalizálta a személyek magánéletével kapcsolatos információk média általi törvénytelen terjesztésével okozott károk után fizetendő kártérítés összegét. Az ügy a legnagyobb litván napilap címlapsztorijából alakult ki, amelyben azt állították, hogy a felperes HIV-fertőzött. A cikk továbbá kritizálta a felperes magatartását, és megkérdőjelezte erkölcsi normáit.

Az EJEB emlékeztetett arra, hogy a személyes adatok, nem utolsósorban pedig az egészségügyi adatok védelme alapvető fontosságú az EJEE szerinti magánélet tiszteletben tartásához való jog szempontjából. Az egészségügyi adatok titkossága különösen fontos, mivel az egészségügyi adatok (a jelen esetben a felperes HIV-fertőzöttsége) drámaian befolyásolhatják az egyén magán- és családi életét, munkaviszonyát és társadalomba való beilleszkedését. A Bíróság különös jelentőséget tulajdonított annak, hogy az újságban szereplő tudósítás szerint a kórházi egészségügyi személyzet tájékoztatást nyújtott a felperes HIV-fertőzöttségéről, ami nyilvánvalóan sérti az orvosi titoktartási kötelezettséget. Ezért nem volt jogos a beavatkozás a felperes magánélethez való jogába.

A cikket a sajtó közzétette, és a véleménynyilvánítás szabadsága szintén egy EJEE szerinti alapjog. Annak vizsgálatakor azonban, hogy létezett-e a felperesre vonatkozó ilyen információ közzétételét indokoló közérdek, a Bíróság megállapította, hogy a közzététel fő indoka az újság forgalmának növelése volt az olvasói kíváncsiság kielégítésén keresztül. Az ilyen cél nem tekinthetők olyan célnak, amely valamely általános társadalmi érdekű vitához járul hozzá. Mivel ez az ügy a „sajtószabadsággal való felháborító visszaélésnek" minősül, a kártalanítási intézkedések súlyos korlátozása és a nemzeti jog által biztosított nem vagyoni kártérítés alacsony összege azt jelentette, hogy Litvánia nem tett eleget a felperes magánélethez való joga védelmére irányuló pozitív kötelezettségének. Az EJEB ezért megállapította, hogy megsértették az EJEE 8. cikkét.

97 EJEB, *Biriuk kontra Litvánia*, 23373/03. sz. ügy, 2008. november 25.

A véleménynyilvánítás szabadságához való jog és a személyes adatok védelméhez való jog nem mindig ellentétes. Vannak esetek, amikor a személyes adatok hatékony védelme garantálja a véleménynyilvánítás szabadságát.

Példa: Az EUB a *Tele2 Sverige* ügyben megállapította, hogy a 2006/24 irányelv (adatmegőrzési irányelv) által okozott beavatkozás a Charta 7. és 8. cikkében meghatározott alapjogokba „széles körű, és azt különösen súlyosnak kell tekinteni. [Az továbbá,] hogy az adatok megőrzésére és azok későbbi felhasználására anélkül kerül sor, hogy az előfizetőt vagy a nyilvántartott felhasználót erről tájékoztatnák, az érintett személyekben [...] azt az érzést keltheti, hogy magánéletük állandó felügyelet alatt áll". Az EUB azt is megállapította, hogy a forgalmi és helymeghatározó adatok általános megőrzése befolyásolhatja az elektronikus hírközlési berendezések használatát, és „ennek következtében a Charta 11. cikkében biztosított véleménynyilvánítás szabadságának ezen felhasználók általi gyakorlását".[98] Ebben az értelemben az arra vonatkozó szigorú biztosítékok előírásával, hogy az adatok megőrzése ne általánosságban történjen, az adatvédelmi szabályok végső soron hozzájárulnak a véleménynyilvánítás szabadságának gyakorlásához.

A tájékoztatáshoz való jogot illetően, amely szintén a véleménynyilvánítás szabadságának részét képezi, egyre inkább felismerik az állam átláthatóságának fontosságát a demokratikus társadalom működése szempontjából. Az átláthatóság egy közérdekű cél, amely tehát indokolhatja az adatvédelemhez való jogba való beavatkozást, amennyiben az szükséges és arányos, az 1.2 szakaszban ismertetettek szerint. Az elmúlt két évtizedben a hatóságoknál lévő okiratokhoz való hozzáférést minden uniós polgár, valamint a tagállamokban tartózkodó vagy székhellyel rendelkező bármely természetes vagy jogi személy fontos jogának ismerték el.

Az **Európa Tanács joga szerint** a hivatalos dokumentumokhoz való hozzáférésre vonatkozó ajánlásban szereplő elvekre is hivatkozni lehet, amely ajánlás a hivatalos

98 EUB, *Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016. december 21., 101. pont; EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8., 28. pont.

dokumentumokhoz való hozzáférésről szóló egyezmény (205. Egyezmény) szövegezőire is hatással volt.[99]

Az uniós jog szerint a dokumentumokhoz való hozzáférés jogát az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről szóló 1049/2001/EK rendelet (a dokumentumokhoz való hozzáférésről szóló rendelet)[100] garantálja. A Charta 42. cikke és az EUMSZ 15. cikk (3) bekezdése „az Unió intézményeinek, szerveinek és hivatalainak dokumentumai[ra]" is kiterjesztette ezt a hozzáférési jogot, „függetlenül azok megjelenési formájától".

E jog ütközhet az adatvédelmi joggal, ha egy dokumentumhoz való hozzáférés mások személyes adatait felfedné. Az általános adatvédelmi rendelet egyértelműen rendelkezik arról, hogy a közjogi hatóságok és közfeladatot ellátó szervek birtokában lévő hivatalos dokumentumokban szereplő személyes adatokat az érintett hatóság vagy szerv az Unió[101] vagy a tagállam jogával összhangban nyilvánosságra hozhatja az adatvédelemhez való jog és a hivatalos dokumentumokhoz való nyilvános hozzáférés jogának rendelet szerinti összeegyeztetése érdekében.

Ezért a hatóságok által kezelt dokumentumokhoz vagy információkhoz való hozzáférés iránti kérelmek elbírálásakor meg kell teremteni az egyensúlyt a hozzáférési jog és azon személyek adatvédelemhez való joga között, akiknek adatait a kért dokumentumok tartalmazzák.

Példa: A *Volker und Markus Schecke és Hartmut Eifert kontra Land Hessen* ügyben[102] az EUB-nak azt kellett megítélnie, hogy az uniós mezőgazdasági támogatások kedvezményezettjei nevének és az általuk kapott összegeknek – az uniós jogszabályok által előírt – közzététele arányos-e. A közzététel célja az átláthatóság fokozása és a közpénzek közigazgatás általi megfelelő felhasználásának nyilvános ellenőrzése volt. Számos kedvezményezett megtámadta e közzététel arányosságát.

99 Európa Tanács, Miniszteri Bizottság (2002), Rec(81)19. és Rec(2002)2. sz. ajánlás a tagállamoknak a hivatalos dokumentumokhoz való hozzáférésről, 2002. február 21.; Európa Tanács, Egyezmény a hivatalos dokumentumokhoz való hozzáférésről, CETS 205, 2009. június 18. Az egyezmény még nem lépett hatályba.

100 Az Európai Parlament és a Tanács 1049/2001/EK rendelete (2001. május 30.) az Európai Parlament, a Tanács és a Bizottság dokumentumaihoz való nyilvános hozzáférésről, HL L 145., 2001.5.31.

101 A Charta 42. cikke, az EUMSZ 15. cikk (3) bekezdése és az 1049/2009 rendelet.

102 EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9., 47–52., 58., 66–67., 75., 86. és 92. pont.

Az EUB – azzal a megjegyzéssel, hogy az adatvédelemhez való jog nem abszolút – úgy érvelt, hogy két uniós mezőgazdasági támogatási alap kedvezményezettjei nevének és az általuk kapott pontos összegeknek egy internetes oldalon való közzététele általánosságban beavatkozást jelent e személyek magánéletébe, konkrétan pedig sérti személyes adataik védelmét.

Az EUB megítélése szerint a Charta 7. és 8. cikkének szóban forgó megsértését jogszabály írta elő, a rendelkezés pedig az EU által elismert közérdekű célt szolgálta, azaz többek között a közösségi alapok felhasználása átláthatóságának fokozását. Az EUB mindazonáltal megállapította, hogy a szóban forgó két alapból uniós mezőgazdasági támogatásban részesült kedvezményezett természetes személyek nevének és az általuk kapott pontos összegeknek a közzététele aránytalan intézkedés volt, ami – figyelemmel a Charta 52. cikkének (1) bekezdésére – nem volt indokolt. Elismerte annak fontosságát, hogy egy demokratikus társadalomban folyamatosan tájékoztassák az adófizetőket a közpénzek felhasználásáról. Azonban kimondta, hogy „az átláthatóságra vonatkozó cél semmiképpen nem élvezhet automatikusan elsőbbséget a személyes adatok védelméhez való joggal szemben”,[103] az uniós intézmények kötelezettsége pedig az volt, hogy mérlegeljék az Unió átláthatósághoz fűződő érdekét a magánélethez és az adatvédelemhez való jogok kedvezményezettek által a közzététel eredményeképp elszenvedett korlátozásával összevetve.

Az EUB úgy vélte, hogy az uniós intézmények nem teremtettek megfelelő egyensúlyt az érintett jogok között, mivel lehetséges volt olyan intézkedéseket előirányozni, amelyek kevésbé hátrányosan érintették volna az egyének alapjogait, miközben hatékonyan hozzájárulhattak volna az átláthatóság közzététellel követett céljának eléréséhez. Például, az összes kedvezményezettet érintő általános közzététel helyett, amelyben megadták minden egyes kedvezményezett nevét és a kapott pontos összeget, különbséget lehetett volna tenni a lényeges kritériumok alapján, mint például az időszak, amelyen keresztül a szóban forgó személyek a támogatást kapták, a támogatás gyakorisága, összege és jellege.[104] Ezért

103 *Uo.*, 85. pont.

104 *Uo.*, 89. pont.

az EUB az európai mezőgazdasági alapok kedvezményezettjeire vonatkozó információk nyilvánosságra hozataláról szóló uniós jogszabályt részlegesen érvénytelennek nyilvánította.

Példa: A *Rechnungshof kontra Österreichischer Rundfunk és társai* ügyben[105] az EUB egyes osztrák jogszabályoknak az uniós adatvédelmi joggal való összeegyeztethetőségét vizsgálta. A jogszabály előírta egy állam szerv számára, hogy gyűjtsön és továbbítson jövedelemre vonatkozó adatokat abból a célból, hogy különféle állami szervezetek munkavállalóinak nevét és jövedelmi adatait közzétegyék a nyilvánosság számára hozzáférhető éves jelentésben. Néhány egyén adatvédelemre hivatkozva megtagadta adatainak közlését.

Véleményében az EUB az alapjogok védelmére mint az uniós jog alapelvére, valamint az EJEE 8. cikkére hagyatkozott, emlékeztetve arra, hogy a Charta akkor még nem volt kötelező erejű. Megállapította, hogy az egyének jövedelmére vonatkozó adatok gyűjtése, és különösen azok közlése harmadik felek számára a magánélet tiszteletben tartásához fűződő jog hatálya alá tartozik, és e jog megsértésének minősül. A beavatkozás jogszerű lehetne, ha az a jogszabályokkal összhangban lenne, törvényes cél előmozdítását szolgálná és e cél elérése szükséges lenne egy demokratikus társadalomban. Az EUB megjegyezte, hogy az osztrák jogszabályok törvényes célt szolgáltak, mivel céljuk az volt, hogy az állami alkalmazottak jövedelmét észszerű határok között tartsák, ami egyben az ország gazdasági jólétéhez kapcsolódó szempont is. Ugyanakkor Ausztriának a közpénzek legjobb felhasználásának biztosításához fűződő érdekét az érintett személyek magánélet tiszteletben tartásához való jogába történő beavatkozás súlyosságával összevetve kellett mérlegelnie.

Miközben a nemzeti bíróságokra hagyta annak megállapítását, hogy az egyének jövedelmi adatainak közzététele szükséges és arányos volt-e a jogszabály által követett célhoz mérten, az EUB felhívta a nemzeti bíróságokat annak megvizsgálására, hogy egy ilyen célt nem lehetett-e volna kevésbé beavatkozó jellegű eszközök révén azonos hatékonysággal elérni. Ilyen lehet például a személyes adatok továbbítása kizárólag az állami ellenőrző szervek, nem pedig a nyilvánosság felé.

105 EUB, *Rechnungshof kontra Österreichischer Rundfunk és társai,* valamint *Christa Neukomm és Joseph Lauermann kontra Österreichischer Rundfunk*, C-465/00., C-138/01. és C-139/01. sz. egyesített ügyek, 2003. május 20.

A későbbi ügyekben nyilvánvalóvá vált, hogy az adatvédelem és a dokumentumokhoz való hozzáférés egymással szembeni mérlegeléséhez részletes, eseti elemzés szükséges. Egyik jog sem előzheti meg automatikusan a másikat. Az EUB-nek lehetősége volt két ügyben is értelmezni a személyes adatokat tartalmazó dokumentumokhoz való hozzáférés jogát.

Példa: Az *Európai Bizottság kontra Bavarian Lager* ügyben[106] az EUB az uniós intézmények dokumentumaihoz való hozzáféréssel összefüggésben meghatározta a személyes adatok védelmének terjedelmét, továbbá az 1049/2001/EK rendelet (dokumentumokhoz való hozzáférésről szóló rendelet) és a 45/2001/EK rendelet (uniós intézmények adatvédelmi rendelete) közötti viszonyt. Az 1992-ben alapított Bavarian Lager üveges német sört importál az Egyesült Királyságba, elsősorban vendéglőkbe és bárokba. A cég azonban nehézségekkel találta szemben magát, mert a brit jogszabályok *ténylegesen* előnyben részesítették a nemzeti termelőket. A Bavarian Lager panaszára válaszul az Európai Bizottság eljárást indított az Egyesült Királyság ellen kötelezettségszegés miatt, aminek eredményeként az Egyesült Királyság módosította és az uniós joghoz igazította a vitatott rendelkezéseket. Ezt követően a Bavarian Lager – más dokumentumok mellett – a Bizottság, a brit hatóságok és a *Confédération des Brasseurs du Marché Commun* (CBMC) képviselői részvételével tartott ülés jegyzőkönyvének másolatát kérte a Bizottságtól. A Bizottság beleegyezett az üléssel kapcsolatos egyes dokumentumok közzétételébe, de a jegyzőkönyvben szereplő öt nevet kitakarta – ketten közülük kifejezetten tiltakoztak személyazonosságuk felfedése ellen, három másik személyt pedig a Bizottság nem tudott elérni. A Bizottság 2004. március 18-i döntésével elutasította a Bavarian Lager újabb, az ülés teljes jegyzőkönyvének kiadására vonatkozó kérelmét, konkrét hivatkozással a szóban forgó személyeknek az uniós intézmények adatvédelmi rendeletében biztosított, a magánélet védelméhez való jogára.

Mivel nem volt elégedett ezzel az állásponttal, a Bavarian Lager az ügyet az elsőfokú bíróság elé vitte. Ez a bíróság hatályon kívül helyezte a 2007. november 8-i bizottsági határozatot (*The Bavarian Lager Co. Ltd kontra az Európai Közösségek Bizottsága*, T-194/04. sz. ügy), megállapítva azt, hogy

106 EUB, *Európai Bizottság kontra The Bavarian Lager Co. Ltd.* [nagytanács], C-28/08. P. sz. ügy, 2010. június 29.

az ülésen az általuk képviselt szerv nevében részt vevők listáján szereplő kérdéses személyek nevének puszta megadása nem sérti a magánéletet és semmilyen módon nem veszélyezteti az illetők magánéletét.

A Bizottság fellebbezése nyomán az EUB hatályon kívül helyezte az elsőfokú ítéletet. Az EUB megállapította, hogy a dokumentumokhoz való hozzáférésről szóló rendelet „egyedi és megerősített védelmi rendszert hoz létre azon személyek vonatkozásában, akiknek a személyes adatai adott esetben nyilvánosan hozzáférhetővé tehetők". Az EUB szerint, amennyiben a dokumentumokhoz való hozzáférésről szóló rendeleten alapuló kérelem célja személyes adatokat tartalmazó dokumentumokhoz való hozzáférés, az uniós intézmények adatvédelmi rendeletének rendelkezései teljes mértékben alkalmazandóvá válnak. Az EUB ezt követően arra a következtetésre jutott, hogy a Bizottság helyesen utasította el az 1996. októberi ülés teljes jegyzőkönyvéhez való hozzáférés iránti kérelmet. Az ülésen részt vevő öt személy hozzájárulásának hiányában a Bizottság kellően eleget tett a nyíltságra vonatkozó kötelezettségének azáltal, hogy a dokumentum szóban forgó változatában áthúzta az öt nevet.

Ezenfelül az EUB szerint „[m]ivel a Bavarian Lager nem terjesztett elő semmilyen kifejezett és törvényes célt, illetve meggyőző érvet e személyes adatok továbbításának szükségességét alátámasztandó, a Bizottság nem tudta az érintett felek különböző érdekeit mérlegelni. Nem tudta azt ellenőrizni, hogy nincs semmilyen ok annak feltételezésére, hogy e továbbítás sértené az érintettek jogos érdekeit", amint azt az uniós intézmények adatvédelmi rendelete előírja.

Példa: A *Client Earth, PAN Europe kontra EFSA* ügyben[107] az EUB azt vizsgálta meg, hogy az Európai Élelmiszerbiztonsági Hatóságnak (EFSA) a felperesek dokumentumokhoz való teljes hozzáférésének elutasítására irányuló határozata szükséges volt-e azon személyek magánélethez és adatvédelemhez való jogainak védelme érdekében, akikre a dokumentumok hivatkoztak. Az érintett dokumentumok az EFSA egyik munkacsoportja által külső szakértőkkel közreműködve készített, növényvédő szerek piaci forgalomba hozatalára vonatkozó iránymutatásokat tartalmazó jelentéstervezetet érintettek. Az EFSA először részleges

107 EUB, *ClientEarth, Pesticide Action Network Europe (PAN Europe) kontra Európai Élelmiszerbiztonsági Hatóság (EFSA), Európai Bizottság*, C-615/13. P. sz. ügy, 2015. július 16.

hozzáférést biztosított a felperesek számára, megtagadva a hozzáférést az iránymutatásokat tartalmazó jelentéstervezet néhány munkaverziójához. Később hozzáférést biztosított azon tervezethez, amely tartalmazta a külső szakértők egyéni észrevételeit. A szakértők nevét azonban, hivatkozva a személyes adatok uniós intézmények és szervek által történő feldolgozásáról szóló 45/2001 rendelet 4. cikke (1) bekezdésének b) pontjára, valamint a külső szakértők magánélete védelmének szükségességére, kitakarta. Első fokon az Európai Unió Törvényszéke fenntartotta az EFSA határozatát.

A felperesek fellebbezése nyomán az EUB hatályon kívül helyezte az elsőfokú ítéletet. Arra a következtetésre jutott, hogy a szóban forgó esetben a személyes adatok átadása szükséges volt annak megállapítására, hogy az egyes külső szakértők feladataik teljesítése során tudósként elfogulatlanok voltak, valamint annak biztosítására, hogy az Európai Élelmiszerbiztonsági Hatóság döntéshozatali folyamata átlátható maradjon. Az EUB véleménye szerint az Európai Élelmiszerbiztonsági Hatóság nem részletezte, hogy az iránymutatásokat tartalmazó jelentéstervezethez konkrét megjegyzéseket fűző külső szakértők nevének felfedése miként sérti a szakértők jogos érdekeit. Az az általános érvelés, hogy a nyilvánosságra hozatal sértheti a magánéletet, nem elégséges, amennyiben azt nem támasztják alá az egyes esetekre vonatkozó konkrét bizonyítékok.

Ezen ítéletek szerint a dokumentumokhoz való hozzáférés vonatkozásában az adatvédelmi jogba való beavatkozáshoz konkrét és alapos indok szükséges. A dokumentumokhoz való hozzáférés joga nem írhatja automatikusan felül az adatvédelemhez való jogot.[108]

Ez a megközelítés hasonló az EJEB megközelítéséhez a magánélet és a dokumentumokhoz való hozzáférés vonatkozásában, ahogy azt a következő ítélet is igazolja. A *Magyar Helsinki Bizottság* ítéletben az EJEB leszögezte, hogy a 10. cikk nem ruházza fel az egyént egy hatóság birtokában lévő információhoz való hozzáférés jogával vagy kötelezi a kormányt az ilyen információ egyénnel való közlésére. Egy ilyen jog vagy kötelezettség azonban felmerülhet: először is akkor, ha az információ felfedését jogerőre emelkedett bírósági végzés írja elő, másodszor, ha

108 Lásd azonban az EDPS *Nyilvános hozzáférés személyes adatokat tartalmazó dokumentumokhoz a* Bavarian Lager ügyben *hozott ítélet után* című, 2011-es tanulmányában (Brüsszel, 2011. március 24.) található részletes megfontolásokat.

az információhoz való hozzáférés a véleménynyilvánítási jog – különösen az információk megismeréséhez és közléséhez való jog – gyakorlásának az eszköze, és megtagadása a szóban forgó jogba való beavatkozásnak minősül.[109] Azt, hogy az információhoz való hozzáférés megtagadása beavatkozásnak minősül-e a felperes véleménynyilvánítási jogába, és ha igen, milyen mértékben, minden egyes esetben külön-külön, a konkrét körülményekre figyelemmel kell értékelni, beleértve a következőket: (i) az információkérés célja; (ii) a kért információ jellege; (iii) a felperes szerepe; és (iv) azt, hogy az információk azonnal elérhetők voltak-e.

Példa: A *Magyar Helsinki Bizottság kontra Magyarország* ügyben[110] a felperes, egy emberi jogi civil szervezet információt kért a rendőrségtől a hivatalból kirendelt védők munkájára vonatkozóan egy, a magyarországi kirendelt védői rendszer működéséről készített tanulmányhoz. A rendőrség megtagadta az információk kiadását, azzal érvelve, hogy azok nyilvánosságra nem hozható személyes adatokat tartalmaznak. A fenti kritériumokat alkalmazva az EJEB megállapította, hogy megvalósult a beavatkozás egy, a 10. cikkben védett jogba. Pontosabban a felperes gyakorolni szerette volna arra vonatkozó jogát, hogy jogos közérdek tárgyát képező ügyben tájékoztatást adjon, és ebből a célból kért hozzáférést az információkhoz, és az információ szükséges volt a felperes véleménynyilvánítás szabadságához való jogának gyakorlásához. A kirendelt védők kinevezésére vonatkozó információ közérdekű adat volt. Nem volt ok annak kétségbe vonására, hogy a szóban forgó felmérés olyan típusú információt tartalmaz, amelynek a nagyközönséggel való közlését a felperes civil szervezet vállalta, és amelynek megismeréséhez a nagyközönségnek joga is van. A Bíróság ezért meggyőződött arról, hogy a felperesnek szüksége volt a kért információkhoz való hozzáférésre a feladat teljesítéséhez. Végezetül pedig az információk készen voltak, rendelkezésre álltak.

Az EJEB megállapította, hogy a kért információkhoz való hozzáférés megtagadása ebben az esetben csorbította az információk megismeréséhez és közléséhez való jog lényegét. E következtetés levonásához a bíróság megvizsgálta különösen a kért információk célját és azt, hogy az milyen

109 EJEB, *Magyar Helsinki Bizottság kontra Magyarország* [Nagykamara], 18030/11. sz. ügy, 2016. november 8., 148. pont.

110 *Uo.*, 181., 187–200. pont.

mértékben járul hozzá egy fontos nyilvános vitához, a kért információ természetét, és hogy az közérdekű-e, valamint a felperes társadalomban betöltött szerepét.

Indokolásában a Bíróság megjegyezte, hogy a civil szervezet által készített tanulmány az igazságszolgáltatás működését és a tisztességes eljáráshoz való jogot érintette, amely az EJEE értelmében kiemelkedő fontosságú jog. Mivel a kért információ nem érintett nyilvánosan nem hozzáférhető adatokat, az érintettek (hivatalból kirendelt védők) magánélethez való jogai nem sérültek volna, ha a rendőrség a felperes számára hozzáférést biztosított volna az információkhoz. A felperes által kért információ statisztikai jellegű adatokból állt arra vonatkozóan, hogy a hivatalból kirendelt védők hány alkalommal kaptak megbízást vádlottak nyilvános büntetőeljárásban történő képviseletére.

A Bíróság szerint figyelemmel arra, hogy a tanulmány célja az volt, hogy hozzájáruljon egy nyilvánvalóan közérdekű kérdésről folytatott vitához, a civil szervezet tervezett publikációjára vonatkozó bármilyen korlátozást a lehető legalaposabban kell kivizsgálni. A szóban forgó információ közérdekű volt, mivel a közérdek olyan kérdésekre vonatkozik, „amelyek adott esetben súlyosan ellentmondásosak lehetnek, amelyek fontos társadalmi kérdést érintenek, vagy olyan problémával függnek össze, amelyről a nagyközönségnek tudnia kell”.[111] Ezért tehát természetesen beletartozik az igazságszolgáltatás működéséről és a tisztességes eljárásokról folytatott vita is, amely a felperes tanulmányának tárgyát képezte. A különböző jogok mérlegelésével és az arányosság elvének alkalmazásával az EJEB megállapította, hogy megvalósult a felperes EJEE 10. cikke szerinti jogának indokolatlan megsértése.

1.3.2 Szakmai titoktartás

A nemzeti jog értelmében egyes információk szakmai titoktartás hatálya alá tartozhatnak. A szakmai titoktartás érthető speciális etikai kötelezettségnek, amely egyes őszinteségen és bizalmon alapuló szakmákhoz és funkciókhoz kapcsolódó jogszabályi kötelezettséget von maga után. E funkciókat betöltő személyek és intézmények kötelesek megőrizni a feladatuk ellátása során kapott bizalmas információkat.

111 *Uo.*, 156. pont.

A szakmai titoktartás elsősorban az egészségügyi és az ügyvédi szakmában érvényes. Számos joghatóság elismeri a pénzügyi ágazat szakmai titoktartási kötelezettségét is. A szakmai titoktartás nem alapjog, azonban a magánélet tiszteletben tartásához való jog formájában védelmet élvez. Az EUB például egyes esetekben úgy ítélkezett, hogy „szükséges lehet bizonyos, bizalmasnak minősülő információknak a nyilvánosságra hozatalát megtagadni valamely vállalkozásnak az EJEE 8. cikkében és a Charta 7. cikkében rögzített magánélethez való alapvető jogának védelme érdekében".[112] Az EJEB-et is kérték már fel arra, hogy hozzon ítéletet arra vonatkozóan, hogy a szakmai titoktartás korlátozásával megvalósul-e az EJEE 8. cikkének megsértése a kiemelt példákban bemutatottak szerint.

Példa: A *Pruteanu kontra Románia* ügyben[113] a felperes egy kereskedelmi vállalat ügyvédjeként járt el, amelyet csalás gyanúja miatt eltiltottak banki tranzakciók végzésétől. Az ügy kivizsgálása során a román bíróságok engedélyt adtak az ügyészségnek, hogy hallgassák le és rögzítsék a vállalat partnerével egy meghatározott időszak alatt folytatott telefonbeszélgetéseket. A hívások rögzítése és a lehallgatás kiterjedt az ügyvédjével folytatott kommunikációkra is.

Pruteanu azt állította, hogy ez sértette a magánélet tiszteletben tartásához és a kapcsolattartáshoz való jogát. Ítéletében az EJEB kiemelte az ügyvéd és ügyfele közötti kapcsolat státuszát és jelentőségét. Egy ügyvéd ügyfelével folytatott beszélgetéseinek lehallgatása kétségtelenül sértette a szakmai titoktartást, amely e két személy közötti kapcsolat alapját képezte. Ilyen esetben az ügyvéd is élhet panasszal a magánélet tiszteletben tartásához és a kapcsolattartáshoz való jogának megsértése miatt. Az EUB megállapította, hogy megsértették az EJEE 8. cikkét.

Példa: A *Brito Ferrinho Bexiga Villa-Nova kontra Portugália* ügyben[114] a felperes, egy ügyvéd, szakmai titoktartásra és banktitokra hivatkozva megtagadta magán banki kivonatainak adóhatóság számára történő átadását. Az ügyészség adócsalás miatt indított nyomozást, és kérte

112 EUB, *Pilkington Group Ltd kontra Európai Bizottság*, T-462/12. R. sz. ügy, a Törvényszék elnökének végzése, 2013. március 11., 44. pont.

113 EJEB, *Pruteanu kontra Románia*, 30181/05. sz. ügy, 2015. február 3.

114 EJEB, *Brito Ferrinho Bexiga Villa-Nova kontra Portugália*, 69436/10. sz. ügy, 2015. december 1.

a szakmai titoktartás felfüggesztését. A nemzeti hatóságok elrendelték a titoktartás és banktitok alóli felmentést, mert úgy ítélték meg, hogy a közérdek a felperes magánérdekei felett áll.

Amikor az ügy az EJEB elé került, a Bíróság megállapította, hogy a felperes banki kivonataihoz való hozzáféréssel megvalósul a beavatkozás a magánélet körébe tartozó szakmai titoktartás tiszteletben tartásához való jogába. A beavatkozásnak volt jogalapja, ugyanis az a büntető törvénykönyvön alapult, továbbá törvényes célt szolgált. A beavatkozás szükségessége és arányossága vizsgálatakor azonban az EJEB rámutatott arra, hogy a titoktartás felfüggesztésére irányuló eljárást a felperes részvétele vagy tudomása nélkül indították. A felperes ezért nem tudta benyújtani az érveit. Ezenkívül, bár a hazai jog rendelkezik arról, hogy ilyen eljárásban konzultálni kell az ügyvédek szakmai szervezetével, a szervezettel nem konzultáltak. Végezetül pedig a felperes számára nem volt lehetőség arra, hogy ténylegesen megtámadja a titoktartás felfüggesztését, sem pedig hogy jogorvoslati lehetőséggel éljen az intézkedés megtámadására. Az eljárási garanciák és a titoktartási kötelezettséget felfüggesztő intézkedés feletti hatékony bírói ellenőrzés hiánya miatt az EJEB arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

A szakmai titoktartás és az adatvédelem közötti kapcsolat gyakran ambivalens. Egyrészről a jogszabályban megállapított adatvédelmi szabályok és biztosítékok segítenek biztosítani a szakmai titoktartást. Azon szabályok célja például, amelyek előírják az adatkezelők és adatfeldolgozók számára, hogy hajtsanak végre robusztus adatbiztonsági intézkedéseket, többek között az, hogy megelőzzék a szakmai titoktartással védett személyes adatok bizalmas jellegének sérülését. Ezenkívül az EU általános adatvédelmi rendelete lehetővé teszi az egészségügyi adatok kezelését, amelyek kiemelt védelmet élvező személyes adatok speciális kategóriáját alkotják, de azt az érintettek jogait védő megfelelő és konkrét intézkedések, nevezetesen szakmai titoktartás meglététől teszi függővé.[115]

Másrészről az adatkezelők és adatfeldolgozók szakmai titoktartásra vonatkozó kötelezettsége egyes személyes adatok tekintetében korlátozhatja az érintett jogait, nevezetesen a tájékoztatáshoz való jogot. Annak ellenére, hogy az általános adatvédelmi rendelet tartalmazza azon információk kimerítő listáját, amelyeket elvben

115 Általános adatvédelmi rendelet, 9. cikk (2) bekezdés h) pont és 9. cikk (3) bekezdés.

biztosítani kell az érintett számára, ha a személyes adatokat nem az érintettől szerezték meg, ez a követelmény nem vonatkozik azokra az esetekre, amikor a személyes adatoknak bizalmasnak kell maradniuk valamely nemzeti vagy uniós jogban előírt szakmai titoktartási kötelezettség alapján.[116]

Az általános adatvédelmi rendelet lehetőséget biztosít a tagállamok számára, hogy jogszabályban különös rendelkezéseket hozhatnak annak érdekében, hogy a szakmai vagy más, azzal egyenértékű titoktartási kötelezettségeket biztosítsák, ha a személyes adatok védelméhez való jogot a szakmai titoktartásra vonatkozó kötelezettséggel kell összeegyeztetni.[117]

Az általános adatvédelmi rendelet rendelkezik arról, hogy a tagállamok egyedi szabályokat fogadhatnak el a felügyeleti hatóságok hatáskörét illetően olyan adatkezelőkre vagy adatfeldolgozókra vonatkozóan, amelyek szakmai titoktartási kötelezettség hatálya alá tartoznak. Ezek az egyedi szabályok az adatkezelő vagy az adatfeldolgozó helyiségeihez, az adatkezeléshez használt felszereléséhez és a birtokolt személyes adatokhoz való hozzáférésre vonatkoznak, amennyiben az ilyen személyes adatokat az adatkezelő vagy az adatfeldolgozó a titoktartási kötelezettség hatálya alá tartozó tevékenység során kapott vagy szerzett. Az adatvédelemmel megbízott felügyeleti hatóságoknak tehát tiszteletben kell tartaniuk az adatkezelőket és adatfeldolgozókat kötő szakmai titoktartási kötelezettséget. Ráadásul a felügyeleti hatóságok tagjai maguk is szakmai titoktartási kötelezettség alá tartoznak hivatali időszakuk alatt és után. Feladatuk ellátása során a felügyeleti hatóságok tagjai és munkatársai bizalmas információkhoz juthatnak hozzá. A rendelet 54. cikkének (2) bekezdése egyértelműen kimondja, hogy az ilyen bizalmas információk tekintetében szakmai titoktartási kötelezettségük van.

Az általános adatvédelmi rendelet előírja a tagállamok számára, hogy tájékoztassák a Bizottságot azokról a szabályokról, amelyet az adatvédelem és a rendeletben a szakmai titoktartási kötelezettséggel kapcsolatban megállapított elvek összeegyeztetése érdekében fogadnak el.

1.3.3 A vallás és a meggyőződés szabadsága

A vallás és a meggyőződés szabadságát az EJEE 9. cikke (gondolat-, lelkiismeret- és vallásszabadság) és az EU Alapjogi Chartájának 10. cikke védelemben részesíti.

116 *Uo.*, 14. cikk (5) bekezdés d) pont.

117 *Uo.*, (164) preambulumbekezdés és 90. cikk.

A vallási vagy filozófiai meggyőződést felfedő személyes adatok „különleges adatoknak" minősülnek az uniós és az Európa Tanács joga alapján egyaránt, és kezelésük, valamint felhasználásuk fokozott védelem alá tartozik.

Példa: A felperes a *Sinak Isik kontra Törökország* ügyben[118] az alevi vallási közösség tagja volt, amelynek hitére hatással volt a szúfizmus és egyéb iszlám előtti meggyőződés, és egyes tudósok szerint külön vallásnak minősül, míg mások szerint az iszlám vallás részét képezi. Az felperes sérelmezte, hogy személyi igazolványa tartalmazott egy a vallását jelző megjegyzést, ahol kérése ellenére az „alevi" helyett „iszlám" szerepelt. A hazai bíróságok arra irányuló kérését, hogy személyi igazolványán a vallását „alevire" módosítsák, elutasították arra hivatkozva, hogy ez a szó az iszlám egyik alcsoportját jelöli, nem pedig egy külön vallást. Ezt követően az EJEB-nél sérelmezte, hogy hozzájárulása nélkül kötelezték hitének nyilvánosságra hozatalára, mivel a személyi igazolványon kötelező volt feltüntetni a vallást, és ez a vallás és meggyőződés szabadságához való joga megsértésének minősül. Figyelemmel különösen arra, hogy személyi igazolványán helytelenül szerepelt az „iszlám" megnevezés.

Az EJEB ismételten rámutatott arra, hogy a vallásszabadság magában foglalja az egyén vallásának szabad megnyilvánulását közösségben, nyilvánosan vagy azonos hitet valló emberek körében, de akár egyénileg, egyedül is. Az akkoriban hatályos hazai szabályozás kötelezte az egyéneket, hogy vallásukat tartalmazó személyi igazolványt tartsanak maguknál, amit bármely hatóság vagy magánvállalkozás kérésére be kell mutatni. Az ilyen kötelezettség nem ismeri el, hogy a vallás szabad megnyilvánulásához való jog fordított jogot is biztosít, vagyis, hogy az egyén ne legyen köteles hitének nyilvánosságra hozatalára. A kormány arra vonatkozó érvelése ellenére, hogy a nemzeti szabályozást úgy módosították, hogy az egyének kérhessék a személyi igazolványukon a vallás helyének üresen hagyását, a Bíróság álláspontja szerint annak puszta tényével, hogy kérelmezni kell a vallás törlését, megvalósul a vallásra vonatkozó attitűd közlése. Ezenkívül, ha a személyi igazolványon szerepel egy hely a vallás megadására, ennek üresen hagyása különös jelentőséggel bír, mivel a vallási információkat nem tartalmazó személyi igazolvány birtokosa kilóg azon egyének sorából, akik

118 EJEB, *Sinan Işık kontra Törökország*, 21924/05. sz. ügy, 2010. február 2.

vallási meggyőződésüket tartalmazó igazolvánnyal rendelkeznek. Az EJEB arra a következtetésre jutott, hogy a hazai szabályozás megsértette az EJEE 9. cikkét.

Az egyázak és vallási szervezetek vagy közösségek működéséhez szükséges tagjaik személyes adatainak kezelése, hogy lehetővé tegyék a gyülekezeten belüli kommunikációt, illetve tevékenységek szervezését. Az egyházak és vallási szervezetek tehát gyakran bevezettek személyes adatok kezelésére vonatkozó szabályokat. Az általános adatvédelmi rendelet 91. cikke értelmében amennyiben az ilyen szabályok átfogók, azok tovább alkalmazhatók, ha összhangba hozzák őket a rendelettel. Az ilyen szabályokat alkalmazó egyház vagy vallási szervezet egy független felügyeleti hatóság ellenőrzése alá kell, hogy tartozzon, amely lehet egy külön, e célra egyedileg kijelölt hatóság is, feltéve hogy megfelel az általános adatvédelmi rendeletben megállapított feltételeknek.[119]

A vallási szervezetek számos okból végezhetnek személyesadat-kezelést, például a gyülekezettel való kapcsolattartás vagy események, vallási vagy jótékonysági rendezvények szervezésére vonatkozó tájékoztatás érdekében. Egyes államokban az egyházaknak adóügyi okokból tagjaikról nyilvántartást kell vezetniük, mivel a vallási létesítményekben való tagság befolyásolja az egyén által fizetendő adó mértékét. Az európai jog alapján a vallási meggyőződésre vonatkozó adatok minden esetben különleges adatnak minősülnek, és az egyházaknak elszámoltathatónak kell lenniük az ilyen adatok kezelése és feldolgozása tekintetében különösen azért, mert a vallási szervezetek által kezelt adatok gyakran gyermekeket, időseket vagy a társadalom egyéb sérülékeny tagjait érintik.

1.3.4 A művészet és a tudomány szabadsága

Egy másik jog, amelynek esetében meg kell teremteni az egyensúlyt a magánélet tiszteletben tartásához és az adatvédelemhez való joggal szemben, a művészet és a tudomány szabadsága, amelyet az EU Alapjogi Chartájának 13. cikke kifejezetten védelemben részesít. E jog elsősorban a gondolatszabadságból, valamint a véleménynyilvánítás szabadságából származik, és a Charta 1. cikkének (az emberi méltóság) tiszteletben tartása mellett kell gyakorolni. Az EJEB úgy véli, a művészet szabadságát az EJEE 10. cikke védelemben részesíti.[120] A Charta 13. cikkében garantált

119 Általános adatvédelmi rendelet, 91. cikk (2) bekezdés.

120 EJEB, *Müller és társai kontra Svájc*, 10737/84. sz. ügy, 1988. május 24.

jog korlátozható a Charta 52. cikkének (1) bekezdésével összhangban, ami szintén értelmezhető az EJEE 10. cikke (2) bekezdésén keresztül.[121]

Példa: A *Vereinigung bildender Künstler kontra Ausztria* ügyben[122] az osztrák bíróságok eltiltották a felperes szervezetet egy festmény további kiállításától, amely szexuális helyzetben ábrázol alakokat, akiknek az arcát különböző közszereplőkről készült fotókkal helyettesítették. Egy osztrák parlamenti képviselő, akinek a fényképét felhasználták a festményen, eljárást indított a felperes szervezet ellen, és a festmény kiállítását megtiltó végzés kiadását kérte. A hazai bíróság kiadta ezt a végzést. Az EJEB ismételten rámutatott, hogy az EJEE 10. cikke olyan gondolatok közlésére is alkalmazható, amelyek az államot vagy a lakosság bármely csoportját sértik, megbotránkoztatják vagy zavarják. Az alkotást létrehozó, előadó, terjesztő vagy kiállító személyek hozzájárulnak a gondolatok és vélemények cseréjéhez, és az államot az a kötelesség terheli, hogy indokolatlanul ne csorbítsa a véleménynyilvánítás szabadságát. Figyelemmel arra, hogy a festmény kollázs volt, amely a személyeknek csupán a portréját ábrázoló fényképeket használt fel, a testeket pedig irreális, túlzó módon festették meg, amely nyilván nem a valóságra utalt, illetve nyilván nem azt kívánta sugallni, az EJEB azt is megállapította, hogy „a festmény aligha értelmezhető úgy, hogy a megfestett személyek magánéletének részleteivel foglalkozik, inkább nyilvános politikusi szerepükre utal", és „[az ábrázolt személynek] e minőségében nagyobb türelmet kell tanúsítania a kritikával szemben". A szóban forgó különböző érdekeket mérlegelve az EJEB megállapította, hogy a festmény további kiállításának korlátlan betiltása aránytalan. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 10. cikkét.

Az európai adatvédelmi jog elismeri továbbá a tudomány társadalom számára nyújtott speciális értékét. Az általános adatvédelmi rendelet és a Korszerűsített 108. Egyezmény megengedi az adatok hosszabb távon történő megőrzését, amennyiben a személyes adatok kezelése kizárólag tudományos vagy történelmi kutatások céljából történik. Továbbá egy konkrét adatkezelési tevékenység eredeti céljától függetlenül a személyes adatok későbbi felhasználása tudományos és történelmi

121 Magyarázatok az Alapjogi Chartához, HL C 303., 2007.12.14.

122 EJEB, *Vereinigung bildender Künstler kontra Ausztria*, 68354/01. sz. ügy, 2007. január 25., 26. és 34. pont.

kutatási célból nem minősül az eredeti céllal össze nem egyeztethetőnek.[123] Ugyanakkor az érintettek jogainak és szabadságainak védelme érdekében megfelelő garanciákat kell alkalmazni az ilyen adatkezelésre. Az uniós vagy a tagállami jog biztosíthat eltéréseket az érintettek jogaira vonatkozóan, például az adatokhoz való hozzáférést, az adatok helyesbítését, az adatkezelés korlátozását és kifogásolását illetően, amennyiben a személyes adatok tudományos kutatás, történelmi vagy statisztikai célú kezeléséről van szó (lásd még a 6.1 és 9.4 szakaszt is).

1.3.5 A szellemi tulajdon védelme

A tulajdon védelméhez fűződő jogot az EJEE első kiegészítő jegyzőkönyvének 1. cikke, valamint az EU Alapjogi Chartája 17. cikkének (1) bekezdése is tartalmazza. A tulajdon védelméhez fűződő jog egyik fontos, az adatvédelem szempontjából különösen releváns vonatkozása a szellemi tulajdon védelme, amelyet a Charta 17. cikkének (2) bekezdése kifejezetten megemlít. Az Unió jogrendjében számos irányelv igyekszik hatékony védelemben részesíteni a szellemi tulajdont, különösen a szerzői jogot. A szellemi tulajdon körébe nemcsak az irodalmi és művészeti tulajdon, hanem a szabadalom, a védjegy és a szomszédos jogok is beletartoznak.

Ahogyan az EUB ítélkezési gyakorlata már világossá tette, egyensúlyt kell teremteni különösen a tulajdonhoz való alapvető jog védelme és az adatvédelemhez való jog között.[124] Voltak olyan ügyek, amelyekben szerzői jogvédő szervezetek azt követelték, hogy internetszolgáltatók fedjék fel az internetes fájlmegosztó platformok felhasználóinak személyazonosságát. Az ilyen platformok gyakran lehetővé teszik, hogy internethasználók zenei fájlokat töltsenek le ingyenesen annak ellenére, hogy ezek a címek szerzői jogilag védettek.

> Példa: A *Promusicae kontra Telefónica de España* ügy[125] tárgya az volt, hogy a Telefónica spanyol internetszolgáltató megtagadta, hogy kiadja a zenei producereket, valamint zenei és audiovizuális felvételek kiadóit tömörítő, Promusicae nonprofit szervezetnek bizonyos személyek személyes adatait, akik számára internet-hozzáférést biztosított. A Promusicae azért kérte az információk átadását, hogy polgári jogi eljárást indíthasson a szóban forgó

123 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés b) pont és Korszerűsített 108. Egyezmény 5. cikk (4) bekezdés b) pont.

124 EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008. január 29., 62–68. pont.

125 *Uo.*, 54. és 60. pont.

személyek ellen, akik állítása szerint fájlcsereprogramot használtak, amely olyan hangfelvételekhez biztosít hozzáférést, amelyek hasznosítási jogai a Promusicae-tagokat illetik.

A spanyol bíróság az EUB elé utalta az ügyet, azt a kérdést felvetve, hogy a hatékony szerzői jogi védelem biztosítása érdekében a szóban forgó személyes adatokat a közösségi jog szerint – a polgári jogi eljárással összefüggésben – közölni kell-e. Hivatkozott a 2000/31/EK, a 2001/29/EK és a 2004/48/EK irányelvre – a Charta 17. és 47. cikkének figyelembevételével is értelmezve őket. Az EUB arra a következtetésre jutott, hogy e három irányelv – az elektronikus hírközlési adatvédelmi irányelvvel (2002/58/EK irányelv) kiegészítve – nem zárja ki, hogy a tagállamok polgári jogi eljárással összefüggésben – a hatékony szerzői jogi védelem biztosítása céljából – személyes adatok közlésére vonatkozó kötelezettséget írjanak elő.

Az EUB rámutatott, hogy az ügy tehát felveti a különböző alapvető jogok – azaz a magánélet tiszteletben tartásához való jog, illetve a tulajdon védelméhez és a hatékony jogorvoslathoz való jog – védelmére vonatkozó követelmények közötti egyeztetés kérdését.

Arra a következtetésre jutott, hogy „a tagállamok feladata, hogy a fent említett irányelvek átültetése során figyeljenek arra, hogy ezen irányelvek olyan értelmezésére támaszkodjanak, amely lehetővé teszi a közösségi jogrend által védett különböző alapjogok igazságos egyensúlyának a biztosítását. Továbbá az említett irányelvek átültetésére vonatkozó intézkedések végrehajtása során a tagállami hatóságoknak és bíróságoknak nemcsak az a kötelessége, hogy nemzeti jogukat az utóbbiakkal összhangban értelmezzék, hanem az is, hogy ne támaszkodjanak ezen irányelvek olyan értelmezésére, amely sérti az alapvető jogokat vagy a közösségi jog egyéb általános elveit, úgymint az arányosság elvét”.[126]

Példa: A *Bonnier Audio AB és társai kontra Perfect Communication Sweden AB* ügy[127] a szellemi tulajdonhoz való jogok és a személyes adatok védelmének összeegyeztetésével foglalkozott. A felperesek – 27 hangoskönyv szerzői jogával rendelkező öt kiadóvállalat – eljárást indítottak a svéd bíróságon azt

126 *Uo.*, 65. és 68. pont; lásd még: EUB, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) kontra Netlog NV*, C-360/10. sz. ügy, 2012. február 16.

127 EUB, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB kontra Perfect Communication Sweden AB*, C-461/10. sz. ügy, 2012. április 19.

állítva, hogy egy FTP-szerverrel (egy fájlátviteli protokoll, amely lehetővé teszi adatok megosztását és átvitelét az interneten keresztül) megsértették ezeket a szerzői jogokat. A felperesek kérték az internetszolgáltatót, hogy adja ki azon IP-címet használó személy nevét és címét, amelyikről elküldték a szóban forgó fájlokat. Az internetszolgáltató, az ePhone kifogásolta a kérvényt arra hivatkozva, hogy az sérti a 2006/24 irányelvet (adatmegőrzési irányelv – 2014-ben hatályon kívül helyezték).

A svéd bíróság az ügyet az EUB elé vitte, azt kérdezve, hogy a 2006/24 irányelv kizárja-e egy, a 2004/48 irányelv (a szellemi tulajdonjogok érvényesítéséről szóló irányelv) 8. cikkén alapuló olyan nemzeti rendelkezés alkalmazását, amely rendelkezés lehetővé teszi olyan bírói határozat kiadását, amely kötelezi az internetszolgáltatót azon előfizetők adatainak szerzői jog tulajdonosai részére történő kiadására, akiknek az IP-címét állítólagosan használták a jogsértés során. A kérdés azon feltételezésen alapult, hogy a felperes egyértelmű bizonyítékot szolgáltatott egy konkrét szerzői jog megsértésére, és hogy az intézkedés arányos.

Az EUB rámutatott arra, hogy a 2006/24 irányelv kizárólag az elektronikus hírközlési szolgáltatók által létrehozott adatok kezelésével és megőrzésével foglalkozott súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása céljából, valamint ezek illetékes nemzeti hatóságok számára történő közlése érdekében. A szellemi tulajdonjogok érvényesítéséről szóló irányelvet átültető nemzeti rendelkezés tehát nem tartozik a 2006/24 irányelv hatálya alá, és ennélfogva azt nem zárja ki a szóban forgó irányelv.[128]

Ami a kérdéses nevek és címek felperesek által kért közlését illeti, az EUB megállapította, hogy az személyes adatok kezelésének minősül a 2002/58 irányelv alapján (elektronikus hírközlési adatvédelmi irányelv), és annak hatálya alá tartozik. Azt is megjegyezte, hogy ezeket az adatokat egy polgári eljárás keretében kérelmezték a szerzői jog jogosultja javára a szerzői jog hatékony védelmének biztosítása céljából, így tehát a kérelem a tárgyára tekintettel a 2004/48 irányelv hatálya alá tartozik.[129]

128 *Uo.*, 40–41. pont.

129 *Uo.*, 52–54. pont. Lásd még: EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008. január 29., 58. pont.

Az EUB arra a következtetésre jutott, hogy a 2002/58 és 2004/48 irányelvet úgy kell értelmezni, hogy azokkal nem ellentétes az alapeljárásban előfordulóhoz hasonló nemzeti jogszabály, amennyiben ez a jogszabály a kereshetőségi joggal rendelkező személy által előterjesztett, személyes adatok közlésére vonatkozó meghagyás iránti kérelem tárgyában eljáró nemzeti bíróság számára lehetővé teszi, hogy az egyes esetek körülményei alapján és az arányosság elvéből eredő követelmények megfelelő figyelembevételével mérlegelje az ellentétes érdekeket.

1.3.6 Adatvédelem és gazdasági érdekek

A digitális korszakban vagy az óriás méretű adathalmazok korában az adatokat a gazdasági innovációt és kreativitást beindító „új olajnak" titulálták.[130] Számos vállalat az adatkezelésre épülő robusztus üzleti modelleket alakított ki, és ez az adatkezelés gyakran személyes adatokat érint. Egyes vállalatok azt hihetik, hogy a személyes adatok védelméhez kapcsolódó konkrét szabályok a gyakorlatban a gazdasági érdekeiket befolyásoló túlzott terheket tartalmazó kötelezettségeket írnak elő. Így tehát felmerül a kérdés, hogy adatkezelők és adatfeldolgozók gazdasági érdekei, vagy a nyilvánosság gazdasági érdekei indokolhatják-e az adatvédelemhez való jog korlátozását.

Példa: A *Google Spain* ügyben[131] az EUB megállapította, hogy bizonyos feltételek mellett az egyéneknek jogukban áll kérni személyes adataik internetes keresőmotorok találati listájából való törlését. Indokolásában az EUB rámutatott arra, hogy a keresőmotorok és a találati listák lehetővé teszik, hogy létrehozzák egy egyén részletes profilját. Ezek az információk az egyén magánéletének számos vonatkozását érinthetik, és ezeket a keresőmotor nélkül nem, vagy csak nagyon nehezen lehetett volna összekapcsolni. Ezért ez potenciálisan az érintettek magánélethez és a személyes adatok védelméhez fűződő alapjogaiba való súlyos beavatkozásnak minősül.

130 Lásd például: *Financial Times* (2016), „Data is the new oil... who's going to own it?", 2016. november 16.

131 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13.

Az EUB ezt követően megvizsgálta, hogy a beavatkozás indokolható-e. A keresőmotort üzemeltető vállalat adatkezeléshez fűződő gazdasági érdekeire figyelemmel az EUB leszögezte, hogy „meg kell állapítani, hogy azt [a beavatkozást] önmagában a keresőmotor működtetőjének ezen adatkezeléshez fűződő gazdasági érdeke nem igazolhatja", és – főszabály szerint – a Charta 7. és 8. cikke alapján megillető alapvető jogok megelőzik a nyilvánosság azon érdekét, hogy az érintett neve alapján történő kereséssel megtalálják ezen információkat.[132]

Az európai adatvédelmi jog egyik fő megfontolása az, hogy az egyének számára biztosítja a személyes adataik feletti fokozottabb ellenőrzést. Különösen a digitális korban felborult az egyensúly a hatalmas mennyiségű személyes adatot kezelő és azokhoz hozzáféréssel rendelkező gazdasági szereplők ereje és e személyes adatok érintettjeinek ereje között az információk ellenőrzése terén. Az EUB eseti alapú megközelítést alkalmaz az adatvédelem és a gazdasági érdekek – például harmadik felek részvénytársaságokkal és korlátolt felelősségű társaságokkal kapcsolatos érdekei – mérlegelésekor, ahogy azt a Manni ítélet is szemlélteti.

Példa: A *Manni* ügy[133] egy magánszemély személyes adatainak kereskedelmi nyilvántartásba történő felvételével foglalkozott. Salvatore Manni kérelmezte a leccei kereskedelmi kamaránál adatainak nyilvántartásból való törlését, miután felfedezte, hogy ha a potenciális ügyfelek megnézik a nyilvántartást, azt látják, hogy egy olyan vállalatnak az ügyvezetője volt, amely több mint egy évtizeddel korábban csődbe ment. Ez az információ elfogulttá tette potenciális ügyfeleit, és negatív hatást gyakorolhatott kereskedelmi érdekeire.

Az EUB-t annak megállapítására kérték fel, hogy az uniós jog elismeri-e ebben az esetben a törléshez való jogot. Ítéletében a bíróság mérlegelte az uniós adatvédelmi szabályokat és S. Manninak a korábbi vállalata csődjére vonatkozó információk törléséhez fűződő kereskedelmi érdekeit, összevetve azokat az információhoz való hozzáféréshez fűződő közérdekkel. Tekintetbe vette, hogy a közhitelű cégnyilvántartások nyilvánosságra hozatalát törvény, és különösen egy, a vállalati információk harmadik felek általi hozzáférésének

132 *Uo.*, 81. és 97. pont.

133 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017. március 9.

megkönnyítésére irányuló uniós irányelv írja elő. Az adatszolgáltatás azon harmadik felek érdekeinek védelmére irányul, akik egy adott vállalattípussal kívánnak üzleti tevékenységet bonyolítani, mivel a részvénytársaságoknak és a korlátolt felelősségű társaságoknak kizárólag a társasági vagyonuk áll rendelkezésükre biztosítékul harmadik személyek számára. E célból „az érintett társaság lényeges okirataiba betekintést kell biztosítani annak érdekében, hogy harmadik személyek megbizonyosodhassanak ezek tartalmáról és a társaságra vonatkozó egyéb adatokról, különösen a társaság nevében történő kötelezettségvállalásra feljogosított személyek adatait illetően".[134]

Figyelemmel a nyilvántartás által szolgált törvényes cél fontosságára, az EUB megállapította, hogy S. Manninak nem volt joga személyes adatainak törlését kérni, mivel magasabb rendű annak szükségessége, hogy a harmadik személyek érdekei a részvénytársaságokkal és a korlátolt felelősségű társaságokkal kapcsolatosan védelemben részesüljenek, és hogy a jogbiztonságot, a kereskedelmi ügyletek tisztességességét, és ily módon a belső piac megfelelő működését biztosítsák. Ez különösen így van figyelemmel arra, hogy azok a természetes személyek, akik ilyen társaság közvetítésével kívánnak részt venni a gazdasági életben, tudomással bírnak arról, hogy kötelesek nyilvánossá tenni a személyazonosságukkal és az e társaságban betöltött tisztségükkel kapcsolatos adatokat.

Bár megállapította, hogy ebben az esetben nem volt indok az adatok törlését kérni, az EUB elismerte az adatkezelés elleni tiltakozáshoz való jogot, megjegyezve, hogy: „nem zárható ki, […] hogy felmerülhetnek olyan különös helyzetek, amelyekben az érintett személy sajátos helyzetével kapcsolatos lényeges, jogos érdekek kivételesen igazolják, hogy a rá vonatkozó, a nyilvántartásba bejegyzett személyes adatokhoz való hozzáférést […] kellően hosszú időszak elteltével az adatokba való betekintéshez fűződő különös érdeküket igazoló harmadik személyekre korlátozzák".[135]

Az EUB leszögezte, hogy a nemzeti bíróságok feladata megvizsgálni az egyes esetekben, és figyelemmel az egyén valamennyi lényeges körülményére, azon jogos vagy kényszerítő okokat, amelyek kivételesen igazolhatják harmadik felek azon jogának korlátozását, hogy hozzáférjenek

134 *Uo.*, 49. pont.

135 *Uo.*, 60. pont.

a cégnyilvántartásokban található személyes adatokhoz. Tisztázta ugyanakkor, hogy S. Manni esetében kizárólag azon körülmény, miszerint potenciális ügyfélkörét állítólag befolyásolta személyes adatainak cégnyilvántartásban való közzététele, nem minősül ilyen jogos és kényszerítő oknak. S. Manni potenciális ügyfeleinek jogos érdeke fűződik a korábbi vállalkozásának csődjére vonatkozó információkat megismerni.

S. Manninak és a nyilvántartásban szereplő többi személynek a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő, a Charta 7. és 8. cikkében garantált alapjogaiba való beavatkozás közérdekű célt szolgált és szükséges és arányos volt.

A *Manni* ügyben ezért az EUB azt állapította meg, hogy az adatvédelemhez és magánélethez való jogok nem előzik meg harmadik felek azon jogát, hogy hozzáférjenek a cégnyilvántartásban részvénytársaságokkal és korlátolt felelősségű társaságokkal összefüggésben szereplő adatokhoz.

2 Adatvédelmi terminológia

EU	Tárgyalt kérdések	Európa Tanács
Személyes adatok		
Általános adatvédelmi rendelet, 4. cikk 1. pont Általános adatvédelmi rendelet, 4. cikk 5. pont és 5. cikk (1) bekezdés e) pont Általános adatvédelmi rendelet, 9. cikk EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010 EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008 EUB, *Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10. sz. ügy, 2011 EUB, *Patrick Breyer kontra Bundesrepublik Deutschland*, C-582/14. sz. ügy, 2016 EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel* és *Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014	**Az adatvédelem jogi meghatározása**	Korszerűsített 108. Egyezmény, 2. cikk a) pont EJEB, *Bernh Larsen Holding AS és társai kontra Norvégia*, 24117/08. sz. ügy, 2013 EJEB, *Uzun kontra Németország*, 35623/05. sz. ügy, 2010 EJEB, *Amann kontra Svájc* [Nagykamara], 27798/95. sz. ügy, 2000

EU	Tárgyalt kérdések	Európa Tanács
EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003	**Személyes adatok különleges kategóriái (különleges adatok)**	Korszerűsített 108. Egyezmény, 6. cikk (1) bekezdés
EUB, *Peter Nowak kontra Data Protection Commissioner*, C-434/16. sz. ügy, 2017	**Anonimizált és álnevesített személyes adatok**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés e) pont A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 50. pont
Adatfeldolgozás		
Általános adatvédelmi rendelet, 4. cikk 2. pont EUB, *František Ryneš kontra Úřad pro ochranu osobních údajů*, C-212/13. sz. ügy, 2014 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014	**Fogalom-meghatározások**	Korszerűsített 108. Egyezmény, 2. cikk b) és c) pont
Adatfelhasználók		
Általános adatvédelmi rendelet, 4. cikk 7. pont EUB, *František Ryneš kontra Úřad pro ochranu osobních údajů*, C-212/13. sz. ügy, 2014 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014	**Adatkezelő**	Korszerűsített 108. Egyezmény, 2. cikk d) pont A profilalkotásra vonatkozó ajánlás, 1. cikk g) pont*

EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 4. cikk 8. pont	**Adatfeldolgozó**	Korszerűsített 108. Egyezmény, 2. cikk f) pont A profilalkotásra vonatkozó ajánlás, 1. cikk h) pont
Általános adatvédelmi rendelet, 4. cikk 9. pont	**Címzett**	Korszerűsített 108. Egyezmény, 2. cikk e) pont
Általános adatvédelmi rendelet, 4. cikk 10. pont	**Harmadik fél**	
Hozzájárulás		
Általános adatvédelmi rendelet, 4. cikk 11. pont és 7. cikk EUB, *Deutsche Telekom AG kontra Bundesrepublik Deutschland*, C-543/09. sz. ügy, 2011 EUB, *Tele2 (Netherlands) BV és társai kontra Autoriteit Consument en Markt (AMC)*, C-536/15. sz. ügy, 2017	**Az érvényes hozzájárulás fogalmának meghatározása és követelményei**	Korszerűsített 108. Egyezmény, 5. cikk (2) bekezdés Az orvosi adatokra vonatkozó ajánlás, 6. cikk, valamint különböző későbbi ajánlások EJEB, *Elberte kontra Lettország*, 61243/08. sz. ügy, 2015

*Megjegyzés: * Az Európa Tanács Miniszteri Bizottságának Rec(2010)13. sz. ajánlása a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről (a profilalkotásra vonatkozó ajánlás), 2010. november 23.*

2.1 Személyes adatok

Főbb pontok

- Az adatok akkor minősülnek személyes adatnak, ha azonosított vagy azonosítható természetes személyre, az érintettre vonatkoznak.
- Annak megállapítására, hogy a természetes személy azonosítható-e, az adatkezelőnek vagy más személynek minden olyan észszerű eszközt – például a megjelölést – figyelembe kell vennie, amelyek segítségével a természetes személy közvetlenül vagy közvetetten azonosítható.
- A hitelesítés annak bizonyítását jelenti, hogy egy bizonyos személy egy bizonyos személyazonossággal és/vagy bizonyos tevékenységek folytatására vonatkozó engedéllyel rendelkezik.

- Vannak olyan, a Korszerűsített 108. Egyezményben és az uniós adatvédelmi jogban felsorolt különleges adatkategóriák, az úgynevezett különleges adatok, amelyek fokozott védelmet igényelnek, ezért különleges jogi szabályozás vonatkozik rájuk.
- Az adatok akkor anonimizáltak, ha azok már nem vonatkoznak egy azonosított vagy azonosítható természetes személyre.
- Az álnevesítés egy olyan művelet, amely révén a személyes adatok további információk nélkül nem kapcsolhatók az érintetthez. Az érintett ismételt azonosítását lehetővé tevő „kulcsot" elkülönítve és biztonságos helyen kell tárolni. Az álnevesítésen átesett adatok továbbra is személyes adatok maradnak. Az uniós jogban nem létezik az „álnevesített adat" fogalma.
- Az adatvédelem elvei és szabályai nem vonatkoznak az anonimizált adatokra, az álnevesített adatokra viszont igen.

2.1.1 A személyes adat fogalmának főbb vonatkozásai

Mind az **uniós jog**, mind az **Európa Tanács joga** szerint a „személyes adat" egy azonosított vagy azonosítható természetes személyre vonatkozó bármely információt jelent.[136] Egy olyan személyre vonatkozó információkat jelent, akinek a személyazonossága vagy nyilvánvalóan egyértelmű, vagy további információk segítségével megállapítható. Annak megállapítására, hogy egy személy azonosítható-e, az adatkezelőnek vagy másik személynek minden olyan észszerű eszközt figyelembe kell vennie, amelyek segítségével az egyén közvetlenül vagy közvetetten azonosítható, ilyen például a megjelölés, ami lehetővé teszi valamely személy másiktól eltérő kezelését.[137]

Ha ilyen személlyel kapcsolatos adatok kezelésére kerül sor, ezt a személyt „érintettnek" nevezik.

Az érintett

Az **uniós jogban** a természetes személyek az adatvédelmi szabályok[138] egyetlen kedvezményezettjei, és az európai adatvédelmi jog kizárólag élőlényeket részesít

136 Általános adatvédelmi rendelet, 4. cikk 1. pont; Korszerűsített 108. Egyezmény, 2. cikk a) pont.

137 Általános adatvédelmi rendelet, (26) preambulumbekezdés.

138 *Uo.*, 1. cikk.

védelemben.[139] Az általános adatvédelmi rendelet meghatározása szerint a személyes adat azonosított vagy azonosítható természetes személyre vonatkozó bármely információ.

Az **Európa Tanács joga**, nevezetesen a Korszerűsített 108. Egyezmény is az egyének védelmére hivatkozik személyes adataik kezelését illetően. A személyes adat ennél is egy azonosított vagy azonosítható egyénre vonatkozó bármely információt jelent. Ezt a természetes személyt vagy egyént, ahogy az általános adatvédelmi rendelet, illetve a Korszerűsített 108. Egyezmény hivatkozik rá, az adatvédelmi jog érintettnek nevezi.

A jogi személyek is részesülnek bizonyos mértékű védelemben. Az EJEB ítélkezési gyakorlatában létezik jogi személyek kereseti kérelme ügyében hozott ítélet, amelyet jogi személy adatainak felhasználásával szembeni, az EJEE 8. cikke szerinti védelemhez való jog állítólagos megsértésével kapcsolatban hozott. Az EJEE 8. cikke kiterjed a magán- és családi élet, a lakás és a kapcsolattartás tiszteletben tartásához való jogra egyaránt. A Bíróság ezért inkább ez utóbbi, semmint a magánélethez való jog alapján vizsgálhat meg ügyeket.

Példa: A *Bernh Larsen Holding AS és társai kontra Norvégia* ügy[140] három norvég társaság által egy adóhatósági határozattal kapcsolatban benyújtott panasszal foglalkozott, amely határozat előírta, hogy a nevezett társaságok az általuk közösen használt számítógépes szerveren található összes adatról készítsenek másolatot, és adják át az adóellenőröknek.

Az EJEB megállapította, hogy a felperes társaságok erre való kötelezése beavatkozás az EJEE 8. cikke értelmében vett „lakás" és „kapcsolattartás" tiszteletben tartásához való jogba. A Bíróság azonban azt állapította meg, hogy az adóhatóság tényleges és megfelelő garanciákat biztosított a visszaéléssel szemben: a felperes társaságokat jóval korábban tájékoztatták; a helyszíni beavatkozás során jelen voltak, és lehetőségük volt észrevételek benyújtására; és az anyagot az adóellenőrzés befejezését követően meg kellett semmisíteni. Ilyen körülmények között igazságos egyensúlyt teremtettek egyrészről a felperes társaságok „lakás" és

139 *Uo.*, (27) preambulumbekezdés. Lásd még a 29. cikk szerinti munkacsoport (2007) *4/2007. sz. véleményét a személyes adat fogalmáról*, WP 136, 2007. június 20., 22. o.

140 EJEB, *Bernh Larsen Holding AS és társai kontra Norvégia*, 24117/08. sz. ügy, 2013. március 14. Lásd még azonban: EJEB, *Liberty és társai kontra Egyesült Királyság*, 58243/00. sz. ügy, 2008. július 1.

„kapcsolattartás" tiszteletben tartásához való joga és a náluk dolgozó személyek adatainak védelméhez fűződő joga, másrészről az adóellenőrzés céljából végzett hatékony szemléhez fűződő közérdek között. A Bíróság ezért arra a következtetésre jutott, hogy nem sértették meg a 8. cikket.

A **Korszerűsített 108. Egyezmény értelmében** az adatvédelem elsősorban a természetes személyeket részesíti oltalomban, azonban a részes felek nemzeti jogszabályaikban az adatvédelmet kiterjeszthetik a jogi személyekre is, például gazdasági társaságokra és egyéb szervezetekre. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kimondja, hogy a nemzeti jog védheti a jogi személyek jogos érdekeit az egyezmény hatályának ilyen szereplőkre való kiterjesztésével.[141] Az **uniós adatvédelmi jog** nem terjed ki a jogi személyeket érintő adatkezelésre, és különösen nem foglalkozik a jogi személyként létrehozott vállalkozásokkal, beleértve a jogi személy nevét és formáját, továbbá elérhetőségét.[142] Az elektronikus hírközlési adatvédelmi irányelv azonban védi a közlések titkosságát és a jogi személyek jogos érdekeit az előfizetői és felhasználói adatok automatikus tárolását és feldolgozását szolgáló növekvő kapacitásra tekintettel.[143] Hasonlóképp, az elektronikus hírközlési adatvédelmi rendelet tervezete is kiterjed a jogi személyek védelmére.

Példa: A *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* ügyben[144] az EUB a mezőgazdasági támogatás kedvezményezettjeire vonatkozó személyes adatok közzétételét vizsgálva megállapította, hogy „a jogi személyek csak annyiban részesülhetnek az ilyen nevesítéssel szembeni, a Charta 7. és 8. cikke szerinti védelemben, amennyiben a jogi személy hivatalos neve alapján azonosítható egy vagy több természetes személy. [...] A magánélethez való jognak a személyes adatok védelméhez való jog tekintetében történő tiszteletben tartása – amelyet a Charta 7. és 8. cikke elismer – az azonosított vagy azonosítható természetes személyre vonatkozó valamennyi információra kiterjed [...]".[145]

141 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 30. pont.

142 Általános adatvédelmi rendelet, (14) preambulumbekezdés.

143 Elektronikus hírközlési adatvédelmi irányelv, (7) preambukumbekezdés és 1. cikk (2) bekezdés.

144 EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9., 53. pont.

145 *Uo.*, 52–53. pont.

Egyrészt az EU arra irányuló érdekeinek, hogy biztosítsa a támogatások odaítélésének átláthatóságát, másrészt pedig a támogatásban részesülő egyének magánélethez és adatvédelemhez való jogának mérlegelése során az EUB úgy vélte, hogy a beavatkozás ezekbe az alapjogokba aránytalan volt. Úgy vélte, hogy az átláthatóságra vonatkozó célját egyéb, az egyének szóban forgó jogába kevésbé beavatkozó jellegű intézkedésekkel is el lehetett volna érni. Amikor azonban a támogatásban részesült jogi személyekkel kapcsolatban vizsgálta az adatok közzétételének arányosságát, az EUB más következtetésre jutott, és kimondta, hogy az ilyen közzététel nem lépte túl az arányosság elvének korlátait. Megállapította, hogy „a személyes adatok védelméhez való jog sérelmének jelentősége ugyanis eltér a jogi személyek és a természetes személyek esetében”.[146] A jogi személyeket a rájuk vonatkozó információk közzététele tekintetében súlyosabb kötelezettségek terhelik. Az EUB úgy vélte, hogy az érintett nemzeti hatóságokra aránytalanul nagy adminisztratív terhet róna annak vizsgálata az adatok közzététele előtt, hogy az egyes jogi személy kedvezményezettek neve alapján azonosíthatók-e természetes személyek. Ezért a jogi személyekre vonatkozó általános adatközzétételt előíró jogszabály tisztességes egyensúlyt teremtett a szóban forgó versengő érdekek között.

Az adatok jellege

Mindenfajta információ személyes adat lehet, amennyiben egy azonosított vagy azonosítható személyre vonatkozik.

Példa: Egy munkavállaló munkateljesítményének felettese általi és a munkavállaló személyes aktájában tartott értékelése a munkavállalóra vonatkozó személyes adatnak minősül. Ez a helyzet akkor is, ha az csak – részben vagy egészben – a felettes személyes véleményét tükrözi, például: „a munkavállaló nem végzi odaadással a munkáját”, és nem tartalmaz konkrétumokat, mint például: „a munkavállaló az elmúlt hat hónapban öt hetet hiányzott”.

146 *Uo.*, 87. pont.

A személyes adatok körébe a személy magánéletére, amely magában foglalja szakmai tevékenységeit is, valamint közéleti tevékenységére vonatkozó információk tartoznak.

Az *Amann* ügyben[147] az EJEB a „személyes adat" fogalmát úgy értelmezte, hogy az nem korlátozódik csupán az egyén magánszférájába tartozó dolgokra. A „személyes adat" fogalmának ilyen értelmezése az általános adatvédelmi rendelet esetében is igaz.

Példa: A *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* ügyben[148] az EUB megállapította, hogy „e tekintetben nincs jelentősége annak a ténynek, hogy a közzétett adatok szakmai tevékenységre vonatkoznak [...]. E tekintetben az Emberi Jogok Európai Bírósága az EJEE 8. cikkének értelmezésére vonatkozóan kimondta, hogy a »magánélet« fogalmát nem lehet megszorítóan értelmezni, és semmiféle elv nem teszi lehetővé a szakmai [...] tevékenységek »magánélet« fogalmából való kizárását".

Példa: Az *YS kontra Minister voor Immigratie, Integratie en Asiel* és *Minister voor Immigratie, Integratie en Asiel kontra M és S* egyesített ügyekben[149] az EUB kimondta, hogy a Bevándorlási és Honosítási Szolgálat határozattervezetében szereplő és a tartózkodási engedély iránti kérelmekkel foglalkozó jogi elemzés annak ellenére, hogy tartalmazhat néhány személyes adatot, önmagában nem minősül személyes adatnak.

Az EJEB-nek az EJEE 8. cikkével kapcsolatos ítélkezési gyakorlatának tanúsága szerint előfordulhat, hogy a magán- és a szakmai élet kérdései nehezen különíthetők el egymástól.[150]

147 Lásd: EJEB, *Amann kontra Svájc* [Nagykamara], 27798/95. sz. ügy, 2000. február 16., 65. pont.

148 EUB, *Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen* [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9., 59. pont.

149 EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel* és *Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014. július 17., 39. pont.

150 Lásd például: EJEB, *Rotaru kontra Románia* [Nagykamara], 28341/95. sz. ügy, 2000. május 4., 43. pont; EJEB, *Niemietz kontra Németország*, 13710/88. sz. ügy, 1992. december 16., 29. pont.

Példa: A *Bărbulescu kontra Románia* ügyben[151] a felperest azért bocsátották el, mert munkaidőben a belső szabályzat megszegésével használta munkáltatójának internetét. A munkáltatója megfigyelte levelezését, és a jegyzőkönyveket, amelyek tisztán magánjellegű üzeneteket tartalmaztak, a hazai eljárás során készítették. Annak megállapítása során, hogy a 8. cikk alkalmazandó-e, az EJEB nyitva hagyta annak kérdését, hogy a munkáltató korlátozó előírásából a felperesnek következtetnie kellett volna annak magánélethez való jogokra gyakorolt észszerű vonzataira, azonban semmiképpen sem vélte úgy, hogy a munkáltató utasításai nullára csökkenthetnék a magánjellegű közösségi életet a munkahelyen. A korlátozás megalapozottságát illetően a részes államoknak széles mozgásteret kell biztosítani annak mérlegelésére, hogy szükséges-e azon feltételeket illetően jogi keretrendszert kialakítani, amelyek mellett a munkáltatók szabályozhatják munkavállalóik nem szakmai – elektronikus vagy egyéb – kommunikációját a munkahelyen. Mindazonáltal a hazai hatóságoknak biztosítaniuk kell, hogy a levelezések és egyéb kommunikációk megfigyelésére irányuló intézkedések munkáltatói bevezetéséhez – az ilyen intézkedések mértékétől és tartamától függetlenül – társuljanak megfelelő és elégséges garanciák a visszaéléssel szemben. Arányosság és eljárási garanciák szükségesek az önkényesség ellen, és az EJEB számos olyan tényezőt azonosított, amelyek relevánsak lehetnek az adott körülmények között. Ezek a tényezők tartalmazták többek között a munkavállalók munkáltató általi megfigyelésének terjedelmét és a munkavállaló magánéletébe történő beavatkozás mértékét, a munkavállalóra vonatkozó következményeket, valamint azt, hogy biztosítottak-e megfelelő garanciákat. Emellett a hazai hatóságoknak biztosítaniuk kell, hogy azon munkavállaló számára, akinek a közléseit megfigyelték, rendelkezésre álljon egy olyan bíróság előtti jogorvoslat lehetősége, amely hatáskörrel rendelkezik annak – legalábbis lényegében történő – megállapítására, hogy a megfogalmazott kritériumok miként lettek alkalmazva, és hogy a megtámadott intézkedések törvényesek voltak-e. Ebben az ügyben az EJEB megállapította a 8. cikk megsértését, mivel a hazai hatóságok nem biztosították a felperes magánélet és kapcsolattartás tiszteletben tartásához való jogának megfelelő védelmét, és következésképpen nem sikerült tisztességes egyensúlyt teremteniük a szóban forgó érdekek között.

151 EJEB, *Bărbulescu kontra Románia* [Nagykamara], 61496/08. sz. ügy, 2017. szeptember 5., 121. pont.

Az **uniós jog** és az **Európa Tanács joga szerint** az információ akkor tartalmaz személyre vonatkozó adatokat, ha:

- az egyén ezzel az információval azonosított vagy azonosítható; vagy
- ha az egyén, bár nem azonosították, az adott információval olyan módon megjelölhető, ami további kutatással lehetővé teszi az érintett személyazonosságának megállapítását.

Az európai adatvédelmi jog mindkét típusú információt azonos módon védi. Az egyének közvetlen vagy közvetett azonosítását folyamatosan értékelni kell, „számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését".[152] Az EJEB ismételten kimondta, hogy a „személyes adat" EJEE szerinti fogalma azonos a 108. Egyezményben szereplő fogalommal, különösen ami az azonosított vagy azonosítható személyekre vonatkozó feltételt illeti.[153]

Az általános adatvédelmi rendelet kiköti, hogy valamely természetes személy akkor azonosítható, ha „ közvetlen vagy közvetett módon, különösen valamely azonosító, például név, azonosító szám, helymeghatározó adat, online azonosító vagy a személy testi, fiziológiai, genetikai, szellemi, gazdasági, kulturális vagy szociális azonosságára vonatkozó egy vagy több tényező alapján azonosítható".[154] Az azonosításhoz tehát olyan elemek szükségesek, amelyek úgy írnak le egy személyt, hogy az illető minden más embertől megkülönböztethető és egyénként azonosítható lesz. Az ilyen leíró elemek kiváló példája az egyén neve, amely közvetlenül azonosíthat egy személyt. Néhány esetben egyéb jellemzők a névhez hasonló hatással rendelkezhetnek, és általuk valamely személy közvetlenül azonosíthatóvá válik. A telefonszám, társadalombiztosítási szám és a gépjármű rendszáma például mind olyan információ, amellyel egy egyén azonosítható. Egyéb jellemzőket is lehet használni – például számítógépes fájlokat, sütiket és webforgalom-megfigyelő eszközöket – az egyének viselkedésük és szokásaik azonosításával történő megjelölésére. A 29. cikk szerinti munkacsoport egyik véleményében kifejtettek szerint „még akár az egyén nevének és címének lekérdezése nélkül is lehet a személyt kategorizálni társadalmi-gazdasági, pszichológiai, filozófiai vagy egyéb feltételek alapján, és bizonyos döntéseket neki tulajdonítani, mivel az egyén csatlakozási pontja (a számítógép) szűken értelmezve már nem feltétlenül kéri a személyazonosság

152 Általános adatvédelmi rendelet, (26) preambulumbekezdés.

153 Lásd: EJEB, *Amann kontra Svájc* [Nagykamara], 27798/95. sz. ügy, 2000. február 16., 65. pont.

154 Általános adatvédelmi rendelet, 4. cikk 1. pont

megadását".[155] A személyes adatok definíciója az Európa Tanács joga és az uniós jog alapján egyaránt elég tág ahhoz, hogy az azonosítás valamennyi lehetséges módját (és ennélfogva az azonosíthatóság minden fokát) lefedje.

Példa: A *Promusicae kontra Telefónica de España* ügyben[156] az EUB megállapította, hogy „nem vitatott, hogy [egy bizonyos internetes fájlmegosztó platform] meghatározott használói nevének és címének Promusicae által kért közlése a személyes adatok, vagyis – a 95/46 irányelv 2. cikke a) pontja [jelenleg az általános adatvédelmi rendelet 4. cikk 1. pontja] fogalommeghatározásának megfelelően – azonosított vagy azonosítható természetes személyre vonatkozó információk rendelkezésre bocsátásának minősül. A Promusicae szerint a Telefónica által tárolt – amelyet ez utóbbi nem vitatott – információk e közlése személyes adatok feldolgozásának minősül".[157]

Példa: A *Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)* ügyben[158] a Scarlet internetszolgáltató megtagadta, hogy fájlcserélő szoftverek útján zajló elektronikus adatátvitelt szűrő rendszert telepítsen a SABAM – szerzőket, zeneszerzőket és kiadókat képviselő jogkezelő szervezet – által védett szerzői jogokat sértő fájlcserék megakadályozása érdekében. Az EUB azt állapította meg, hogy a felhasználók IP-címei „védett személyes adatok, hiszen lehetővé teszik az említett felhasználók pontos azonosítását".

Mivel sok név nem egyedi, a személyazonosság megállapításához további jellemzőkre is szükség lehet annak biztosításához, hogy a személyt ne tévesszék össze más személlyel. Néha a közvetlen és közvetett jellemzőket kombinálni kell azon egyén azonosítása érdekében, akire az információk vonatkoznak. A születési időt és helyet gyakran használják erre a célra. Ezenfelül egyes országokban – a polgárok jobb megkülönböztethetősége érdekében – személyi azonosító számokat is

155 29. cikk szerinti munkacsoport, *4/2007. sz. vélemény a személyes adat fogalmáról*, WP 136, 2007. június 20., 15. o.

156 EUB, *Productores de Música de España (Promusicae) kontra Telefónica de España SAU* [nagytanács], C-275/06. sz. ügy, 2008. január 29., 45. pont.

157 A korábbi 95/46 irányelv 2. cikkének b) pontja, most az általános adatvédelmi rendelet 4. cikkének 2. pontja.

158 EUB, *Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, C-70/10. sz. ügy, 2011. november 24., 51. pont.

bevezettek. Továbbított adóügyi adatok,[159] közigazgatási dokumentumban szereplő, tartózkodási engedélyt kérelmezőre vonatkozó adatok,[160] valamint banki és bizalmi kapcsolatokra vonatkozó dokumentumok[161] személyes adatnak minősülhetnek. A biometrikus adatok, köztük az ujjlenyomatok, a digitális fényképek vagy az íriszfelismerés, a helymeghatározó adatok, illetve online jellemzők a technológia korában egyre nagyobb szerepet kapnak a személyek azonosítása terén.

Az európai adatvédelmi jog alkalmazhatóságához azonban nincs szükség az érintett tényleges azonosítására, elegendő, hogy az érintett személy azonosítható. Valamely személy akkor minősül azonosíthatónak, ha elegendő olyan elem áll rendelkezésre, amelyek segítségével a személy közvetlenül vagy közvetetten azonosítható.[162] Az általános adatvédelmi rendelet (26) preambulumbekezdése értelmében a döntő az, hogy valószínű-e, hogy rendelkezésre fognak állni az azonosítás észszerű eszközei, és az adatok előre látható felhasználói felhasználják-e azokat; ez magában foglalja a harmadik fél adatátvevőket is (lásd a 2.3.2 szakaszt).

Példa: Egy helyi hatóság elhatározza, hogy adatokat gyűjt a helyi utcákon gyorshajtást elkövető autókról. Lefényképezi a gépkocsikat, automatikusan rögzítve az időt és a helyet annak érdekében, hogy az adatokat az illetékes hatóságnak továbbítsa, hogy ez utóbbi hatóság megbüntethesse a sebességhatárt túllépő személyeket. Egy érintett panaszt nyújt be azzal, hogy a helyi hatóságnak az adatvédelmi törvény értelmében nem volt jogalapja az ilyen adatgyűjtésre. A helyi hatóság fenntartja, hogy nem gyűjt személyes adatokat. A rendszámtáblák szerinte anonimek. A helyi hatóságnak nincs hozzáférési engedélye az általános gépjármű-nyilvántartáshoz, amelyből kideríthetné a gépjármű tulajdonosának vagy vezetőjének kilétét.

Ez az indoklás nincs összhangban az általános adatvédelmi rendelet (26) preambulumbekezdésével. Figyelemmel arra, hogy az adatgyűjtés célja egyértelműen a gyorshajtók azonosítása, várható, hogy megkísérlik az azonosítást. Bár a helyi hatóságok nem rendelkeznek az azonosításra alkalmas közvetlen eszközökkel, továbbítják az adatokat

159 EUB, *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015. október 1.

160 EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel* és *Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014. július 17.

161 EJEB, *M.N. és társai kontra San Marino*, 28005/12. sz. ügy, 2015. július 7.

162 Általános adatvédelmi rendelet, 4. cikk 1. pont.

az illetékes hatóságnak, a rendőrségnek, amelynek viszont vannak ilyen eszközei. A (26) preambulumbekezdés is kifejezetten tartalmaz olyan forgatókönyvet, mely szerint valószínű, hogy az adatok közvetlen felhasználójától eltérő további címzettek megkísérlik a személy azonosítását. A (26) preambulumbekezdés figyelembevételével a helyi hatóság intézkedése kimeríti az azonosítható személyekről való adatgyűjtés fogalmát, ezért az adatvédelmi törvény szerint jogalap szükséges hozzá.

„Annak meghatározásakor, hogy mely eszközökről feltételezhető észszerűen, hogy egy adott természetes személy azonosítására fogják felhasználni, az összes objektív tényezőt figyelembe kell venni, így például az azonosítás költségeit és időigényét, számításba véve az adatkezeléskor rendelkezésre álló technológiákat, és a technológia fejlődését".[163]

Példa: A *Breyer kontra Bundesrepublik Deutschland* ügyben[164] az EUB az érintettek közvetett azonosíthatóságának fogalmát vizsgálta. Az ügy dinamikus IP-címekkel foglalkozott, amelyek minden új internetkapcsolat létrehozásakor változnak. A szövetségi német intézmények által üzemeltetett weboldalak regisztrálták és tárolták a dinamikus IP-címeket annak érdekében, hogy megelőzzék a kibertámadásokat és szükség esetén büntetőeljárásokat kezdeményezhessenek. Csak a Patrick Breyer által igénybe vett internetszolgáltató rendelkezett az azonosításához szükséges további adatokkal.

Az EUB úgy vélte, hogy valamely online médiaszolgáltató által a nyilvánosság számára hozzáférhetővé tett internetes honlap valamely személy által történő felkeresésekor az e szolgáltató által rögzített dinamikus IP-cím személyes adatnak minősül akkor is, ha csak egy harmadik félnek – a jelen ügyben az internetszolgáltatónak – állnak rendelkezésére a személy azonosításához szükséges további adatok.[165] Azt állapította meg, hogy ahhoz, hogy az adatok személyes adatokat testesítsenek meg, „egyáltalán nem szükséges, hogy az érintett azonosítását lehetővé tevő információk egyetlen személy kezében legyenek". Egy internetszolgáltató által regisztrált

163 *Uo.*, (26) preambulumbekezdés.

164 EUB, *Patrick Breyer kontra Bundesrepublik Deutschland*, C-582/14. sz. ügy, 2016. október 19., 43. pont.

165 Az Európai Parlament és a Tanács 1995. október 24-i már nem hatályos 95/46/EK irányelve a személyes adatok feldolgozása vonatkozásában az egyének védelméről és az ilyen adatok szabad áramlásáról, 2. cikk a) pont.

dinamikus IP-címek használói bizonyos szituációkban azonosíthatók, például kibertámadások esetén büntetőeljárás keretében egyéb személyek segítségével.[166] Az EUB álláspontja szerint, amennyiben a szolgáltatónak „jogszerű eszközök állnak a rendelkezésére az érintett személynek az e személy internet-hozzáférést nyújtó szolgáltatójának rendelkezésére álló további adatok révén történő azonosításához", az olyan módszernek minősül, amelyet „valószínűleg felhasználnak az érintett személy azonosítására". Ezért az ilyen adatok személyes adatnak minősülnek.

Az **Európa Tanács joga** szerint is ehhez hasonlóan kell értelmezni az azonosíthatóságot. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés hasonló leírást tartalmaz: az „azonosítható" fogalma nem pusztán önmagában az egyén polgári vagy jogi azonosítására utal, hanem arra is, hogy mi teszi lehetővé egy személy „egyéniesítését" vagy megjelölését, és ennek eredményeképp esetleges másoktól eltérő kezelését. Ez az „egyéniesítés" történhet például kifejezetten az illetőre, vagy egy azonosító számhoz rendelt készülékre vagy készülékek kombinációjára (számítógép, mobiltelefon, kamera, játékeszköz stb.), fedőnévre, biometrikus vagy genetikai adatokra, helymeghatározó adatokra, IP-címre vagy más azonosítóra történő hivatkozással.[167] Az egyén nem minősül „azonosíthatónak", ha azonosítása észszerűtlenül sok időt, erőfeszítést vagy erőforrásokat igényel. Ez a helyzet akkor például, ha egy érintett azonosítása túlzottan összetett, hosszadalmas és költséges műveleteket igényelne. Az észszerűtlenül sok időt, erőfeszítést vagy erőforrásokat eseti alapon kell vizsgálni, mely során figyelembe kell venni olyan tényezőket, mint az adatkezelés célja, az azonosítás költsége és előnyei, az adatkezelő típusa és az igénybe vett technológia.[168]

A személyes adatok tárolásának vagy felhasználásának formáját illetően fontos megjegyezni, hogy az nem releváns az adatvédelmi törvény alkalmazhatósága szempontjából. Személyes adatokat és képeket írásbeli vagy szóbeli kommunikáció egyaránt tartalmazhat,[169] a zárt láncú televíziós (CCTV) felvételeket[170] vagy

166 EUB, *Patrick Breyer kontra Bundesrepublik Deutschland*, C-582/14. sz. ügy, 2016. október 19., 47–48. pont.

167 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 18. pont.

168 *Uo.*, 17. pont.

169 EJEB, *Von Hannover kontra Németország*, 59320/00. sz. ügy, 2004. június 24.; EJEB, *Sciacca kontra Olaszország*, 50774/99. sz. ügy, 2005. január 11.; EUB, *František Ryneš kontra Úřad pro ochranu osobních údajů*, C-212/13. sz. ügy, 2014. december 11.

170 EJEB, *Peck kontra Egyesült Királyság*, 44647/98. sz. ügy, 2003. január 28; EJEB, *Köpke kontra Németország*, 420/07. sz. ügy, 2010. október 5.; EDPS (2010), *Az európai adatvédelmi biztos videokamerás megfigyelésre vonatkozó iránymutatásai*, 2010. március 17.

hangfelvételeket is beleértve.[171] Az elektronikusan rögzített információ és a papír alapú információ is minősülhet személyes adatnak. Még az emberi szövetből vett – DNS-t tartalmazó – sejtminták is lehetnek biometrikus adatok kinyerésére alkalmas források,[172] amennyiben az adatok az egyén öröklött vagy szerzett genetikai jellemzőire vonatkoznak, egyedi információkat szolgáltatnak az egyén egészségi vagy fiziológiai állapotáról, és az adott személyből nyert biológiai minta elemzésének az eredményei.[173]

Anonimizálás

A személyes adatok korlátozott tárolhatóságának az általános adatvédelmi rendeletben és a Korszerűsített 108. Egyezményben meghatározott elvei szerint (részletesebben a 3. fejezet tárgyalja) az adatokat úgy kell tárolni, „hogy kizárólag addig tegyék lehetővé az érintettek azonosítását, amíg az a személyes adatok feldolgozásának [helyesen: kezelésének] célja szempontjából indokolt."[174] Következésképpen az adatokat törölni vagy anonimizálni kellene, ha az adatkezelő azokat az után is tárolni szeretné, hogy nincs már szükség rájuk, és már nem szolgálják az eredeti célt.

Az anonimizálás azt jelenti, hogy a személyes adatállományokból kiszűrik az összes azonosító elemet úgy, hogy az érintett többé ne legyen azonosítható.[175] 05/2014. számú véleményében a 29. cikk szerinti munkacsoport a különböző anonimizálási technikák hatékonyságát és korlátait elemzi.[176] Elismeri az ilyen technikák lehetséges értékét, azonban hangsúlyozza, hogy egyes technikák nem feltétlenül válnak be minden esetben. Egy adott helyzetben az optimális megoldás megtalálásához eseti alapon kell meghatározni, hogy melyik a legmegfelelőbb anonimizálási eljárás. Függetlenül a használt technikától, az azonosítást visszafordíthatatlanul meg kell akadályozni. Ez azt jelenti, hogy az adatok anonimizálásához nem maradhat olyan elem az információban, amely a továbbiakban – észszerű erőfeszítés mellett – lehetővé tehetné az érintett személy(ek) azonosítását.[177] Az újbóli azonosítás kocká-

171 EJEB, *P.G. és J.H. kontra Egyesült Királyság*, 44787/98. sz. ügy, 2001. szeptember 25., 59–60. pont; EJEB, *Wisse kontra Franciaország*, 71611/01. sz. ügy, 2005. december 20. (francia nyelvi változat).

172 Lásd: 29. cikk szerinti munkacsoport (2007), *4/2007. sz. vélemény a személyes adat fogalmáról*, WP 136, 2007. június 20., 9. o.; Európa Tanács, A Miniszteri Bizottság Rec(2006)4. sz. ajánlása a tagállamok részére az emberi eredetű biológiai anyagok kutatásáról, 2006. március 15.

173 Általános adatvédelmi rendelet, 4. cikk 13. pont.

174 *Uo.*, 5. cikk (1) bekezdés e) pont; Korszerűsített 108. Egyezmény, 5. cikk (2) bekezdés e) pont.

175 Általános adatvédelmi rendelet, (26) preambulumbekezdés.

176 29. cikk szerinti munkacsoport (2014), *05/2014. sz. vélemény az anonimitást biztosító technikákról*, WP 216, 2014. április 10.

177 Általános adatvédelmi rendelet, (26) preambulumbekezdés.

zata felmérhető, ha figyelembe vesszük „az ehhez szükséges időt, erőfeszítéseket vagy erőforrásokat figyelemmel az adatok jellegére, felhasználásuk összefüggésére, az újbóli azonosításhoz rendelkezésre álló technológiákra és a kapcsolódó költségekre".[178]

Az adatok sikeres anonimizálását követően azok már nem minősülnek személyes adatnak, és a továbbiakban nem vonatkoznak rájuk az adatvédelmi szabályok.

Az általános adatvédelmi rendelet rendelkezik arról, hogy a személyes adatok kezelését ellenőrző személy vagy szervezet nem köteles kiegészítő információkat megőrizni, beszerezni vagy kezelni annak érdekében, hogy pusztán azért azonosítsa az érintettet, hogy megfeleljen e rendeletnek. E szabály alól azonban van egy komoly kivétel: minden alkalommal, amikor az érintett abból a célból, hogy gyakorolja az adathozzáféréshez, helyesbítéshez, törléshez, az adatkezelés korlátozásához és az adatok hordozhatóságához való jogát, az adatkezelő számára az azonosítását lehetővé tevő kiegészítő információkat nyújt, a korábban anonimizált adatok ismét személyes adatokká válnak.[179]

Álnevesítés

A személyes adatok olyan jellemzőket tartalmaznak, mint például a név, születési adat, nem, cím vagy egyéb elemek, amelyek alkalmasak arra, hogy tulajdonosukat azonosítsák. A személyes adatok álnevesítése egy olyan folyamat, amely során ezeket a jellemzőket álnevekre cserélik.

Az **uniós jog** az „álnevesítést" a következőképpen határozza meg: „a személyes adatok olyan módon történő kezelése, amelynek következtében további információk felhasználása nélkül többé már nem állapítható meg, hogy a személyes adat mely konkrét természetes személyre vonatkozik, feltéve hogy az ilyen további információt külön tárolják, és technikai és szervezési intézkedések megtételével biztosított, hogy azonosított vagy azonosítható természetes személyekhez ezt a személyes adatot nem lehet kapcsolni"[180]. Az anonimizált adatokkal szemben az álnevesített adatok továbbra is személyes adatoknak minősülnek, és ezért az adatvédelmi szabályok hatálya alá tartoznak. Bár az álnevesítés csökkentheti

178 Európa Tanács, 108. Egyezmény bizottsága (2017), *Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában*, 2017. január 23., 6.2. pont.

179 Általános adatvédelmi rendelet, 11. cikk.

180 *Uo.*, 4. cikk 5. pont.

az érintettek számára a biztonsági kockázatokat, az nem mentesül az általános adatvédelmi rendelet hatálya alól.

Az általános adatvédelmi rendelet az álnevesítés különféle felhasználási módjait az adatvédelmet fokozó technikai intézkedésként ismeri el, és kifejezetten megemlíti az adatkezelés megtervezésével és biztonságával összefüggésben.[181] Ezenfelül egy megfelelő garancia lehet a személyes adatoknak az adatgyűjtés eredeti céljától eltérő célból történő kezelésekor.[182]

Az álnevesítést nem említi kifejezetten az **Európa Tanács** Korszerűsített 108. Egyezménye. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés azonban egyértelműen kimondja, hogy „álnév vagy bármilyen digitális azonosító/digitális személyazonosság használata nem eredményezi az adatok anonimizálását, mivel az érintett továbbra is azonosítható vagy egyéniesíthető marad."[183] Az adatok álnevesítésének egyik módja az adattitkosítás. Miután megtörtént az adatok álnevesítése, egy álnév és egy visszafejtő kulcs formájában megmarad a kapcsolat a személyazonossággal. Ilyen kulcs nélkül nehéz azonosítani az álnevesített adatot. A visszafejtő kulcs használatára jogosultak számára azonban könnyen lehetséges az újbóli azonosítás. A dekódoló kulcsok jogosulatlan személyek általi használata ellen különösen védekezni kell. Ezért, „az [ál]anonimizált adat [...] személyes adatnak minősül [...]" és a Korszerűsített 108. Egyezmény hatálya alá tartozik.[184]

Hitelesítés

A hitelesítés olyan eljárás, amellyel a személy bizonyítani tudja személyazonosságát és/vagy azt, hogy engedéllyel rendelkezik bizonyos dolgokhoz, pl. egy biztonsági területre való belépésre vagy egy bankszámláról pénz kivételére. Hitelesítés elérhető a biometrikus adatok, például útlevélben szereplő fénykép vagy ujjlenyomatok és a pl. határt átlépő személyforgalom ellenőrzésénél megjelenő személy adatainak összehasonlításával;[185] vagy olyan információ elkérésével, amelyet csak egy adott személyazonossággal vagy felhatalmazással rendelkező személy ismer, például személyes azonosító szám (PIN) vagy jelszó; vagy egy meghatározott token felhasználásával, amely kizárólag egy adott személyazonossággal vagy felhatalmazással

181 *Uo.*, 25. cikk (1) bekezdés.

182 *Uo.*, 6. cikk (4) bekezdés.

183 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 18. pont.

184 *Uo.*

185 *Uo.*, 56–57. pont.

rendelkező személy birtokában lehet, például egy egyedi chipkártya vagy banki széf kulcsa. A jelszón vagy chipkártyán kívül az elektronikus aláírás – egyes esetekben a PIN-kóddal együtt – is a személy azonosítására és hitelesítésére alkalmas eszköz lehet az elektronikus kommunikáció során.

2.1.2 Személyes adatok különleges kategóriái

Az **uniós jogban** és az **Európa Tanács jogában** is vannak olyan különleges személyesadat-kategóriák, amelyek kezelésük esetén – jellegüknél fogva – veszélyt jelenthetnek az érintettre nézve, ezért fokozott védelmet igényelnek. Az ilyen adatok tilalom elve alá tartoznak, és korlátozott azon feltételek száma, amelyek mellett ezen adatok kezelése jogszerű.

A Korszerűsített 108. Egyezmény (6. cikk) és az általános adatvédelmi rendelet (9. cikk) keretében a következő kategóriák minősülnek különleges adatnak:

- faji vagy etnikai hovatartozásra vonatkozó személyes adatok;
- politikai véleményre, vallási vagy egyéb világnézeti meggyőződésre – ideértve a filozófiai meggyőződést is – vonatkozó személyes adatok;
- szakszervezeti tagságra utaló személyes adatok;
- a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok;
- az egészségügyi adatok és a szexuális életre vagy szexuális irányultságra vonatkozó személyes adatok.

Példa: A *Bodil Lindqvist* ügy[186] egy olyan internetes oldallal foglalkozott, ahol a különböző személyekre név szerint vagy egyéb módon, például telefonszámmal vagy hobbijukra vonatkozó információkkal hivatkoztak. Az EUB kimondta, hogy „annak feltüntetése, hogy valamely személy lába megsérült, és ezért részleges betegszabadságon van, egészségi állapotra vonatkozó személyes adatnak minősül”.[187]

186 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003. november 6., 51. pont.

187 A korábbi 95/46/EK irányelv 8. cikkének (1) bekezdése, most az általános adatvédelmi rendelet 9. cikkének (1) bekezdése.

Büntetőjogi felelősség megállapítására vonatkozó határozatokhoz és bűncselekményekhez kapcsolódó személyes adatok

A Korszerűsített 108. Egyezmény a személyes adatok különleges kategóriáinak felsorolásában tartalmaz bűncselekményekkel, büntetőeljárásokkal és ítéletekkel kapcsolatos személyes adatokat, illetve kapcsolódó biztonsági intézkedéseket.[188] Az általános adatvédelmi rendelet keretében a büntetőjogi felelősség megállapítására vonatkozó határozatokhoz és bűncselekményekhez kapcsolódó személyes adatokat vagy a kapcsolódó biztonsági intézkedéseket nem említi ilyenként a különleges adatkategóriák listája, azonban azokkal egy külön cikk foglalkozik. Az általános adatvédelmi rendelet 10. cikke kiköti, hogy az ilyen adatok kezelésére kizárólag „abban az esetben kerülhet sor, ha az közhatalmi szerv adatkezelésében történik, vagy ha az adatkezelést az érintett jogai és szabadságai tekintetében megfelelő garanciákat nyújtó uniós vagy tagállami jog lehetővé teszi". Másrészt a büntetőjogi felelősség megállapítására vonatkozó határozatok teljes körű nyilvántartása csak konkrét közhatalmi szerv által végzett adatkezelés keretében történhet.[189] Az EU-ban a személyes adatok bűnüldözéssel összefüggő kezelését egy külön jogi eszköz, az (EU) 2016/680 irányelv szabályozza.[190] Az irányelv különös szabályokat határoz meg az adatvédelem tekintetében, amelyek betartása kötelező az illetékes hatóságok számára a személyes adatok kifejezetten bűncselekmények megelőzése, kivizsgálása, felderítése és büntetőeljárás alá vonása céljából történő kezelése során (lásd a 8.2.1 szakaszt).

2.2 Adatkezelés

Főbb pontok

- „Adatkezelés": a személyes adatokon végzett bármely művelet.
- A „kezelés" az automatizált és nem automatizált adatkezelést is magában foglalja.

188 Korszerűsített 108. Egyezmény, 6. cikk (1) bekezdés.

189 Általános adatvédelmi rendelet, 10. cikk.

190 Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4.

- Az uniós jogban az „adatkezelés" fogalmába a strukturált nyilvántartó rendszerekben való kézi adatkezelés is beletartozik.
- Az Európa Tanács joga értelmében az „adatkezelés" fogalmát a hazai jog a kézi adatkezelésre is kiterjesztheti.

2.2.1 Az adatkezelés fogalma

A személyes adatok kezelésének fogalma **az EU és az Európa Tanács jogában** egyaránt átfogó: „»adatkezelés«: a személyes adatokon [...] végzett bármely művelet [...], így a gyűjtés, rögzítés, rendszerezés, tagolás, tárolás, átalakítás vagy megváltoztatás, lekérdezés, betekintés, felhasználás, közlés továbbítás, terjesztés vagy egyéb módon történő hozzáférhetővé tétel útján, összehangolás vagy összekapcsolás, korlátozás, törlés, illetve megsemmisítés".[191] A Korszerűsített 108. Egyezmény a meghatározást kiegészíti a személyes adatok megőrzésével.[192]

Példa: A *František Ryneš* ügyben[193] F. Ryneš az otthonában ablakokat betörő két személy képmását rögzítette az általa vagyonvédelmi célból telepített CCTV biztonsági rendszerrel. Az EUB azt állapította meg, hogy a személyes adatok rögzítésével és tárolásával járó videokamerás megfigyelés automatikus adatkezelésnek minősül, amely az EU adatvédelmi törvényének hatálya alá tartozik.

Példa: A *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni* ügyben[194] S. Manni azon személyes adatainak törlését kérte egy minősítő cég nyilvántartásából, amelyek összekapcsolták őt egy ingatlanokkal foglalkozó vállalat felszámolásával, és ezáltal rontották hírnevét. Az EUB úgy vélte, hogy „a cégnyilvántartást vezető hatóság azzal, hogy az említett információkat e nyilvántartásba bejegyzi, ott tárolja, és azokat adott esetben kérelemre harmadik felekkel közli, „személyes adatokat kezel", és ezen adatkezelés tekintetében ő az „adatkezelő".

191 Általános adatvédelmi rendelet, 4. cikk 2. pont. Lásd még a Korszerűsített 108. Egyezmény 2. cikkének b) pontját.

192 Korszerűsített 108. Egyezmény, 2. cikk b) pont.

193 EUB, *František Ryneš kontra Úřad pro ochranu osobních údajů*, C-212/13. sz. ügy, 2014. december 11., 25. pont.

194 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017. március 9., 35. pont.

Példa: Munkáltatók adatokat gyűjtenek és kezelnek munkavállalóikról, a munkavállalók fizetésére vonatkozó információkat is beleértve. Ennek jogszerű végzéséhez munkaszerződésük biztosítja a jogalapot.

A munkáltatóknak a személyzet fizetési adatait továbbítaniuk kell az adóhatósághoz. Ez az adattovábbítás a Korszerűsített 108. Egyezmény és az általános adatvédelmi rendelet szerinti értelemben véve szintén „adatkezelésnek" minősül. Az ilyen közzététel jogalapja azonban nem a munkaszerződés. Az adatkezelési műveletekre vonatkozóan további jogalapnak is kell lennie, amelynek eredményeként a fizetési adatokat a munkáltató az adóhatósághoz továbbítja. Ezt a jogalapot általában a nemzeti adójogszabályok rendelkezései tartalmazzák. Ilyen rendelkezések nélkül – és az adatkezelés egyéb jogszerű oka hiányában – a személyes adatok e továbbítása törvénytelen adatkezelésnek minősülne.

2.2.2 Automatizált adatkezelés

A Korszerűsített 108. Egyezmény és az általános adatvédelmi rendelet értelmében az adatvédelem teljeskörűen vonatkozik az automatizált adatkezelésre.

Az **uniós jog** értelmében az automatizált adatkezelés a „személyes adatok részben vagy egészben automatizált módon történő kezelése".[195] A Korszerűsített 108. Egyezmény hasonló meghatározást tartalmaz.[196] Ez gyakorlatilag azt jelenti, hogy a személyes adatok minden automatizált módon, például számítógép, mobiltelefon vagy router segítségével történő kezelésére az EU és az Európa Tanács adatvédelmi szabályai egyaránt kiterjednek.

Példa: A *Bodil Lindqvist* ügy[197] egy olyan internetes oldallal foglalkozott, ahol a különböző személyekre név szerint vagy egyéb módon, például telefonszámmal vagy hobbijukra vonatkozó információkkal hivatkoztak. Az EUB azt állapította meg, hogy „internetes oldalon több személyre történő hivatkozás, és azoknak akár nevükkel, akár más módon – például telefonszámukkal vagy munkakörülményeikre és időtöltésükre vonatkozó

195 Általános adatvédelmi rendelet, 2. cikk (1) bekezdés és 4. cikk 2. pont.

196 Korszerűsített 108. Egyezmény, 2. cikk b) pont; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 21. pont.

197 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003. november 6., 27. pont.

információkkal – történő azonosítása a 95/46 irányelv 3. cikkének (1) bekezdése értelmében »személyes adatok részben vagy egészben automatizált módon való feldolgozásá[nak] [helyesen: kezelésének]« minősül".[198]

Példa: A *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* ügyben[199] M. C. González neve és a Google keresőmotorjának találati listájában megjelenő, társadalombiztosítási tartozások behajtására irányuló ingatlanárverésről szóló két újságcikk közötti kapcsolat törlését vagy módosítását kérte. Az EUB kimondta, hogy „a keresőmotorok az interneten közzétett információk keresése során automatikus, állandó és rendszerezett módon kutatják az internetet, és ezáltal ilyen adatok »gyűjtését« végzik, amelyeket ezt követően ezen indexáló programok keretei között »visszakeresnek«, »rögzítenek« és »rendszereznek«, szervereiken »tárolják«, illetve adott esetben – a keresés találati listájaként – felhasználóikkal »közölnek«, és »hozzáférhetővé tesznek« a számukra."[200] Az EUB azt a következtetést vonta le, hogy az ilyen tevékenységek adatkezelésnek minősülnek, „és nincs jelentősége annak, hogy a keresőmotor működtetője más típusú információkon is végez ugyanilyen műveleteket, és nem tesz különbséget az ilyen információk, illetve a személyes adatok között."

2.2.3 Nem automatizált adatkezelés

A kézi adatkezelésnél is szükség van adatvédelemre.

Az **uniós jog szerinti** adatvédelem semmiképpen sem korlátozódik az automatizált adatkezelésre. Ennek megfelelően az uniós jog értelmében az adatvédelem a manuális nyilvántartási rendszerben, azaz valamilyen strukturált papíralapú nyilvántartásban történő személyesadat-kezelésre is vonatkozik.[201] A strukturált nyilvántartó rendszer olyan rendszer, amely úgy kategorizálja a személyesadat-állományokat, hogy azok bizonyos kritériumok alapján hozzáférhetővé váljanak. Például, ha egy munkáltató papíralapú aktát vezet „munkavállalók szabadságai" címen,

198 Általános adatvédelmi rendelet, 2. cikk (1) bekezdés.

199 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13.

200 *Uo.*, 28. pont.

201 Általános adatvédelmi rendelet, 2. cikk (1) bekezdés.

amely betűrendbe rendezve a személyzet előző évben kivett szabadságaira vonatkozó minden adatot tartalmaz, az akta az uniós adatvédelmi szabályok értelmében kézi nyilvántartási rendszernek minősül. Az adatvédelem ilyen kiterjesztésének okai a következők:

- a papíralapú nyilvántartások szerkezete kialakítható olyan módon, ami lehetővé teszi az információk gyors és könnyű megtalálását;

- személyes adatok strukturált papíralapú nyilvántartásban történő tárolása esetén az automatizált adatfeldolgozásra vonatkozó jogszabályi korlátozások könnyen megkerülhetők.[202]

Az **Európa Tanács joga** szerint azonban az automatizált adatfeldolgozás fogalommeghatározása elismeri, hogy az automatizált műveletek között bizonyos manuális személyesadat-felhasználási lépésekre is szükség lehet.[203] A Korszerűsített 108. Egyezmény 2. cikkének c) pontja kimondja, hogy „(a)mennyiben nem alkalmaznak automatizált adatkezelést, az adatkezelés azon műveletet vagy műveletek összességét jelenti, amelyet a személyes adatokon elvégeznek ilyen, bizonyos kritériumok szerint hozzáférhető vagy visszakereshető strukturált adatállományon belül".

2.3 A személyes adatok felhasználói

Főbb pontok

- Az adatvédelmi rendelet értelmében az a személy, aki meghatározza mások személyes adatai kezelésének módját és célját, az „adatkezelő"; ha ezt a döntést több személy közösen hozza meg, „közös adatkezelőkről" beszélünk.

- Az „adatfeldolgozó" egy természetes vagy jogi személy, aki az adatkezelő nevében személyes adatokat dolgoz fel.

- Az adatfeldolgozó adatkezelővé válik, ha saját maga határozza meg az adatkezelés módját és céljait.

- Minden olyan személy, aki számára személyes adatokat hoznak nyilvánosságra, „címzett".

202 *Uo.*, (15) preambulumbekezdés.

203 Korszerűsített 108. Egyezmény, 2. cikk b) és c) pont.

- Valamely „harmadik fél” az a természetes vagy jogi személy, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak.
- A hozzájárulás, mint a személyes adatok kezelésének jogalapja, az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
- Különleges adatkategóriák beleegyezés alapján történő kezeléséhez kifejezett hozzájárulás szükséges.

2.3.1 Adatkezelők és adatfeldolgozók

Annak, hogy valaki adatkezelőnek vagy adatfeldolgozónak minősül, az a legfontosabb következménye, hogy jogilag felel az adatvédelmi jog értelmében fennálló kötelezettségek betartásáért. A magánszektorban az adatkezelő, illetve az adatfeldolgozó általában természetes vagy jogi személy, a közszférában pedig rendszerint hatóság. Jelentős különbség van az adatkezelő és az adatfeldolgozó között: az előző a kezelés céljait és eszközeit meghatározó természetes vagy jogi személy, míg az utóbbi az a természetes vagy jogi személy, amely az adatkezelő nevében személyes adatokat kezel, szigorú utasítások szerint. Elvben az adatkezelőnek kell ellenőriznie az adatkezelést, és ő tartozik felelősséggel ezért, beleértve a jogi felelősséget is. Ugyanakkor az adatvédelmi szabályok reformjával az adatfeldolgozók immár kötelesek eleget tenni számos, az adatkezelőkre vonatkozó kötelezettségnek. Az általános adatvédelmi rendelet értelmében az adatfeldolgozóknak például nyilvántartást kell vezetniük az adatkezelési tevékenységek minden kategóriájáról a rendelet szerinti kötelezettségeik teljesítésének igazolására.[204] Az adatfeldolgozók emellett kötelesek megfelelő technikai és szervezési intézkedéseket végrehajtani annak érdekében, hogy garantálják az adatkezelés biztonságát,[205] egyes esetekben adatvédelmi tisztviselőt kinevezni[206] és értesíteni az adatkezelőt az adatvédelmi incidensekről.[207]

Az, hogy valamely személy képes-e eldönteni és meghatározni az adatkezelés célját és módját, az adott eset ténybeli elemeitől és körülményeitől függ. Az általános

204 Általános adatvédelmi rendelet, 30. cikk (2) bekezdés.

205 *Uo.*, 32. cikk.

206 *Uo.*, 37. cikk.

207 *Uo.*, 33. cikk (2) bekezdés.

adatvédelmi rendelet adatkezelőre vonatkozó meghatározása szerint bármely természetes személy, jogi személy vagy bármely más szervezet lehet adatkezelő. A 29. cikk szerinti munkacsoport azonban hangsúlyozta, hogy annak érdekében, hogy az egyéneknek az irányelv szerinti jogaik gyakorlásához stabilabb és megbízhatóbb referenciaintézmény álljon rendelkezésükre, „előnyben kell részesíteni azt, hogy egy vállalatot vagy szervet mint egészet tekintsünk adatkezelőnek, és ne a vállalaton vagy szerven belüli egy meghatározott személyt".[208] Például, egy egészségügyi cikkeket orvosoknak értékesítő vállalat az adatkezelő az egy adott területen praktizáló összes orvost tartalmazó forgalmazási lista összeállítása és karbantartása tekintetében, nem pedig az az értékesítő, aki ténylegesen használja és karbantartja a listát.

Példa: Ha a Sunshine vállalat marketing részlege piackutatáshoz adatok feldolgozását tervezi, a szóban forgó feldolgozás tekintetében nem a marketing részleg munkatársai, hanem a Sunshine vállalat lesz az adatkezelő. A marketing részleg nem lehet adatkezelő, mivel nem önálló jogi személy.

Természetes személyek az EU és az Európa Tanács joga alapján egyaránt lehetnek adatkezelők. Azonban másokra vonatkozó adatoknak kizárólag személyes vagy otthoni tevékenység keretében végzett kezelése nem tartozik az általános adatvédelmi rendelet vagy a Korszerűsített 108. Egyezmény szabályainak hatálya alá, és ilyenkor nem minősülnek adatkezelőnek.[209] Az az egyén, aki megőrzi levelezését, a barátokkal és kollégákkal való érintkezését leíró személyes naplóját és a családtagok orvosi papírjait, mentesül az adatvédelmi szabályok alól, mivel ezek a tevékenységek kizárólag személyes vagy otthoni tevékenységnek minősülhetnek. Az általános adatvédelmi rendelet tovább részletezi, hogy a személyes vagy otthoni tevékenység magában foglalhat közösségi hálózatokon történő kapcsolattartást és online tevékenységet is, amikor azokat az ilyen tevékenységek keretében végzik.[210] Ezzel szemben az adatvédelmi szabályok teljeskörűen vonatkoznak azokra az adatkezelőkre és adatfeldolgozókra, akik a személyes adatok ilyen személyes vagy

208 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16.

209 Általános adatvédelmi rendelet, (18) preambulumbekezdés és 2. cikk (2) bekezdés c) pont; Korszerűsített 108. Egyezmény, 3. cikk (1a) bekezdés.

210 Általános adatvédelmi rendelet, (18) preambulumbekezdés.

otthoni tevékenység keretében végzett kezeléséhez az eszközöket biztosítják (például közösségi platformok).[211]

Azzal, hogy a polgárok internet-hozzáféréssel rendelkeznek, és az e-kereskedelmi platformokat, közösségi hálózatokat és blogger oldalakat arra használhatják, hogy önmagukra vonatkozó személyes információkat osszanak meg, egyre nehezebbé válik a személyes célú adatkezelés különválasztása a nem személyes célú adatkezeléstől.[212] Az, hogy a tevékenységek tisztán személyes vagy otthoni tevékenységnek minősülnek-e, az adott körülményektől függ.[213] A szakmai vagy kereskedelmi vonatkozású tevékenységek nem eshetnek az otthoni tevékenységre vonatkozó mentesítés alá.[214] Így tehát amennyiben az adatkezelés mértéke és gyakorisága szakmai vagy teljes munkaidőben végzett tevékenységre utal, a magánszemély adatkezelőnek minősül. Az adatkezelési tevékenység szakmai vagy kereskedelmi jellegén kívül figyelembe kell venni egy másik tényezőt is, mégpedig azt, hogy a személyes adatokat jelentős számú személy számára teszik-e elérhetővé, ezáltal nyilvánvalóan az egyén magánszféráján kívül eső körben. Az adatvédelmi irányelv keretében az ítélkezési gyakorlat azt állapította meg, hogy alkalmazandó az adatvédelmi törvény, ha a magánszemély az internethasználat során nyilvános weboldalon másokról adatokat tesz közzé. Az EUB hasonló tények alapján még nem hozott olyan ítéletet az általános adatvédelmi rendelet értelmében, amely részletesebb iránymutatást nyújtana olyan témák tekintetében, amelyek az otthoni tevékenységekre vonatkozó mentesség értelmében esetleg nem minősülnek az adatvédelmi szabályozás hatálya alá tartozónak, mint például a közösségi média személyes célú használata.

Példa: A *Bodil Lindqvist* ügy[215] egy olyan internetes oldallal foglalkozott, ahol a különböző személyekre név szerint vagy egyéb módon, például telefonszámmal vagy hobbijukra vonatkozó információkkal hivatkoztak. Az EUB fenntartotta, hogy „internetes oldalon több személyre történő

211 *Uo.*, (18) preambulumbekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 29. pont.

212 Lásd a 29. cikk szerinti munkacsoport nyilatkozatát az adatvédelmi reformcsomag körüli vitákra vonatkozóan (2013), *2. melléklet: Proposals and Amendments regarding exemption for personal or household activities (Javaslatok és módosítások a személyes vagy otthoni tevékenységek mentesítése tekintetében)*, 2013. február 27.

213 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 28. pont.

214 Lásd: általános adatvédelmi rendelet, (18) preambulumbekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 27. pont.

215 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003. november 6.

hivatkozás, és azoknak akár nevükkel, akár más módon [...] történő azonosítása a 95/46 irányelv 3. cikkének (1) bekezdése értelmében „személyes adatok részben vagy egészben automatizált módon való feldolgozásá[nak] [helyesen: kezelésének] minősül".[216]

Az ilyen személyesadat-kezelés nem tartozik a kizárólag személyes célra végzett vagy az otthoni tevékenységek közé, amelyek kívül esnek az uniós adatvédelmi szabályok hatályán, mivel ezt a kivételt „úgy kell [...] értelmezni, hogy az kizárólag a magánszemélyek magán- vagy családi élete keretébe tartozó tevékenységekre vonatkozik, nyilvánvalóan nem erről van azonban szó a személyes adatok interneten való közzétételét jelentő olyan feldolgozás esetében, amely során ezen adatok meghatározatlan számú személy számára válnak hozzáférhetővé".[217]

Az EUB véleménye szerint bizonyos körülmények között a magántulajdonban lévő biztonsági kamerák által készített vizuális felvételekre is kiterjedhet az EU adatvédelmi szabályozása.

Példa: A *František Ryneš* ügyben[218] F. Ryneš az otthonában ablakokat betörő két személy képmását rögzítette az általa vagyonvédelmi célból telepített CCTV biztonsági rendszerrel. A felvételeket átadták a rendőrségnek, és azokat felhasználták a büntetőeljárás során.

Az EUB kimondta, hogy „[m]ivel az olyan videokamerás megfigyelés [...] ugyan csak részben, de közterületre is kiterjed, és így a kamerás megfigyelőrendszerrel adatkezelést végző személy magánszféráján kívülre irányul, nem tekinthető [...] kizárólag »személyes, illetve otthoni« tevékenységnek." [219]

216 *Uo.*, 27. pont; a korábbi 95/46/EK irányelv 3. cikkének (1) bekezdése, most az általános adatvédelmi rendelet 2. cikkének (1) bekezdése.

217 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003. november 6., 47. pont.

218 EUB, *František Ryneš kontra Úřad pro ochranu osobních údajů*, C-212/13. sz. ügy, 2014. december 11., 33. pont.

219 A korábbi 95/46/EK irányelv 3. cikke (1) bekezdésének második franciabekezdése, most az általános adatvédelmi rendelet 2. cikke (2) bekezdésének c) pontja.

Adatkezelő

Az **uniós jogban** az adatkezelő az a természetes vagy jogi személy, amely „önállóan vagy másokkal együtt meghatározza a személyes adatok feldolgozásának céljait és módját".[220] Az adatkezelő döntése határozza meg, miért és hogyan történjen az adatok kezelése.

Az **Európa Tanács joga alapján** a Korszerűsített 108. Egyezmény meghatározása szerint az „adatkezelő" „az a természetes vagy jogi személy, közhatalmi szerv, szolgálat, ügynökség vagy bármely egyéb közjogi feladatot ellátó szerv, amely a személyes adatok kezelésének céljait és eszközeit illetően önállóan vagy másokkal együtt döntéshozatali jogkörrel rendelkezik".[221] Az ilyen döntési jogkör kiterjed az adatkezelés céljaira és módjára, valamint a kezelendő adatkategóriákra és az adatokhoz való hozzáférésre.[222] Azt, hogy ez a jogkör jogszabály alapján történő kinevezés vagy a tényleges körülmények eredménye, eseti alapon kell eldönteni.[223]

Példa: A *Google Spain* ügyet[224] egy spanyol állampolgár indította, aki töröltetni akart a Google-ból egy a korábbi pénzügyi helyzetére vonatkozó régi újságcikket.

Az EUB-nek feltették a kérdést, hogy a Google mint a keresőmotor üzemeltetője az adatvédelmi irányelv 2. cikkének d) pontja értelmében vett „adatkezelőnek" minősül-e.[225] Az EUB úgy vélte, hogy az „adatkezelő" fogalmának tág meghatározása arra irányul, hogy az érintetteknek hatékony és teljes védelmet biztosítson.[226] Az EUB megállapította, hogy a keresőmotor üzemeltetője határozta meg a tevékenység céljait és módját, és hogy a weboldalak közzétevői által az internetes oldalakra feltöltött adatokat

220 Általános adatvédelmi rendelet, 4. cikk 7. pont.

221 Korszerűsített 108. Egyezmény, 2. cikk d) pont.

222 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 22. pont.

223 *Uo.*

224 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13.

225 Általános adatvédelmi rendelet, 4. cikk 7. pont; EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 21. pont.

226 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 34. pont.

bármely internethasználó számára elérhetővé teszi, aki az érintett nevére rákeres.[227] Az EUB ezért megállapította, hogy a Google „adatkezelőnek" tekinthető.[228]

Amikor az adatkezelő vagy adatfeldolgozó EU-n kívüli székhellyel rendelkezik, az illető vállalkozásnak írásban ki kell jelölnie egy EU-n belüli képviselőt.[229] Az általános adatvédelmi rendelet kiemeli, hogy a képviselőnek tevékenységi hellyel kell rendelkeznie „az egyik olyan tagállamban, ahol azon érintettek tartózkodnak, akiknek személyes adatait áruknak vagy szolgáltatásoknak a részükre történő nyújtása során kezelik vagy akiknek a magatartását megfigyelik".[230] Ha nincs kijelölt képviselő, akkor is indítható jogi eljárás maga az adatkezelő vagy az adatfeldolgozó ellen.[231]

Közös adatkezelés

Az általános adatvédelmi rendelet rendelkezik arról, hogy amennyiben kettő vagy több adatkezelő közösen határozzák meg az adatkezelés célját és módját, ezek közös adatkezelőknek minősülnek. Ez azt jelenti, hogy ők együtt döntenek adatoknak egy bizonyos közös célból történő kezeléséről.[232] A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kimondja, hogy több adatkezelő vagy társ-adatkezelés is lehetséges **az Európa Tanács keretrendszerén belül**.[233]

A 29. cikk szerinti munkacsoport rámutatott arra, hogy a közös adatkezelésnek különböző formái lehetnek, és hogy a különböző adatkezelők részvétele az adatkezelési tevékenységben eltérő lehet.[234] Az ilyen rugalmasság lehetővé teszi az egyre összetettebb adatkezelési realitások kezelését.[235] A közös adatkezelőknek ezért

227 *Uo.*, 35–40. pont.

228 *Uo.*, 41. pont.

229 Általános adatvédelmi rendelet, 27. cikk (1) bekezdés.

230 *Uo.*, 27. cikk (3) bekezdés.

231 *Uo.*, 27. cikk (5) bekezdés.

232 *Uo.*, 4. cikk 7. pont és 26. cikk.

233 Korszerűsített 108. Egyezmény, 2. cikk d) pont; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 22. pont.

234 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 19. o.

235 *Uo.*

a közöttük létrejött külön megállapodásban kell meghatározniuk a rendelet szerinti kötelezettségek teljesítéséért fennálló felelősségük megoszlását.[236]

A közös adatkezelés az adatkezelési tevékenység tekintetében közös felelősséget eredményez.[237] Az **uniós jog** alapján ez azt jelenti, hogy az érintett hatékony kártalanítása érdekében minden egyes adatkezelő vagy adatfeldolgozó teljes felelősséggel tartozik a közös adatkezelés által okozott teljes kárért.[238]

Példa: Egy több hitelintézet által közösen működtetett, a késedelmes ügyfeleik adatait tartalmazó adatbázis jó példa a közös adatkezelésre. Amikor valaki hitelkérelmet nyújt be egy bankhoz, amely a közös adatkezelők egyike, a bankok az adatbázis segítségével hozhatnak tájékozott döntést az igénylő hitelképességéről.

A törvényi előírások kifejezetten nem mondják ki, hogy a közös adatkezeléshez az is szükséges, hogy mindegyik adatkezelő célja azonos legyen, vagy elég az is, ha céljaik csupán részben átfedik egymást. Jelenleg még nem áll rendelkezésre európai szintű ítélkezési gyakorlat. Az adatkezelőkre és adatfeldolgozókra vonatkozó 2010-es véleményében a 29. cikk szerinti munkacsoport kimondja, hogy a közös adatkezelők vagy közösen határozzák meg az adatkezelés valamennyi célját és módját, vagy csak néhány célt vagy módot, illetve azok egy részét határozzák meg közösen.[239] Míg az első eset egy nagyon szoros, az utóbbi egy lazább kapcsolatot feltételez a különböző szereplők között.

A 29. cikk szerinti munkacsoport a közös adatkezelés fogalmának tágabb értelmezését támogatja azzal a céllal, hogy bizonyos szintű rugalmasságot tegyen lehetővé a jelenlegi adatkezelési valóság egyre növekvő összetettségének kezelésére.[240] A Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaságot (SWIFT) érintő egyik ügy jól szemlélteti a munkacsoport álláspontját.

236 Általános adatvédelmi rendelet, (79) preambulumbekezdés.

237 *Uo.*, 26. cikk.

238 *Uo.*, 82. cikk (4) bekezdés.

239 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 19. o.

240 *Uo.*

Példa: Az úgynevezett SWIFT-ügyben európai bankok banki tranzakciók során történő adattovábbítás elvégzésével bízták meg a SWIFT-et – kezdetben mint adatfeldolgozót. A SWIFT a szóban forgó, egy egyesült államokbeli (USA) számítógépközpontban tárolt banki tranzakciós adatokat felfedte az USA pénzügyminisztériuma felé anélkül, hogy az őt megbízó európai bankok kifejezetten utasították volna erre. A helyzet jogszerűségének értékelése során a 29. cikk szerinti munkacsoport arra a következtetésre jutott, hogy a SWIFT-et megbízó európai bankok és maga a SWIFT is mint közös adatkezelők felelősek az európai ügyfelek felé az utóbbiak adatainak az amerikai hatóságok felé történt felfedéséért.[241]

Adatfeldolgozó

Az **uniós jog** úgy határozza meg az adatfeldolgozót, mint olyan természetes vagy jogi személyt, amely személyes adatokat dolgoz fel az adatkezelő nevében.[242] Az adatfeldolgozóra bízott tevékenységek valamely igen konkrét feladatra vagy összefüggésre is korlátozódhatnak, de általánosak és átfogóak is lehetnek.

Az **Európa Tanács jogában** az adatfeldolgozó fogalma azonos az uniós jog szerinti fogalommal.[243]

Az adatfeldolgozók – a mások számára történő adatkezelésen kívül – a saját céljaikra történő adatkezelés, például saját munkavállalóik, értékesítéseik és elszámolásaik nyilvántartása tekintetében egyben saját jogú adatkezelők is.

Példa: Az Everready vállalat humánerőforrás-adatok kezelése céljából más vállalatok részére végzett adatkezelésre szakosodott. Ebben a minőségében az Everready adatfeldolgozó. Ha azonban az Everready a saját munkavállalói adatait kezeli, a munkáltatói kötelezettségeinek teljesítése céljából végzett adatkezelési műveletek tekintetében adatkezelő.

241 29. cikk szerinti munkacsoport (2006), *10/2006. sz. vélemény a személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozásáról*, WP 128, Brüsszel, 2006. november 22.

242 Általános adatvédelmi rendelet, 4. cikk 8. pont.

243 Korszerűsített 108. Egyezmény, 2. cikk f) pont.

Az adatkezelő és az adatfeldolgozó közötti jogviszony

Ahogy fentebb már láthattuk, az adatkezelő a fogalommeghatározás szerint az a természetes vagy jogi személy, amely meghatározza az adatfeldolgozás céljait és módját. Az általános adatvédelmi rendelet egyértelműen kimondja, hogy az adatfeldolgozó kizárólag az adatkezelő utasítása alapján végezhet adatkezelést, kivéve, ha uniós vagy tagállami jog az adatfeldolgozót arra kötelezi.[244] Az adatkezelő és az adatfeldolgozó közötti szerződés a közöttük lévő jogviszony elengedhetetlen eleme, és törvényi előírás.[245]

> Példa: A Sunshine vállalat igazgatója úgy dönt, hogy a Cloudy vállalat – felhő alapú adattárolásra szakosodott társaság – kezelje a Sunshine ügyféladatait. A Sunshine vállalat marad az adatkezelő, és a Cloudy vállalat kizárólag adatfeldolgozó lesz, mivel a szerződés értelmében a Cloudy vállalat a Sunshine társaság ügyféladatait kizárólag a Sunshine által meghatározott célokra használhatja fel.

Ha az adatkezelés módjának meghatározására vonatkozó jogkört az adatfeldolgozóra ruházzák, az adatkezelőnek ettől még megfelelő szintű ellenőrzést kell tudni gyakorolni az adatfeldolgozónak az adatkezelés módjára vonatkozó döntései felett. A végső felelősség továbbra is az adatkezelőé, akinek felügyelnie kell az adatfeldolgozókat annak biztosítása érdekében, hogy döntéseik megfeleljenek az adatvédelmi jognak és saját utasításainak.

Ezenkívül, ha az adatfeldolgozó nem tartja tiszteletben az adatkezelő által az adatkezelésre vonatkozóan előírt feltételeket, a feldolgozó legalábbis az adatkezelő utasításai megszegésének erejéig adatkezelővé válik. Ez minden valószínűség szerint jogellenesen eljáró adatkezelővé teszi a feldolgozót. Az eredeti adatkezelőnek viszont meg kell magyaráznia, hogyan volt lehetséges, hogy a feldolgozó megszegje megbízatását.[246] A 29. cikk szerinti munkacsoport csakugyan hajlamos az ilyen helyzetekben közös adatkezelést feltételezni, mivel ez eredményezi az érintettek érdekének legjobb védelmét.[247]

244 Általános adatvédelmi rendelet, 29. cikk.

245 *Uo.*, 28. cikk (3) bekezdés.

246 *Uo.*, 82. cikk (2) bekezdés.

247 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 25. o.; 29. cikk szerinti munkacsoport (2006), *10/2006. sz. vélemény a személyes adatok Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi feldolgozásáról*, WP 128, Brüsszel, 2006. november 22.

A felelősség megosztásával kapcsolatban is lehetnek kérdések, ha az adatkezelő kisvállalkozás, a feldolgozó pedig egy nagyvállalat, amely elég erős ahhoz, hogy diktálja a szolgáltatására vonatkozó feltételeket. Ilyen körülmények között azonban a 29. cikk szerinti munkacsoport fenntartja, hogy a felelősség mértéke a gazdasági egyensúly hiánya miatt nem csökkenthető, és az adatkezelő fogalmának értelmét meg kell tartani.[248]

Az egyértelműség és átláthatóság kedvéért, az adatkezelő és az adatfeldolgozó közötti jogviszony részleteit írásbeli szerződésben kell szabályozni.[249] A szerződésnek tartalmaznia kell különösen az adatkezelés tárgyát, jellegét, célját és időtartamát, a személyes adatok típusát és az érintettek kategóriáit. Ebben ki kell kötni az adatkezelő és adatfeldolgozó kötelezettségeit és jogait is, például a titoktartásra és biztonságra vonatkozó előírásokat. Az ilyen szerződés hiánya az adatkezelőnek a kölcsönös felelősségek írásos dokumentációjára vonatkozó kötelezettsége megszegésének minősül, és szankciókat vonhat maga után. Nemcsak az adatkezelő tartozik felelősséggel azokban az esetekben, amikor az adatfeldolgozó az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el és ennek eredményeképp kárt okozott, hanem maga az adatfeldolgozó is.[250] Az adatfeldolgozó köteles nyilvántartást vezetni az adatkezelő nevében végzett adatkezelési tevékenységek minden kategóriájáról.[251] Ezt a nyilvántartást megkeresés alapján a felügyeleti hatóság részére rendelkezésére bocsátja, mivel az adatkezelő és adatfeldolgozó egyaránt köteles együttműködni a hatósággal feladata teljesítése során.[252] Az adatkezelőnek, illetve az adatfeldolgozónak lehetősége van csatlakozni egy jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz annak bizonyítására, hogy teljesíti az általános adatvédelmi rendeletben foglalt követelményeket.[253]

Előfordulhat, hogy az adatfeldolgozók bizonyos feladatokat további feldolgozókkal szeretnének elvégeztetni. Ez jogilag megengedett, amennyiben megfelelő szerződéses kikötések létesültek az adatkezelő és az adatfeldolgozó között, többek között arra vonatkozóan, hogy az adatkezelő engedélye szükséges-e minden egyes esetben, vagy a puszta tájékoztatás is elegendő. Az általános adatvédelmi rendelet

248 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 26. o.

249 Általános adatvédelmi rendelet, 28. cikk (3) bekezdés és 9. cikk.

250 *Uo.*, 82. cikk (2) bekezdés.

251 *Uo.*, 30. cikk (2) bekezdés.

252 *Uo.*, 30. cikk (4) és (31) bekezdés.

253 *Uo.*, 28. cikk (5) és 42. cikk (4) bekezdés.

kiköti, hogy ha a további adatfeldolgozó nem teljesíti adatvédelmi kötelezettségeit, az eredeti adatfeldolgozó tartozik teljes felelősséggel az adatkezelő felé.[254]

Az **Európa Tanács joga** alapján az adatkezelő és adatfeldolgozó a fent kifejtettek szerinti fogalmának értelmezése teljeskörűen alkalmazandó.[255]

2.3.2 Címzettek és harmadik felek

A személyek vagy szervezetek – az adatvédelmi irányelv által bevezetett – e két kategóriája közötti különbség elsősorban az adatkezelővel fennálló jogviszonyukban, valamint ebből következően az adatkezelő által kezelt személyes adatokhoz való hozzáférési jogosultságukban rejlik.

A „harmadik fél" az adatkezelőtől és az adatfeldolgozótól különböző személy. Az általános adatvédelmi rendelet 4. cikkének 10. pontja szerint a harmadik fél „az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, amely nem azonos az érintettel, az adatkezelővel, az adatfeldolgozóval vagy azokkal a személyekkel, akik az adatkezelő vagy adatfeldolgozó közvetlen irányítása alatt a személyes adatok kezelésére felhatalmazást kaptak". Ez azt jelenti, hogy az adatkezelőtől különböző szervezetnél dolgozó személyek – akkor is, ha a szervezet az adatkezelővel azonos vállalatcsoporthoz vagy holdinghoz tartozik – „harmadik félnek" minősülnek (vagy harmadik félhez tartoznak). Másrészről, az ügyfelek számláit vezető, a központ közvetlen irányítása alatt álló bankfiókok nem minősülnek „harmadik félnek".[256]

A „címzett" a „harmadik félnél" tágabb fogalom. Az általános adatvédelmi rendelet 4. cikkének 9. pontja értelmében a címzett „az a természetes vagy jogi személy, közhatalmi szerv, ügynökség vagy bármely egyéb szerv, akivel vagy amellyel a személyes adatot közlik, függetlenül attól, hogy harmadik fél-e". A címzett vagy az adatkezelőn és a feldolgozón kívüli személy (azaz harmadik fél), vagy az adatkezelőn vagy a feldolgozón belüli személy, például az adott vállalat vagy hatóság munkavállalója vagy egy másik részlege.

254 *Uo.*, 28. cikk (4) bekezdés.

255 Lásd például: Korszerűsített 108. Egyezmény, 2. cikk b) és f) pont; a profilalkotásra vonatkozó ajánlás, 1. cikk.

256 29. cikk szerinti munkacsoport (2010), *1/2010. sz. vélemény az „adatkezelő" és az „adatfeldolgozó" fogalmáról*, WP 169, Brüsszel, 2010. február 16., 31. o.

A címzettek és a harmadik felek megkülönböztetése kizárólag az adatok jogszerű közlésének feltételei szempontjából fontos. Az adatkezelő vagy -feldolgozó alkalmazottai minden további jogi követelmény nélkül a személyes adatok címzettjeinek minősülnek, ha részt vesznek az adatkezelő vagy -feldolgozó adatkezelési műveleteiben. Ellenben a harmadik fél, aki az adatkezelőtől és adatfeldolgozótól különálló személy, nem jogosult az adatkezelő által kezelt személyes adatok felhasználására – kivéve, ha konkrét esetben konkrét jogalap áll fenn.

Példa: Egy adatkezelő alkalmazottja, aki a munkáltatója által rábízott feladatok keretében személyes adatokat használ, az adatok címzettje, de nem harmadik fél, mivel az adatkezelő nevében vagy utasításai alapján használja az adatokat. Ha például egy munkáltató munkavállalóira vonatkozó személyes adatokat közöl az emberi erőforrás osztállyal a közelgő teljesítményértékelés céljából, az emberi erőforrás osztály a személyes adatok címzettjévé válik, mivel a személyes adatokat az adatkezelő számára végzett adatkezelés során közölték az osztállyal.

Ha azonban a szervezet a munkavállalóira vonatkozó adatokat egy képzési szolgáltatásokat nyújtó társasággal közli, amely az adatokat arra használja fel, hogy a képzési programot a munkavállalói igényekhez, szükségletekhez igazítsa, ez a társaság harmadik félnek minősül. Ennek az az oka, hogy a képzési szolgáltatásokat nyújtó vállalat nem rendelkezik konkrét legitimációval vagy engedéllyel (amely az „emberi erőforrás" esetében az adatkezelővel fennálló jogviszonyból ered) e személyes adatok kezeléséhez. Más szavakkal, az adatokat nem az adatkezelővel fennálló munkaviszonyuk keretében kapták.

2.4 Hozzájárulás

Főbb pontok

- A hozzájárulás, mint a személyes adatok kezelésének jogalapja, az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítása, amellyel az érintett nyilatkozat vagy a megerősítést félreérthetetlenül kifejező cselekedet útján jelzi, hogy beleegyezését adja az őt érintő személyes adatok kezeléséhez.
- A különleges adatkategóriák kezeléséhez kifejezett hozzájárulás szükséges.

A 4. fejezetben részletesen tárgyaltak szerint a hozzájárulás egyike azon hat jogszerű oknak, amelyek alapján személyes adatokat lehet kezelni. A hozzájárulás „az érintett akaratának önkéntes, konkrét és megfelelő tájékoztatáson alapuló és egyértelmű kinyilvánítását" jelenti.[257]

Az **uniós jog** számos elemet határoz meg ahhoz, hogy a hozzájárulás érvényes legyen; ezek célja annak garantálása, hogy az érintettek valóban bele akartak egyezni adataik adott felhasználásába:[258]

- Az adatkezelésre csak akkor kerülhet sor, ha az érintett egyértelmű megerősítő cselekedettel önkéntes, konkrét, tájékoztatáson alapuló és egyértelmű hozzájárulását adja a természetes személyt érintő személyes adatok kezeléséhez. A hozzájárulás történhet cselekedet vagy nyilatkozat útján.

- Az érintettnek kell, hogy legyen joga bármikor visszavonni a hozzájárulását.

- Az olyan írásos nyilatkozatok összefüggésében, amelyek egyéb ügyekkel is foglalkoznak, például a „szolgáltatási feltételekkel", a hozzájárulásra irányuló felkérést világosan és közérthetően kell megfogalmazni, érthető és könnyen hozzáférhető formában és az egyéb ügyektől egyértelműen megkülönböztethető módon kell előadni; ha ennek a nyilatkozatnak egy része sérti az általános adatvédelmi rendeletet, az nem lehet kötelező erejű.

A hozzájárulás az adatvédelmi törvény összefüggésében csak akkor érvényes, ha valamennyi fenti követelményt teljesíti. Az adatkezelő felelőssége annak igazolása, hogy az érintett hozzájárult személyes adatainak kezeléséhez.[259] Az érvényes hozzájárulás elemeit részletesen a személyes adatok kezelésének jogalapjaival foglalkozó 4.1.1 szakasz tárgyalja.

A 108. Egyezmény nem tartalmaz meghatározást a hozzájárulásra vonatkozóan – azt a nemzeti jogszabályokra hagyja. Az **Európa Tanács joga** szerint azonban az érvényes hozzájárulás elemei megegyeznek a korábban ismertetettekkel.[260]

257 Általános adatvédelmi rendelet, 4. cikk 11. pont. Lásd még a Korszerűsített 108. Egyezmény 5. cikkének (2) bekezdését.

258 Általános adatvédelmi rendelet, 7. cikk.

259 *Uo.*, 7. cikk (1) bekezdés.

260 Korszerűsített 108. Egyezmény, 5. cikk (2) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42–45. pont.

Az érvényes hozzájárulásra vonatkozó polgári jogi kiegészítő követelmények, például a jogképesség, természetesen az adatvédelemmel kapcsolatban is alkalmazandók, mivel e követelmények alapvető jogi előfeltételek. A jogképességgel nem rendelkező személyek érvénytelen hozzájárulása esetén hiányzik a jogalap e személyek adatainak feldolgozásához. A kiskorúak szerződéskötésre irányuló cselekvőképességét illetően az általános adatvédelmi rendelet úgy rendelkezik, hogy az érvényes hozzájárulás megszerzéséhez szükséges minimális életkorra vonatkozó szabályai nem érintik a tagállamok általános szerződési jogát.[261]

A hozzájárulást egyértelmű módon kell megadni, hogy nem maradjon kétség az érintett szándékát illetően.[262] Ha különleges adatok kezeléséről van szó, a hozzájárulásnak kifejezettnek kell lennie, és szóban vagy írásban is megadható.[263] Ez utóbbi elektronikus formában is megtehető.[264] Mind ez **EU**, mind pedig az **Európa Tanács** joga szerint a személyes adatok kezeléséhez való hozzájárulást nyilatkozattal vagy egyértelmű megerősítő cselekedettel kell megadni.[265] Így tehát hozzájárulás nem szerezhető meg hallgatás, előre bejelölt négyzetek vagy nem cselekvés útján.[266]

261 Általános adatvédelmi rendelet, 8. cikk (3) bekezdés.

262 *Uo.*, 6. cikk (1) bekezdés a) pont és 9. cikk (2) bekezdés a) pont.

263 *Uo.*, (32) preambulumbekezdés.

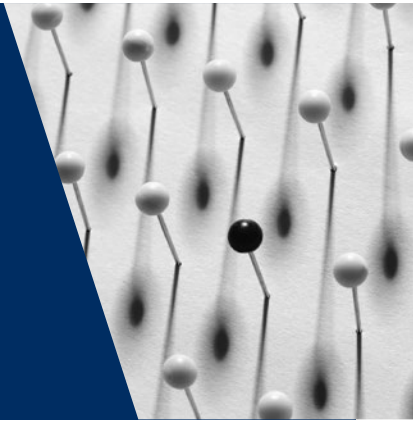
264 *Uo.*

265 *Uo.*, 4. cikk 11. pont; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

266 Általános adatvédelmi rendelet, (32) preambulumbekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

3

Az európai adatvédelmi jog alapelvei



EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont	**A jogszerűség elve**	Korszerűsített 108. Egyezmény, 5. cikk (3) bekezdés
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont	**A tisztességes eljárás elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés a) pont EJEB, *K.H. és társai kontra Szlovákia*, 32881/04. sz. ügy, 2009
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont EUB, *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015	**Az átláthatóság elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés a) pont és 8. cikk EJEB, *Haralambie kontra Románia*, 21737/03. sz. ügy, 2009
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés b) pont	**A célhoz kötöttség elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés b) pont
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés c) pont EUB, *Digital Rights Ireland* és *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014	**Az adattakarékosság elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés c) pont

EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés d) pont EUB, *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer*, C-553/07. sz. ügy, 2009	**Az adatok pontosságának elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés d) pont
Általános adatvédelmi rendelet, 5. cikk (1) bekezdés e) pont EUB, *Digital Rights Ireland és Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014	**A korlátozott tárolhatóság elve**	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés e) pont EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008
Általános adatvédelmi rendelet, 5.cikk (1) bekezdés f) pont és 32. cikk	**Az adatbiztonság (integritás és bizalmas jelleg) elve**	Korszerűsített 108. Egyezmény, 7. cikk
Általános adatvédelmi rendelet, 5. cikk (2) bekezdés	**Az elszámoltathatóság elve**	Korszerűsített 108. Egyezmény, 10. cikk

Az általános adatvédelmi rendelet 5. cikke megállapítja a személyes adatok kezelésére vonatkozó elveket. Ezek az elvek a következők:

- jogszerűség, tisztességes eljárás és átláthatóság;
- célhoz kötöttség;
- adattakarékosság;
- az adatok pontossága;
- korlátozott tárolhatóság;
- integritás és bizalmas jelleg.

Az elvek kiindulási pontként szolgálnak a rendelet következő cikkeiben megfogalmazott részletesebb rendelkezésekhez. Ezek megjelennek a Korszerűsített 108. Egyezmény 5., 7., 8 és 10. cikkeiben is. Valamennyi Európa tanácsi vagy uniós szintű adatvédelmi jogszabálynak meg kell felelnie ezeknek az elveknek, és a jogszabályok értelmezésénél is tekintetbe kell venni őket. Az uniós jog értelmében az adatkezelési elvek korlátozásai kizárólag annyiban megengedettek, ha azok

megfelelnek a 12–22. cikkekben megállapított jogoknak és kötelezettségeknek, és tiszteletben tartják az alapvető jogok és szabadságok lényeges tartalmát. Ezen alapelvek alóli mentességről, illetve az elvek korlátozásáról uniós vagy nemzeti szinten kell rendelkezni;[267] törvényes célt kell szolgálniuk és szükségesnek és arányosnak kell lenniük egy demokratikus társadalomban.[268] Mindhárom feltételnek egyaránt teljesülnie kell.

3.1 A jogszerűség, tisztességes eljárás és átláthatóság elve az adatkezelésben

Főbb pontok

- A jogszerűség, tisztességes eljárás és átláthatóság elve valamennyi adatkezelési tevékenységre vonatkozik.
- Az általános adatvédelmi rendelet értelmében a jogszerűséghez a következők valamelyike szükséges:
  - az érintett hozzájárulása;
  - a szerződéskötés szükségessége;
  - jogszabályi kötelezettség;
  - az érintett vagy más személy létfontosságú érdekei védelmének szükségessége;
  - közérdekből elvégzendő feladat végrehajtásának szükségessége;
  - az adatkezelő vagy valamely harmadik fél jogos érdekének szükségessége, ha az érintett érdekei és jogai nem élveznek elsőbbséget.
- A személyesadat-kezelést tisztességes módon kell végezni.
  - Az érintettet tájékoztatni kell a kockázatokról annak biztosítása érdekében, hogy az adatkezelésnek ne legyenek előre nem látható negatív hatásai.
- A személyesadat-kezelést átlátható módon kell végezni.
  - Az adatkezelést megelőzően az adatkezelőknek tájékoztatniuk kell az érintetteket többek között az adatkezelés céljáról és az adatkezelő kilétéről és címéről.

267 Korszerűsített 108. Egyezmény, 11. cikk (1) bekezdés; általános adatvédelmi rendelet, 23. cikk (1) bekezdés.

268 Általános adatvédelmi rendelet, 23. cikk (1) bekezdés.

- Az adatkezelési műveletekre vonatkozó tájékoztatást világosan és közérthetően kell megfogalmazni, hogy az érintettek könnyen megértsék a szabályokat, kockázatokat, biztosítékokat és az érintett jogokat.
- Az érintettek az adatkezelés helyén hozzáférhetnek adataikhoz.

3.1.1 Az adatkezelés jogszerűsége

Az **uniós és Európa tanácsi adatvédelmi törvények** előírják a személyes adatok jogszerű kezelését.[269] A jogszerű adatkezeléshez szükséges az érintett hozzájárulása vagy az adatvédelmi jogszabályokban meghatározott más jogszerű ok.[270] Az általános adatvédelmi rendelet 6. cikkének (1) bekezdése a hozzájáruláson kívül az adatkezelés öt jogalapját említi, vagyis a személyes adatok kezelése szerződés teljesítéséhez, közhatalmi jogosítvány gyakorlásának keretében végzett feladat végrehajtásához, jogszabályi kötelezettség teljesítéséhez, az adatkezelő vagy egy harmadik fél jogos érdekeinek érvényesítéséhez, illetve az érintett létfontosságú érdekeinek védelme miatt szükséges. Ezt részletesebben a 4.1 szakasz tárgyalja.

3.1.2 Tisztességes adatkezelés

A jogszerű adatkezelés mellett az uniós és Európa tanácsi adatvédelmi törvények előírják a személyes adatok tisztességes kezelését is.[271] A tisztességes adatkezelés elve elsősorban az adatkezelő és az érintett közötti jogviszonyra vonatkozik.

Az adatkezelőknek tájékoztatniuk kell az érintetteket és a nyilvánosságot arról, hogy az adatokat jogszerűen és átlátható módon fogják kezelni, és tudniuk kell igazolni, hogy az adatkezelési műveletek megfelelnek az általános adatvédelmi rendelet előírásainak. Az adatkezelési műveleteket tilos titokban végezni, és az érintetteknek tisztában kell lenniük a lehetséges kockázatokkal. Az adatkezelőknek továbbá – amennyire lehetséges – úgy kell eljárniuk, hogy azonnal teljesítsék az érintettek kéréseit, különösen ha hozzájárulásuk jelenti az adatkezelés jogalapját.

269 Korszerűsített 108. Egyezmény, 5. cikk (3) bekezdés; általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont.

270 Az Európai Unió Alapjogi Chartája, 8. cikk (2) bekezdés; általános adatvédelmi rendelet, (40) preambulumbekezdés és 6–9. cikk; Korszerűsített 108. Egyezmény, 5. cikk (2) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 41. pont.

271 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont; Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés a) pont.

Példa: A *K.H. és társai kontra Szlovákia* ügyben[272] a felpereseket – roma származású nőket – két kelet-szlovákiai kórházban kezelték terhességük és szülésük során. Később egyikük sem tudott teherbe esni, többszöri kísérletre sem. A nemzeti bíróságok elrendelték, hogy a kórházak engedélyezzék a felperesek és képviselőik számára, hogy konzultáljanak és készítsenek írásos kivonatokat a kórlapokról, de – állítólag a visszaélés megelőzése érdekében – elutasították a dokumentumok fénymásolására irányuló kérésüket. Az államoknak az EJEE 8. cikke alapján fennálló pozitív kötelezettségei feltétlenül magukban foglalják azt a kötelezettséget is, hogy az érintettnek másolatot adjanak a saját adatállományáról. Az államnak kellett volna meghatároznia a személyesadat-állományok fénymásolására vonatkozó intézkedéseket, illetve adott esetben megjelölnie az elutasítás kényszerű indokait. A felperesek ügyében a hazai bíróságok elsősorban a vonatkozó információk visszaéléssel szembeni védelmének szükségességével indokolták a kórlapok fénymásolásának megtiltását. Az EJEB azonban nem látta be, hogyan tudtak volna az alperesek, akik mindenképpen hozzáférhettek teljes orvosi kartonjukhoz, visszaélni a saját magukra vonatkozó információkkal. Ezenfelül a visszaélés kockázata a fénymásolatok alperesektől való megtagadásán kívül más eszközökkel – például a kórlapokhoz való hozzáférésre jogosult személyek körének korlátozásával – is kivédhető lett volna. Az állam nem tudott kellően kényszerítő okokat kimutatni ahhoz, hogy az alperesektől megtagadják az egészségi állapotukkal kapcsolatos információkhoz való tényleges hozzáférést. A Bíróság arra a következtetésre jutott, hogy megsértették a 8. cikket.

Internetes szolgáltatásokkal kapcsolatban az adatkezelő rendszerek tulajdonságainak lehetővé kell tenniük, hogy az érintettek valóban megtudják, mi történik az adataikkal. Mindenesetre a tisztességes eljárás elve túlmutat az átláthatóságra vonatkozó kötelezettségeken, és összekapcsolható a személyes adatok etikus kezelésével is.

Példa: Egy egyetemi kutatóosztály kísérletet folytat 50 alany hangulatváltozásának elemzésével. Az alanyoknak egy elektronikus fájlban kell rögzíteniük gondolataikat óránként, egy adott időpontban. Az 50 személy hozzájárulását adta ehhez a konkrét projekthez és adataiknak

272 EJEB, *K.H. és társai kontra Szlovákia*, 32881/04. sz. ügy, 2009. április 28.

az egyetem által történő e sajátos felhasználásához. A kutatóosztály hamar felfedezi, hogy a gondolatok elektronikus naplózása nagyon hasznos lehet egy másik, a mentális egészséggel foglalkozó és egy másik csoport által koordinált projekt számára. Annak ellenére, hogy adatkezelőként az egyetem ugyanazokat az adatokat a szóban forgó adatok kezelése jogszerűségének biztosításához szükséges további intézkedés nélkül felhasználhatta volna egy másik csapata munkájához, feltéve, hogy az adatkezelési célok összeegyeztethetők, az egyetem tájékoztatta az érintetteket, és kutatásokra vonatkozó etikai kódexét és a tisztességes adatkezelés elvét betartva új hozzájárulást kért.

3.1.3 Az adatkezelés átláthatósága

Az uniós és Európa tanácsi adatvédelmi törvények előírják, hogy a személyes adatok feldolgozását „az érintett számára átlátható módon kell végezni".[273]

Ez az elv egy kötelezettséget keletkeztet az adatkezelő számára, hogy tegyen meg minden megfelelő intézkedést annak érdekében, hogy tájékoztassa az érintetteket – akik lehetnek felhasználók, vásárlók vagy ügyfelek – adataik felhasználásának módjáról.[274] Az átláthatóság vonatkozhat az egyén számára az adatkezelés megkezdése előtt adott tájékoztatásra,[275] magára a tájékoztatásra, amelynek az adatkezelés során az érintettek számára könnyen hozzáférhetőnek kell lennie,[276] de vonatkozhat az érintettek számára a saját adataikhoz való hozzáférésre irányuló kérést követően adott tájékoztatásra.[277]

Példa: A *Haralambie kontra Románia* ügyben[278] a felperes csak öt évvel kérelmének benyújtása után kapott hozzáférést a titkosszolgálat által róla tárolt adatokhoz. Az EJEB ismételten rámutatott, hogy azon egyéneknek, akikről állami hatóságok személyes aktát tárolnak, elemi érdeke fűződik ahhoz, hogy hozzáférhessenek a szóban forgó adatállományhoz. A hatóságoknak az információkhoz való hozzáférés megszerzésével

273 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés a) pont; Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés a) pont és 8. cikk.

274 Általános adatvédelmi rendelet, 12. cikk.

275 *Uo.*, 13. cikk (4) és (14) bekezdés.

276 29. cikk szerinti munkacsoport, *2/2017. sz. vélemény a munkahelyi adatkezelésről*, *23. o.*

277 Általános adatvédelmi rendelet, 15. cikk.

278 EJEB, *Haralambie kontra Románia*, 21737/03. sz. ügy, 2009. október 27.

kapcsolatban hatékony eljárásról kellett volna rendelkezniük. Az EJEB úgy vélte, hogy sem a továbbított adatállományok mennyisége, sem az irattári rendszer hiányosságai nem indokolnak ötéves késedelmet a felperesi kérelem megadása tekintetében. A hatóságok nem biztosítottak a felperesnek hatékony és elérhető eljárást arra, hogy észszerű időn belül hozzáférést szerezhessen személyes adatainak állományához. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az adatkezelési műveleteket könnyen érthető módon el kell magyarázni az érintetteknek, hogy megértsék, mi történik adataikkal. Ez azt jelenti, hogy az érintettnek a személyes adatok gyűjtése pillanatában tisztában kell lennie a személyes adatok kezelésének konkrét céljával.[279] Az adatkezelés átláthatósága megkívánja, hogy világos és közérthető nyelvezetet használjanak.[280] Az érintett személyek számára egyértelműnek kell lenni, hogy személyes adataik kezelése milyen kockázatokkal jár, és milyen szabályok, biztosítékok és jogok vonatkoznak az adatkezelésre.[281]

Az **Európa Tanács joga** szintén kimondja, hogy az adatkezelő köteles bizonyos lényeges tájékoztatást proaktív módon megadni az érintettek számára. Az adatkezelő (vagy társadatkezelők) nevével és címével, az adatkezelés jogalapjával, a kezelt adatkategóriákkal és címzettekkel, valamint a jogok gyakorlásának módjával kapcsolatos tájékoztatás bármilyen megfelelő formában (vagy weboldalon keresztül, a személyes készülékeken technológiai eszközök segítségével) megadható mindaddig, amíg a az érintett tisztességes és hatékony tájékoztatásban részesül. A tájékoztatásnak könnyen hozzáférhetőnek, olvashatónak és érthetőnek kell lennie, és a vonatkozó érintettekre kell igazítani (például gyerekbarát nyelvezetű legyen, amennyiben ez szükséges). Meg kell adni minden további információt is, amely szükséges a tisztességes adatkezelés biztosításához, vagy amely az adott cél szempontjából hasznos, például a megőrzési idő, az adatkezelés alapjául szolgáló indoklás ismerete, vagy másik félhez vagy harmadik személyhez történő adattovábbításra vonatkozó információk (függetlenül attól, hogy az adott harmadik személy megfelelő szintű védelmet biztosít-e, illetve az adatkezelő által a megfelelő szintű adatvédelem garantálására tett intézkedésektől). [282]

279 Általános adatvédelmi rendelet, (39) preambulumbekezdés.

280 *Uo.*

281 *Uo.*

282 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 68. pont.

A hozzáférési jog értelmében[283] az érintett jogosult, hogy kérésére az adatkezelőtől visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és ha igen milyen személyes adatok kezelése van folyamatban.[284] Ezenkívül a tájékoztatáshoz való jog értelmében[285] azokat a személyeket, akikre vonatkozó adatok kezelése folyamatban van, az adatkezelőknek vagy adatfeldolgozóknak proaktívan tájékoztatniuk kell többek között az adatkezelés céljáról, időtartamáról, módjáról, elvben az adatkezelési tevékenység megkezdése előtt.

Példa: A *Smaranda Bara és társai kontra Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală és társai* ügy[286] azzal foglalkozott, hogy a nemzeti adóigazgatási ügynökség egyéni vállalkozók jövedelmével kapcsolatos adóügyi adatokat továbbított a román nemzeti egészségbiztosítási pénztár felé, amely alapján a pénztár egészségbiztosítási járulékhátralék megfizetését követelte. Az EUB-t annak megállapítására kérték, hogy az érintetteknek kellett-e volna előzetes tájékoztatást kapniuk az adatkezelő kilétéről és az adatok továbbításának céljáról a szóban forgó adatok nemzeti egészségbiztosítási pénztár általi kezelése előtt. Az EUB azt állapította meg, hogy amennyiben valamely tagállam egyik közigazgatási szerve egy másik közigazgatási szerv felé továbbít személyes adatokat, amely tovább kezeli az érintett adatokat, az érintetteket tájékoztatni kell az adattovábbításról, illetve adatkezelésről.

Egyes esetekben megengedettek eltérések az érintettek adatkezelésről való tájékoztatásának kötelezettségétől; ezeket részletesebben az érintettek jogaival foglalkozó 6.1 szakasz tárgyalja.

3.2 A célhoz kötöttség elve

Főbb pontok

- Az adatkezelés célját még az adatkezelés megkezdése előtt meg kell határozni.

283 Általános adatvédelmi rendelet, 15. cikk.

284 Korszerűsített 108. Egyezmény, 8. cikk és 9. cikk (1) bekezdés b) pont.

285 Általános adatvédelmi rendelet, 13. és 14. cikk.

286 EUB, *Smaranda Bara és társai kontra Casa Naţională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015. október 1., 28–46. pont.

- Nem kerülhet sor az adatok további kezelésére az eredeti céllal nem összeegyeztethető módon, bár az általános adatvédelmi rendelet lehetőséget biztosít e szabály alóli kivételekre közérdekből történő archiválási célból, tudományos vagy történelmi kutatási, valamint statisztikai célból.
- A célhoz kötöttség elve lényegében azt jelenti, hogy a személyes adatok bármely kezelését konkrét, jól meghatározott célból kell végezni, és kizárólag olyan további, meghatározott célokból, amelyek az eredeti céllal összeegyeztethetők.

A célhoz kötöttség elve az európai adatvédelmi jog alapelveinek egyike. Erősen kapcsolódik az átláthatósághoz, kiszámíthatósághoz és felhasználói ellenőrzéshez: ha az adatkezelés célja kellően konkrét és világos, az egyének tisztában lesznek azzal, mire számíthatnak, és fokozódik az átláthatóság, valamint a jogbiztonság. Ugyanakkor a cél világos meghatározása fontos annak érdekében, hogy az érintettek hatékonyan gyakorolhassák jogaikat, például az adatkezelés elleni tiltakozáshoz való jogot.[287]

Az elv előírja, hogy a személyes adatok bármely kezelése konkrét, jól meghatározott célból történjen, és kizárólag olyan további, meghatározott célokból, amelyek az eredeti céllal összeegyeztethetők.[288] Személyes adatok meg nem határozott és/vagy korlátlan célokra való kezelése jogellenes. A személyes adatok meghatározott cél nélküli kezelése abból a megfontolásból, hogy valamikor a jövőben majd jó lehet, szintén nem jogszerű. A személyes adatok kezelésének jogszerűsége függ az adatkezelés céljától, amelynek kifejezettnek, konkrétnak és jogszerűnek kell lennie.

Minden új, az eredetivel nem összeegyeztethető személyesadat-kezelési célhoz saját konkrét jogalapnak kell tartoznia; nem lehet arra hivatkozni, hogy az adatokat eredetileg más jogszerű célra szerezték be vagy kezelték. Másrészt a jogszerű adatkezelés az eredetileg megjelölt célra korlátozódik, minden új kezelési célhoz külön új jogalap szükséges. Például, személyes adatok harmadik felekkel való közlését új célból különösen gondosan kell mérlegelni, mivel az ilyen közlés rendszerint további, az adatgyűjtéshez használttól eltérő jogalapnak minősül.

Példa: Egy légitársaság a járat megfelelő üzemeltetését szolgáló foglalásokhoz adatokat gyűjt utasaitól. A légitársaságnak a következő adatokra lesz szüksége: az utasok ülésszáma; speciális fizikai korlátozások,

287 29. cikk szerinti munkacsoport (2013), *3/2013. sz. vélemény a célok korlátozásáról*, WP 203, 2013. április 2.

288 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés b) pont.

például kerekesszék-igény; valamint speciális élelmiszer-igények, köztük a kóser vagy halal élelmiszer. Ha a légitársaságokat az utasnyilvántartási adatállományban található adatoknak a célállomás helye szerinti bevándorlási hatóságokhoz való továbbítására kérik, a szóban forgó adatokat ezt követően idegenrendészeti ellenőrzés céljára használják fel, ami eltér az adatgyűjtés eredeti céljától. Ezen adatoknak a bevándorlási hatósághoz történő továbbításához tehát új, külön jogalapra lesz szükség.

Egy adott cél terjedelmének és korlátainak mérlegelésekor a Korszerűsített 108. Egyezmény és az általános adatvédelmi rendelet az összeegyeztethetőség fogalmát hívja segítségül: az adatok összeegyeztethető célokra való felhasználása az eredeti jogalap alapján engedélyezett. Az adatok további kezelése ezért nem történhet az érintett számára váratlan, nem megfelelő vagy kifogásolható módon.[289] Annak meghatározásához, hogy a további adatkezelés összeegyeztethetőnek minősül-e, az adatkezelőnek (többek között) a következőket kell mérlegelnie:

- „minden, az említett eredeti célok és a tervezett további adatkezelési célok között fennálló összefüggést;
- az adatgyűjtés körülményeit, ideértve különösen az érintettnek a további adatfelhasználásra vonatkozó, az adatkezelővel fennálló kapcsolatán alapuló észszerű elvárásait is;
- a személyes adatok jellegét;
- a tervezett további adatkezelés következményeit az érintettekre nézve; valamint
- a megfelelő garanciák meglétét mind az eredeti, mind a tervezett további személyes adatok kezelésére vonatkozó műveletek során."[290] Ez történhet például titkosítással vagy álnevesítéssel.

289 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 49. pont.

290 Általános adatvédelmi rendelet, (50) preambulumbekezdés és a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 49. pont.

Példa: A Sunshine vállalat ügyfélkapcsolat-kezelési (CRM) tevékenysége során ügyféladatokra tesz szert. Ezt követően ezeket egy direkt marketing cégnek, a Moonlight vállalatnak továbbítja, amely harmadik cégek marketing kampányainak támogatására kívánja azokat felhasználni. Az adatok Sunshine általi továbbítása más vállalatok marketingtevékenységéhez az adatok új célból történő további felhasználásának minősül, ami összeegyeztethetetlen a Sunshine vállalat eredeti céljával, amelyre az ügyféladatokat gyűjtötte. Az adatok Moonlight vállalatnak történő továbbításához tehát saját jogalap szükséges.

Ezzel szemben, ha a Sunshine vállalat a CRM-adatokat saját marketing céljaira használja fel, például a saját termékeire vonatkozó marketing üzeneteket küld a saját ügyfeleinek, az általában elfogadott mint összeegyeztethető cél.

Az általános adatvédelmi rendelet és a Korszerűsített 108. Egyezmény kimondja, hogy „nem minősül az eredeti céllal össze nem egyeztethetőnek a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő további adatkezelés", vagyis az eleve az eredeti céllal összeegyeztethetőnek minősül.[291] A személyes adatok további kezelése során azonban megfelelő garanciákat kell alkalmazni; ilyen például az adatok anonimizálása, titkosítása vagy álnevesítése, valamint az adatokhoz való hozzáférés korlátozása.[292] Az általános adatvédelmi rendelet ezt kiegészíti azzal, hogy „[h]a az érintett hozzájárulását adta, illetve ha az adatkezelés uniós vagy tagállami jogon alapul, és egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül bizonyos fontos közérdekek védelme szempontjából, a célok összeegyeztethetőségétől függetlenül az adatkezelő jogosult a szóban forgó adatokon további adatkezelést végezni."[293] További adatkezelés végzésekor ezért az érintettet tájékoztatni kell a célokról, valamint jogairól, például az adatkezelés elleni tiltakozáshoz való jogáról.[294]

291 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés b) pont; Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés b) pont. Példa lehet az ilyen nemzeti rendelkezésekre az osztrák adatvédelmi törvény (*Datenschutzgesetz*), Federal Law Gazette I No. 165/1999, 46. pont.

292 Általános adatvédelmi rendelet, 6. cikk (4) bekezdés; Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés b) pont; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 50. pont.

293 Általános adatvédelmi rendelet, (50) preambulumbekezdés.

294 *Uo.*

Példa: A Sunshine vállalat ügyfélkapcsolati (CRM) adatokat gyűjtött és tárolt vásárlóiról. Ezen adatok Sunshine vállalat általi, a vásárlók vásárlási szokásainak statisztikai elemzése céljára való további felhasználása megengedhető, mivel a statisztikai elemzés összeegyeztethető cél. Nincs szükség további jogalapra, például az érintettek hozzájárulására. Ezen adatok statisztikai célokból történő további kezeléséhez azonban a Sunshine vállalatnak megfelelő garanciákat kell biztosítania az érintettek jogainak és szabadságainak védelmére. A Sunshine vállalat által megvalósítandó technikai és szervezési intézkedések között szerepelhet az álnevesítés.

3.3 Az adattakarékosság elve

Főbb pontok

- Az adatkezelést valamely jogszerű cél teljesítéséhez szükségesre kell korlátozni.
- Személyes adatok kezelésére csak akkor kerülhet sor, ha az adatkezelés célja más eszközökkel észszerűen nem teljesíthető.
- Az adatkezelés nem avatkozhat be aránytalanul az érintettek érdekeibe, jogaiba és szabadságaiba.

Csak olyan adatok kezelhetők, amelyek „gyűjtésük és/vagy további [kezelésük] célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek”.[295] A kiválasztott adatkategóriáknak az adatkezelési műveletek általános célja eléréséhez szükségesnek kell lenniük, és az adatkezelőnek szigorúan azon információkra kell korlátoznia az adatgyűjtést, amelyek a kezelés által támogatott konkrét cél szempontjából közvetlenül relevánsak.

Példa: A *Digital Rights Ireland* ügyben[296] az EUB az adatmegőrzési irányelv érvényességét vizsgálta, amelynek célja, hogy harmonizálja a nyilvánosan elérhető elektronikus hírközlési szolgáltatások vagy hálózatok által

295 Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés c) pont; általános adatvédelmi rendelet, 5. cikk (1) bekezdés c) pont.

296 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

létrehozott vagy kezelt személyes adatoknak az illetékes hatóságok számára súlyos bűncselekmények, például szervezett bűnözés vagy terrorizmus leküzdése érdekében történő esetleges továbbítása céljából való megőrzésére vonatkozó nemzeti rendelkezéseket. Annak ellenére, hogy ezt olyan célnak minősítette, amely ténylegesen közérdekű célt szolgál, problematikusnak találta azt, hogy az irányelv általános jelleggel vonatkozik „valamennyi személyre és valamennyi elektronikus hírközlési eszközre, valamint az adatforgalommal kapcsolatos adatok összességére, anélkül hogy a súlyos bűncselekmények elleni küzdelem célja alapján bármilyen megkülönböztetést, korlátozást vagy kivételt alkalmazna”.[297]

Továbbá a a személyes adatok biztonságát növelő speciális technológia igénybevételével néha teljesen elkerülhető a személyes adatok használata, vagy olyan intézkedések alkalmazása, amelyek csökkentik annak lehetőségét, hogy az adatokat összekapcsolják egy érintettel (például álnevesítés útján), ami magánéletvédelmi szempontból jobb megoldást eredményez. Ez a kiterjedtebb adatfeldolgozó rendszerekben különösen helyénvaló.

Példa: Egy városi tanács bizonyos díj ellenében chipkártyát ad a városi tömegközlekedést rendszeresen igénybevevő közlekedőknek. A kártya felületén szerepel a használó neve írásos formában, és a chipben elektronikus formában is rögzítve van. Ha a közlekedő személy autóbuszt vagy villamost vesz igénybe, a chipkártyát el kell húzni a buszra vagy villamosra felszerelt leolvasókészülék előtt. A készülék által leolvasott adatokat elektronikusan összevetik egy adatbázissal, amely az utazási kártyát megvásárolt személyek nevét tartalmazza.

Ez a rendszer nem tartja be optimálisan az adattakarékosság elvét: annak ellenőrzése, hogy egy személy használhatja-e a közlekedési eszközöket, anélkül is megoldható, hogy összevetnék a chipen található személyes adatokat egy adatbázissal. Elég lenne például egy speciális elektronikus kép, pl. vonalkód a kártya chipjében, amely, ha elhúzzák a leolvasókészülék előtt, igazolná a kártya érvényességét. Egy ilyen rendszer nem rögzítené, hogy ki, mikor, milyen közlekedési eszközt használt. Az adattakarékosság elve értelmében ez lenne az optimális megoldás, mivel ez az elv végső fokon az adatgyűjtés minimalizálására vonatkozó kötelezettséget ír elő.

297 *Uo.*, 44. és 57. pont.

A Korszerűsített 108. Egyezmény 5. cikkének (1) bekezdése tartalmaz egy arányossági követelményt a személyes adatok kezelése tekintetében a szolgált törvényes céllal kapcsolatban. Tisztességes egyensúlyt kell teremteni az összes érintett érdek között az adatkezelés minden szakaszában. Ez azt jelenti, hogy „[t]úlzottnak kell tekinteni azokat a személyes adatokat, amelyek megfelelőek és relevánsak, azonban aránytalanul beavatkoznak az érintettet megillető alapvető jogokba és szabadságokba".[298]

3.4 Az adatok pontosságának elve

Főbb pontok

- Az adatok pontosságának elvét az adatkezelőnek minden adatkezelési művelet során érvényesítenie kell.
- A pontatlan adatokat haladéktalanul törölni vagy helyesbíteni kell.
- Az adatok rendszeres ellenőrzése és aktualizálása lehet szükséges a pontosság biztosítása érdekében.

A személyes információkat birtokló adatkezelő anélkül nem használhatja fel ezeket az információkat, hogy lépéseket tenne annak kellő bizonyossággal történő biztosítására, hogy az adatok pontosak és naprakészek.[299]

Az adatok pontosságának biztosítására irányuló kötelezettséget az adatfeldolgozás céljával összefüggésben kell megítélni.

Példa: A *Rijkeboer* ügyben[300] az EUB egy dán állampolgár arra irányuló kérelmét vizsgálta meg, hogy Amszterdam városának helyi önkormányzatától információt kapjon azon személyek kilétéről, akikkel az önkormányzat az elmúlt két évben közölte a róla nyilvántartott adatokat, valamint a kiadott adatok tartalmáról. Az EUB kimondta, hogy

298 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 52. pont; általános adatvédelmi rendelet, 5. cikk (1) bekezdés c) pont.

299 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés d) pont; Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés d) pont.

300 EUB, *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer*, C-553/07. sz. ügy, 2009. május 7.

a „magánélet tiszteletben tartásához való jog magában foglalja, hogy az érintett személy megbizonyosodhasson arról, hogy személyes adatait helyesen és jogszerűen dolgozzák fel, vagyis különösen arról, hogy alapvető adatai helyesek, és azokat arra jogosult személyeknek továbbítják." Az EUB hivatkozott az adatvédelmi irányelv preambulumára, amely kimondja, hogy az érintetteknek biztosítani kell a személyes adataikhoz való hozzáférés jogát az adatok helyességének ellenőrzése céljából.[301]

Lehetnek olyan esetek is, amikor a tárolt adatok frissítését jogszabály tiltja, mert az adatok tárolásának elsődleges célja események, mint múltbeli „pillanatfelvételek" dokumentálása.

Példa: Egy műtéti jegyzőkönyvet nem szabad megváltoztatni, más szóval „frissíteni" még akkor sem, ha a jegyzőkönyvben szereplő megállapítások később tévesnek bizonyulnak. Ilyen körülmények között csupán a jegyzőkönyvben szereplő észrevételekhez fűzhetők kiegészítések, amennyiben egyértelműen megjelölik, hogy utólagos hozzájárulásokról van szó.

Másrészt viszont vannak olyan helyzetek, amikor az adatok pontosságának rendszeres ellenőrzése, a frissítést is beleértve, feltétlenül szükséges, mert ha az adatokat pontatlanul hagyják, az kárt okozhat az érintettnek.

Példa: Ha valaki hitelszerződést akar kötni egy bankkal, a bank általában ellenőrzi a leendő ügyfél hitelképességét. E célból elérhetők speciális adatbankok, amelyek magánszemélyek hiteltörténetére vonatkozóan tartalmaznak adatokat. Ha egy ilyen adatbázis helytelen vagy idejétmúlt adatokat tartalmaz valakiről, ez negatív hatással lehet az illetőre. Ezért az ilyen adatbázisok kezelőinek különösen törekedniük kell a pontosság elvének betartására.

301 A már nem hatályos 95/46/EK irányelv (41) preambulumbekezdése.

3.5 A korlátozott tárolhatóság elve

Főbb pontok

- A korlátozott tárolhatóság elve azt jelenti, hogy a személyes adatokat törölni vagy anonimizálni kell, amint már nincs rájuk szükség arra a célra, amelyre gyűjtötték őket.

Az általános adatvédelmi rendelet 5. cikke (1) bekezdésének e) pontja, valamint a Korszerűsített 108. Egyezmény 5. cikke (4) bekezdésének e) pontja előírja, hogy a személyes adatok „tárolásának olyan formában kell történnie, amely az érintettek azonosítását csak a személyes adatok kezelése céljainak eléréséhez szükséges ideig teszi lehetővé". Az adatokat tehát törölni vagy anonimizálni kell, amint a célok teljesültek. Annak biztosítása érdekében, hogy a személyes adatok tárolása a szükséges időtartamra korlátozódjon, „az adatkezelő törlési vagy rendszeres felülvizsgálati határidőket állapít meg".[302]

Az *S. és Marper* ügyekben az EJEB megállapította, hogy az Európa Tanács vonatkozó eszközeinek alapelvei, valamint a többi szerződő fél joga és gyakorlata előírja, hogy az adatmegőrzésnek az adatgyűjtés céljával arányosnak és időben korlátozottnak kell lennie, különösen a rendőrségi ágazatban.[303]

Példa: Az *S. és Marper* ügyekben[304] az EJEB ítélete szerint a két felperes ujjlenyomatainak, sejtmintáinak és DNS-profiljának határozatlan idejű tárolása egy demokratikus társadalomban aránytalan és szükségtelen volt figyelemmel arra, hogy mindkét felperes ellen folyatott büntetőeljárást megszüntették, egyik esetében felmentéssel, míg a másik esetében perbeszüntetéssel.

A személyes adatok tárolására vonatkozó időbeli korlátozás csak olyan adatokra vonatkozik, amelyeket az érintett azonosítását lehetővé tevő formában tárolnak.

302 Általános adatvédelmi rendelet, (39) preambulumbekezdés.

303 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4., lásd még például: EJEB, *M.M. kontra Egyesült Királyság*, 24029/07. sz. ügy, 2012. november 13.

304 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4.

Azon adatok jogszerű tárolása is lehetséges tehát, amelyekre már nincs szükség, ha az adatokat anonimizálják vagy álnevesítik.

Az adatok közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból hosszabb ideig is tárolhatók, feltéve, hogy az érintett adatokat kizárólag a fenti célokra használják.[305] Megfelelő technikai és szervezési intézkedéseket kell végrehajtani a személyes adatok folyamatos tárolásához és felhasználásához az érintettek jogainak és szabadságainak védelme érdekében.

A Korszerűsített 108. Egyezmény szintén engedélyez kivételeket a korlátozott tárolhatóság elve alól azzal a feltétellel, hogy azokat törvény írja elő, tiszteletben tartják az alapvető jogok és szabadságok lényegét és szükségesek és arányosak korlátozott számú jogszerű célok előmozdításához.[306] Ide tartozik többek között a nemzetbiztonság védelme, bűncselekmények nyomozása és büntetőeljárás lefolytatása, büntetőjogi szankciók végrehajtása, az érintett védelme és mások jogainak, illetve szabadságainak védelme.

Példa: A *Digital Rights Ireland* ügyben[307] az EUB az adatmegőrzési irányelv érvényességét vizsgálta, amelynek célja, hogy harmonizálja a nyilvánosan elérhető elektronikus hírközlési szolgáltatások vagy hálózatok által létrehozott vagy kezelt személyes adatoknak az illetékes hatóságok számára súlyos bűncselekmények, például szervezett bűnözés vagy terrorizmus leküzdése érdekében történő esetleges továbbítása céljából való megőrzésére vonatkozó nemzeti rendelkezéseket. Az adatmegőrzési irányelv előírja, hogy az adatokat „legalább hat hónapig kell megőrizni, anélkül hogy bármilyen különbséget tenne az említett irányelv 5. cikkében szereplő adatkategóriák között azoknak a követett cél szempontjából való esetleges hasznossága alapján vagy az érintett személyek szerint”.[308] Az EUB felvetette továbbá az adatmegőrzési irányelvben szereplő objektív okok hiányának kérdését, amely alapján az adatmegőrzés pontos időtartamát

305 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés e) pont; Korszerűsített 108. Egyezmény, 5. cikk (3) bekezdés b) pont és 9. cikk (2) bekezdés.

306 Korszerűsített 108. Egyezmény, 9.1 cikk; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 91–98. pont.

307 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

308 *Uo.*, 63. pont.

– amely legalább hat hónap, legfeljebb pedig huszonnégy hónap közötti időtartam lehet – kell meghatározni annak biztosítása érdekében, hogy az a feltétlenül szükséges mértékre korlátozódjon.[309]

3.6 Az adatbiztonság elve

Főbb pontok

- A személyes adatok biztonsága és bizalmas jellege kulcsfontosságú az érintettre gyakorolt hátrányos hatások megelőzése érdekében.
- A biztonsági intézkedések lehetnek technikai és/vagy szervezési jellegűek.
- Az álnevesítés egy olyan eljárás, amellyel megvédhetők a személyes adatok.
- A biztonsági intézkedések megfelelőségét eseti alapon kell megállapítani, és rendszeresen felül kell vizsgálni.

Az adatbiztonság elve megköveteli a megfelelő technikai vagy szervezési intézkedések alkalmazását a személyes adatok kezelése során az adatokhoz való véletlen, jogosulatlan vagy törvénytelen hozzáférés, felhasználás, módosítás, közzététel, vesztés, megsemmisülés vagy sérülés elleni védelem érdekében.[310] Az általános adatvédelmi rendelet kimondja, hogy ilyen intézkedések megtételekor az adatkezelőnek és az adatfeldolgozónak figyelembe kell vennie „a tudomány és technológia állás[át] és a megvalósítás költségei[t], továbbá az adatkezelés jelleg[ét], hatókör[ét], körülményei[t] és céljai[t], valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat[ot]”.[311] Az egyes esetek konkrét körülményeitől függően megfelelő technikai és szervezési intézkedés lehet például a személyes adatok álnevesítése és titkosítása, és/vagy az intézkedések rendszeres tesztelése és értékelése az adatkezelés biztonságának biztosítására.[312]

309 *Uo.*, 64. pont.

310 Általános adatvédelmi rendelet, (39) preambulumbekezdés és 5. cikk (1) bekezdés f) pont; Korszerűsített 108. Egyezmény, 7. cikk.

311 Általános adatvédelmi rendelet, 32. cikk (1) bekezdés.

312 *Uo.*

A 2.1.1 szakaszban tárgyaltak szerint az adatok álnevesítése azt jelenti, hogy egy technikai vagy szervezési intézkedés keretében a személyes adatok – érintett azonosítását lehetővé tevő – jellemzőit egy álnévre cserélik, és az érintett jellemzőket elkülönítve tárolják. Az álnevesítést nem szabad összekeverni az anonimizálással, amelynél az egyént azonosító összes kapcsolatot megszüntetik.

Példa: Az a mondat például, hogy „az 1967. április 3-án született Charles Spencer négy gyermek, két fiú és két lány apja", a következőképpen álnevesíthető:

„C.S. 1967 négy gyermek, két fiú és két lány apja"; vagy

„324 négy gyermek, két fiú és két lány apja"; vagy

„YESz3201 négy gyermek, két fiú és két lány apja".

A felhasználók, akik hozzáférnek az álnevesített adatokhoz, a „324"-ből vagy a „YESz3201"-ből rendszerint nem tudják azonosítani „az 1967. április 3-án született Charles Spencert". Ezért az ilyen adatok valószínűsíthetően védenek a visszaéléssel szemben.

Az első példa azonban kevésbé biztonságos. Ha a „C.S. 1976 négy gyermek, két fiú és két lány apja" mondatot abban a kis faluban használják, ahol Charles Spencer él, könnyen felismerhető lehet. Az álnevesítés módszere befolyásolja az adatvédelem hatékonyságát.

A titkosított vagy külön tárolt jellemzőket tartalmazó személyes adatokat számos összefüggésben a személyazonosság titokban tartásának eszközeként használják. Ez különösen akkor hasznos, ha az adatkezelőnek biztosítania kell, hogy ugyanazon érintettekkel foglalkozik, de nem szükséges – vagy nem feltétlenül kell – ismernie az érintettek valódi személyazonosságát. Ez a helyzet például akkor, ha egy kutató olyan betegekkel tanulmányozza egy betegség lefolyását, akiknek a személyazonosságát csak az a kórház ismeri, ahol kezelik őket, és ahonnan a kutató az álnevesített kórtörténeteket kapja. Az álnevesítés tehát erős elem a magánélet védelmét erősítő technológia fegyvertárában. Fontos lehet a beépített adatvédelem megvalósítása során. Ez azt jelenti, hogy a fejlett adatkezelő rendszerek szerkezetébe eleve beépítik az adatvédelmet.

Az általános adatvédelmi rendelet beépített adatvédelemmel foglalkozó 25. cikke példaként hivatkozik kifejezetten az álnevesítésre, mint megfelelő technikai és szervezési intézkedésre, amelyet az adatkezelőknek meg kell tenniük az adatvédelmi elvek teljesítéséhez és a szükséges garanciák beépítéséhez. Ennek során az adatkezelők teljesítik a rendeletben foglalt követelményeket és védik az érintettek jogait személyes adataik kezelése során.

Egy jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozás segíthet igazolni az adatkezelés biztonságára vonatkozó követelményeknek való megfelelést.[313] Az utasnyilvántartási adatállományok feldolgozásának adatvédelmi vonzatairól szóló véleményében az Európa Tanács egyéb példákat is ad az utasnyilvántartó rendszerekben szereplő személyes adatok védelmét szolgáló megfelelő biztonsági intézkedésekre. Ilyen például az adatok biztonságos fizikai környezetben való tárolása, hozzáférés korlátozása többszintű bejelentkezéssel, valamint az adatok közlésének védelme szigorú kriptográfiával.[314]

> Példa: A közösségi oldalak és e-mail-szolgáltatók a kétszintű hitelesítés bevezetésével lehetővé teszik a felhasználók számára, hogy egy plusz védelmi szinttel egészítsék ki az igénybe vett szolgáltatást. A személyes jelszó megadásán túl a felhasználóknak egy második bejelentkezésen is át kell esniük ahhoz, hogy beléphessenek személyes fiókjukba. Ez utóbbi lehet például egy a személyes fiókhoz rendelt mobiltelefonszámra küldött biztonsági kód megadása. A kétlépéses hitelesítés így fokozottabb védelmet biztosít a személyes adatok számára a személyes fiókhoz való jogosulatlan hozzáféréssel szemben a fiók feltörése esetén.

A Korszerűsített 108. Egyezmény további példákat szolgáltat a megfelelő garanciákra. Ilyen például a szakmai titoktartási kötelezettség előírása, vagy minősített technikai biztonsági intézkedések, például adattitkosítás alkalmazása.[315] Sajátos biztonsági intézkedések érvénybe léptetésekor az adatkezelőnek – vagy adott esetben az adatfeldolgozónak – számos elemet kell figyelembe vennie, így például a kezelt személyes adatok jellegét és mennyiségét, a lehetséges káros következményeket az érintettekre nézve, valamint az adatokhoz való korlátozott hozzáférés

313 *Uo.*, 32. cikk (3) bekezdés.

314 Európa Tanács, 108. Egyezmény bizottsága, *Vélemény az utasnyilvántartási adatállományok feldolgozásának adatvédelmi vonzatairól*, T-PD(2016)18rev, 2016. augusztus 19., 9. o.

315 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 56. pont.

szükségességét.[316] Megfelelő biztonsági intézkedések megvalósításakor figyelembe kell venni az adatkezelés során alkalmazható legkorszerűbb adatbiztonsági módszereket és technikákat. Az ilyen intézkedések költségének a lehetséges kockázatok súlyosságával és valószínűségével arányosnak kell lennie. A biztonsági intézkedéseket rendszeresen felül kell vizsgálni, hogy szükség esetén aktualizálni lehessen azokat.[317]

A személyes adatokkal való visszaélés esetén a Korszerűsített 108. Egyezmény és az általános adatvédelmi rendelet egyaránt előírja, hogy az adatkezelő haladéktalanul értesítse az illetékes felügyeleti hatóságot az adatvédelmi incidensről az egyének jogaira és szabadságaira gyakorolt kockázatok megadásával.[318] Hasonló tájékoztatási kötelezettség áll fenn az érintettel szemben, amikor az adatvédelmi incidens valószínűsíthetően kockázattal jár az érintett jogaira és szabadságaira nézve.[319] Az adatvédelmi incidenseket világosan és közérthetően kell közölni az érintettekkel.[320] Ha egy adatvédelmi incidens jut az adatkezelő tudomására, azonnal értesítenie kell az érintetteket.[321] Bizonyos helyzetekben az értesítési kötelezettség alóli kivételek alkalmazhatók. Az adatkezelő például nem köteles értesíteni a felügyeleti hatóságot, ha „az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve".[322] Az érintettet sem szükséges értesíteni akkor, ha az alkalmazott biztonsági intézkedések a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat, vagy a későbbi intézkedések biztosítják, hogy a magas kockázat a továbbiakban ne valósuljon meg.[323] Ha az érintettek tájékoztatása az adatvédelmi incidensről az adatkezelő számára aránytalan erőfeszítést tenne szükségessé, nyilvánosan közzétett információk vagy hasonló intézkedések biztosíthatják „az érintettek hasonlóan hatékony tájékoztatását".[324]

316 *Uo.*, 62. pont.

317 *Uo.*, 63. pont.

318 Korszerűsített 108. Egyezmény, 7. cikk (2) bekezdés; általános adatvédelmi rendelet, 33. cikk (1) bekezdés.

319 Korszerűsített 108. Egyezmény, 7. cikk (2) bekezdés; általános adatvédelmi rendelet, 34. cikk (1) bekezdés.

320 Általános adatvédelmi rendelet, 34. cikk (2) bekezdés.

321 *Uo.*, 33. cikk (1) bekezdés.

322 *Uo.*, 33. cikk (1) bekezdés.

323 *Uo.*, 34. cikk (3) bekezdés a) és b) pont.

324 *Uo.*, 34. cikk (3) bekezdés c) pont.

3.7 Az elszámoltathatóság elve

Főbb pontok

- Az elszámoltathatósághoz az szükséges, hogy az adatkezelők és adatfeldolgozók adatkezelési tevékenységük során aktívan hajtsák végre az adatvédelem előmozdítására és biztosítására irányuló intézkedéseket.
- Adatkezelési műveleteik során az adatkezelők és adatfeldolgozók felelősek az adatvédelmi jog és saját kötelezettségeik betartásáért.
- Az adatkezelőknek bármikor tudniuk kell bizonyítani az adatvédelmi rendelkezések betartását az érintettek, a nyilvánosság és a felügyeleti hatóságok felé. Az adatfeldolgozóknak is meg kell felelniük az elszámoltathatósághoz kapcsolódó néhány szigorú kötelezettségnek (ilyen például a nyilvántartás vezetése az adatkezelési tevékenységekről és adatvédelmi tisztviselő kinevezése).

Az általános adatvédelmi rendelet és a Korszerűsített 108. Egyezmény megállapítja, hogy az adatkezelő felelős a személyes adatok kezelésének ebben a fejezetben ismertetett elveinek betartásáért, és az tudnia kell bizonyítani.[325] E célból az adatkezelőnek megfelelő technikai és szervezési intézkedéseket kell megvalósítania.[326] Bár az elszámoltathatóság általános adatvédelmi rendelet 5. cikkének (2) bekezdésében rögzített elve kizárólag az adatkezelőkre irányul, az adatfeldolgozókkal szemben is elvárás, hogy elszámoltathatók legyenek, figyelemmel arra, hogy számos kötelezettségnek kell eleget tenniük, és azok szorosan kapcsolódnak az elszámoltathatósághoz.

Az uniós és Európa tanácsi adatvédelmi jogszabályok szintén megállapítják, hogy az adatkezelő felelős a 3.1–3.6 szakaszokban tárgyalt adatvédelmi elvek betartásáért, és azok betartatásáért.[327] A 29. cikk szerinti munkacsoport rámutatott arra, hogy „az eljárások és mechanizmusok típusa attól függően változna, hogy milyen kockázatot jelent az adatkezelés és az adatok jellege”.[328]

Az adatkezelők számos módon előmozdíthatják a megfelelőséget, többek között az alábbiakkal:

325 *Uo.*, 5. cikk (2) bekezdés; Korszerűsített 108. Egyezmény, 10. cikk (1) bekezdés.

326 Általános adatvédelmi rendelet, 24. cikk.

327 *Uo.*, 5. cikk (2) bekezdés; Korszerűsített 108. Egyezmény, 10. cikk (1) bekezdés.

328 29. cikk szerinti munkacsoport, *3/2010. sz. vélemény az elszámoltathatóság elvéről*, WP 173, Brüsszel, 2010. július 13., 12. pont.

- az adatvédelmi tevékenységek nyilvántartásba vétele és azok rendelkezésre bocsátása a felügyeleti hatóság kérésére;[329]

- egyes helyzetekben adatvédelmi tisztviselő kinevezése, aki a személyes adatok védelmével kapcsolatos minden kérdésben részt vesz;[330]

- adatvédelmi hatásvizsgálat végzése az adatkezelés olyan típusaira, amelyek valószínűleg magas kockázatot jelentenek a természetes személyek jogaira és szabadságaira nézve;[331]

- beépített és alapértelmezett adatvédelem biztosítása;[332]

- az érintettek jogainak gyakorlására vonatkozó intézkedések és eljárások végrehajtása;[333]

- csatlakozás egy jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz.[334]

Bár az elszámoltathatóság általános adatvédelmi rendelet 5. cikkének (2) bekezdésében foglalt elve nem kifejezetten adatfeldolgozókra irányul, vannak az elszámoltathatósághoz kapcsolódó olyan rendelkezések, amelyek számukra is tartalmaznak kötelezettségeket, például nyilvántartás vezetése az adatkezelési tevékenységekről és adatvédelmi tisztviselő kinevezése bármely olyan adatkezelési tevékenységhez, amelyhez ez szükséges.[335] Az adatfeldolgozóknak biztosítaniuk kell, hogy végrehajtják az adatok biztonságának biztosításához szükséges valamennyi intézkedést.[336] Az adatkezelő és adatfeldolgozó közötti jogilag kötelező érvényű szerződésnek tartalmaznia kell, hogy az adatfeldolgozó segíti az adatkezelőt néhány megfelelőségi követelmény teljesítésében, például adatvédelmi hatásvizsgálat végzésekor, vagy

329 Általános adatvédelmi rendelet, 30. cikk.

330 *Uo.*, 37–39. cikk.

331 *Uo.*, 35. cikk; Korszerűsített 108. Egyezmény, 10. cikk (2) bekezdés.

332 Általános adatvédelmi rendelet, 25. cikk; Korszerűsített 108. Egyezmény, 10. cikk (2)–(3) bekezdés.

333 Általános adatvédelmi rendelet, 12. cikk és 24. cikk.

334 *Uo.*, 40. cikk és 42. cikk.

335 *Uo.*, 5. cikk (2) bekezdés, 30. és 37. cikk.

336 *Uo.*, 28. cikk (3) bekezdés c) pont.

azzal, hogy tájékoztatja az adatkezelőt minden adatvédelmi incidensről, amint azok tudomására jutottak.[337]

2013-ban a Gazdasági Együttműködési és Fejlesztési Szervezet (OECD) adatvédelmi iránymutatásokat fogadott el, amelyek kiemelték az adatkezelők fontos szerepét az adatvédelem gyakorlati megvalósulása terén. Az iránymutatásokban szerepel az elszámoltathatóság elve, miszerint „az adatkezelőnek elszámoltathatónak kell lennie azon intézkedések betartásáért, amelyek érvényre juttatják a fenti [fő] elveket.[338]

Példa: Az elszámoltathatóság elvének hangsúlyozására vonatkozó jogalkotási példa a 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv) 2009-es módosítása[339]. A módosított 4. cikk szerint az irányelv kötelezettséget ír elő „a személyes adatok feldolgozásának biztonságára vonatkozó politika" biztosítására. Ami tehát a szóban forgó irányelv biztonsági rendelkezéseit illeti, a jogalkotó úgy döntött, hogy kifejezett követelményként kell bevezetni a biztonsági politika létrehozását és végrehajtását.

A 29. cikk szerinti munkacsoport véleménye szerint[340] az elszámoltathatóság lényege az adatkezelő arra vonatkozó kötelezettsége, hogy:

- olyan intézkedéseket hozzon, amelyek a feldolgozási műveletekkel összefüggésben – rendes körülmények között – garantálják az adatvédelmi szabályok betartását; valamint

337 *Uo.*, 28. cikk (3) bekezdés d) pont.

338 OECD (2013), *Az adatvédelemre és az országhatárokat átlépő személyesadat-áramlásra vonatkozó iránymutatások*, 14. cikk.

339 Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról, HL L 337., 2009.12.18.

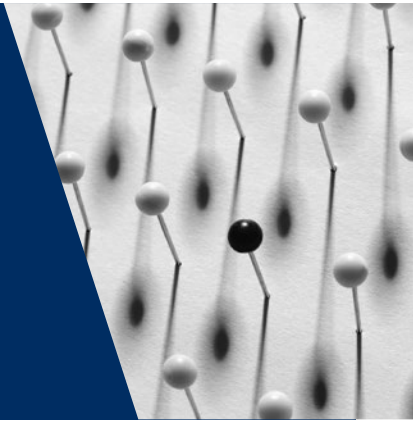
340 29. cikk szerinti munkacsoport, *3/2010. sz. vélemény az elszámoltathatóság elvéről*, WP 173, Brüsszel, 2010. július 13.

- olyan dokumentációval rendelkezzen, amely igazolja az érintettek és a felügyeleti hatóságok számára, hogy milyen intézkedéseket hoztak az adatvédelmi szabályok betartatására.

Az elszámoltathatóság elvéhez tehát az adatkezelőknek aktívan bizonyítaniuk kell a szabályok betartását, nem szabad csupán arra várniuk, hogy az érintettek vagy a felügyeleti hatóságok mutassanak rá a hiányosságokra.

4

Az európai adatvédelmi jog szabályai



EU	Tárgyalt kérdések	Európa Tanács
A jogszerű adatkezelésre vonatkozó szabályok		
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés a) pont EUB, *Deutsche Telekom AG kontra Bundesrepublik Deutschland*, C-543/09. sz. ügy, 2011 EUB, *Tele2 (Netherlands) BV és társai kontra Autoriteit Consument en Markt (AMC)*, C-536/15. sz. ügy, 2017	**Hozzájárulás**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk b) pont és 3.6. cikk Korszerűsített 108. Egyezmény, 5. cikk (2) bekezdés
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés b) pont	**Szerződéses (illetve szerződéskötés előtti) jogviszony**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk b) pont
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés c) pont	**Az adatkezelő jogszabályi kötelezettségei**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk a) pont
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés d) pont	**Az érintett létfontosságú érdekei**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk b) pont
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés e) pont EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008	**Közérdek és hivatali hatáskör gyakorlása**	A profilalkotásra vonatkozó ajánlás, 3.4. cikk b) pont

EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 6. cikk (1) bekezdés f) pont EUB, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde kontra Rīgas pašvaldības SIA „Rīgas satiksme”*, C-13/16. sz. ügy, 2017 EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011	Mások jogos érdekei	A profilalkotásra vonatkozó ajánlás, 3.4. cikk b) pont EJEB, *Y kontra Törökország*, 648/10. sz. ügy, 2015
Általános adatvédelmi rendelet, 6. cikk (4) bekezdés	Kivételek a célhoz kötöttség alól: más célból történő további adatkezelés	Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés b) pont
A különleges adatok jogszerű kezelésére vonatkozó szabályok		
Általános adatvédelmi rendelet, 9. cikk (1) bekezdés	Az adatkezelés általános tilalma	Korszerűsített 108. Egyezmény, 6. cikk
Általános adatvédelmi rendelet, 9. cikk (2) bekezdés	Kivételek az általános tilalom alól	Korszerűsített 108. Egyezmény, 6. cikk
A biztonságos feldolgozásra vonatkozó szabályok		
Általános adatvédelmi rendelet, 32. cikk	Biztonságos adatkezelés biztosításának kötelezettsége	Korszerűsített 108. Egyezmény, 7. cikk (1) bekezdés EJEB, *I. kontra Finnország*, 20511/03. sz. ügy, 2008
Általános adatvédelmi rendelet, 28. cikk és 32. cikk (1) bekezdés b) pont	Titoktartási kötelezettség	Korszerűsített 108. Egyezmény, 7. cikk (1) bekezdés
Általános adatvédelmi rendelet, 34. cikk Elektronikus hírközlési adatvédelmi irányelv, 4. cikk (2) bekezdés	Adatvédelmi incidens bejelentése	Korszerűsített 108. Egyezmény, 7. cikk (2) bekezdés
Az elszámoltathatóságra vonatkozó szabályok és a megfelelőség előmozdítása		
Általános adatvédelmi rendelet, 12., 13. és 14. cikk	Az átláthatóság általában	Korszerűsített 108. Egyezmény, 8. cikk
Általános adatvédelmi rendelet, 37., 38. és 39. cikk	Adatvédelmi tisztviselők	Korszerűsített 108. Egyezmény, 10. cikk (1) bekezdés
Általános adatvédelmi rendelet, 30. cikk	A feldolgozási tevékenységek nyilvántartása	

EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 35. és 36. cikk	**Hatásvizsgálat és előzetes konzultáció**	Korszerűsített 108. Egyezmény, 10. cikk (2) bekezdés
Általános adatvédelmi rendelet, 33. és 34. cikk	**Adatvédelmi incidens bejelentése**	Korszerűsített 108. Egyezmény, 7. cikk (2) bekezdés
Általános adatvédelmi rendelet, 40. és 41. cikk	**Magatartási kódexek**	
Általános adatvédelmi rendelet, 42. és 43. cikk	**Tanúsítás**	
Beépített és alapértelmezett adatvédelem		
Általános adatvédelmi rendelet, 25. cikk (1) bekezdés	**Beépített adatvédelem**	Korszerűsített 108. Egyezmény, 10. cikk (2) bekezdés
Általános adatvédelmi rendelet, 25. cikk (2) bekezdés	**Alapértelmezett adatvédelem**	Korszerűsített 108. Egyezmény, 10. cikk (3) bekezdés

Az elvek szükségképpen általános jellegűek. Konkrét helyzetekre való alkalmazásuk során van bizonyos értelmezési mozgástér, és az eszközök is megválaszthatók. Az **Európa Tanács joga** szerint a Korszerűsített 108. Egyezmény részes felei hazai jogukban maguk pontosíthatják az értelmezést. Más a helyzet az **uniós jogban**: a belső piacon az adatvédelem létrehozása érdekében uniós szinten már részletesebb szabályozást tartottak szükségesnek, hogy összehangolják a tagállamok nemzeti jogszabályainak adatvédelmi szintjét. Az általános adatvédelmi rendelet az 5. cikkében meghatározott elvek alapján részletes szabályokat állapít meg, amelyek közvetlenül alkalmazandók a nemzeti jogrendben. Az európai szintű részletes adatvédelmi szabályokkal kapcsolatos alábbi észrevételek ezért túlnyomórészt az uniós joggal foglalkoznak.

4.1 A jogszerű adatkezelésre vonatkozó szabályok

Főbb pontok

- Személyes adatok akkor kezelhetők jogszerűen, ha azok megfelelnek a következő feltételek valamelyikének:
  - az adatkezelés az érintett hozzájárulásán alapul;
  - egy szerződéses jogviszony írja elő a személyes adatok kezelését;

  - az adatkezelés az adatkezelőre vonatkozó jogszabályi kötelezettségnek teljesítéséhez szükséges;
  - az érintettek vagy más személyek létfontosságú érdeke miatt szükséges adataik kezelése;
  - az adatkezelés közérdekből elvégzendő feladat teljesítéséhez szükséges;
  - az adatkezelés okát harmadik felek törvényes érdekei jelentik, de csak annyiban, amennyiben ezt az indokot az érintettek érdekei vagy alapvető jogai nem írják felül.
- A különleges adatok jogszerű feldolgozása speciális, szigorúbb rend szerint történik.

4.1.1 Az adatkezelés jogalapjai

Az általános adatvédelmi rendelet II., „Elvek" című fejezete rendelkezik arról, hogy valamennyi személyes adatkezelésnek meg kell felelnie az általános adatvédelmi rendelet 5. cikkében meghatározott, és az adatminőséghez kapcsolódó elveknek. Az egyik ilyen elv az, hogy a személyes adatokat „jogszerűen, tisztességesen és átlátható módon kell kezelni". Másodszor, ahhoz, hogy az adatok kezelése jogszerű legyen, az adatkezelésnek meg kell felelnie azon jogalapok egyikének, amelyek az adatkezelést törvényessé teszik.[341] Ezek felsorolását a nem különleges adatok tekintetében a 6. cikk, a különleges adatkategóriák (vagy különleges adatok) esetében pedig a 9. cikk tartalmazza. Hasonlóan, a Korszerűsített 108. Egyezmény II. fejezete, amely meghatározza „a személyes adatok védelmének alapelveit", megállapítja, hogy ahhoz, hogy az adatkezelés törvényes legyen, „arányosnak kell lennie a szolgált törvényes céllal kapcsolatban".

Függetlenül attól, hogy az adatkezelő a személyes adatok kezelésének kezdeményezésekor milyen jogalapra támaszkodik, az adatkezelőnek az általános adatvédelmi jogi rendszer szerinti biztosítékokat is alkalmaznia kell.

341 EUB, *Rechnungshof kontra Österreichischer Rundfunk és társai,* valamint *Christa Neukomm és Joseph Lauermann kontra Österreichischer Rundfunk*, C-465/00., C-138/01. és C-139/01. sz. egyesített ügyek, 2003. május 20., 65. pont; EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008. december 16., 48. pont; EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24., 26. pont.

Hozzájárulás

Az **Európa Tanács jogában** a hozzájárulást a Korszerűsített 108. Egyezmény 5. cikkének (2) bekezdése említi. Az EJEB ítélkezési gyakorlata és számos Európa tanácsi ajánlás is hivatkozik rá.[342] Az **uniós jogban** a hozzájárulás mint a jogszerű adatkezelés alapja egyértelműen megjelenik az általános adatvédelmi rendelet 6. cikkében, és a Charta 8. cikke is kifejezetten említi. Az érvényes hozzájárulás jellemzőit az általános adatvédelmi rendelet 4. cikkben foglalt fogalommeghatározás ismerteti, míg az érvényes hozzájárulás megszerzésének feltételeit a 7. cikk részletezi, a gyermekek hozzájárulásának egyedi szabályait az információs társadalommal összefüggő szolgáltatások vonatkozásában pedig a 8. cikk állapítja meg.

A 2.4 szakaszban ismertetettek szerint a hozzájárulást szabad akaratból, konkrétan, megfelelő tájékoztatás alapján és egyértelműen kell megtenni. A hozzájárulást nyilatkozattal vagy olyan egyértelmű megerősítő cselekedettel kell megadni, amely jelzi az adatkezeléshez való hozzájárulást, és a hozzájárulást adó személy jogosult bármikor visszavonni hozzájárulását. Az adatkezelők kötelesek ellenőrizhető nyilvántartást vezetni a hozzájárulásokról.

Önkéntes hozzájárulás

Az **Európa tanácsi** Korszerűsített 108. Egyezmény keretében az érintett hozzájárulásának „szándékosan hozott döntés szabad kinyilvánítását kell kifejeznie".[343] A szabad akaratból tett hozzájárulás csak akkor érvényes, „ha az érintettnek valódi választási lehetősége van, és nem áll fenn a megtévesztés, megfélemlítés, kényszerítés vagy jelentős negatív következmények kockázata, ha az érintett nem adja hozzájárulását".[344] E tekintetben az **uniós jog** kiköti, hogy a hozzájárulás megadása nem tekinthető önkéntesnek, „ha az érintett nem rendelkezik valós vagy szabad választási lehetőséggel, és nem áll módjában a hozzájárulás anélküli megtagadása vagy visszavonása, hogy ez kárára válna".[345] Az általános adatvédelmi rendelet hangsúlyozza, hogy „(a)nnak megállapítása során, hogy a hozzájárulás önkéntes-e, a lehető legnagyobb mértékben figyelembe kell venni azt a tényt, egyebek mellett,

342 Lásd például: Európa Tanács, a Miniszteri Bizottság CM/Rec(2010)13. sz., 2010. november 23-i ajánlása a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről, 2010. november 23., 3.4. cikk b) pont.

343 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

344 Lásd még: 29. cikk szerinti munkacsoport (2011), *15/2011. sz. vélemény a hozzájárulás fogalmáról*, WP 187, Brüsszel, 2011. július 13., 12. o.

345 Általános adatvédelmi rendelet, (42) preambulumbekezdés.

hogy a szerződés teljesítésének – beleértve a szolgáltatások nyújtását is – feltételéül szabták-e az olyan személyes adatok kezeléséhez való hozzájárulást, amelyek nem szükségesek a szerződés teljesítéséhez".[346] A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kimondja, hogy „[n]em gyakorolható közvetlen vagy közvetett indokolatlan befolyásolás vagy nyomás (amely lehet gazdasági vagy más jellegű) az érintettre, és a hozzájárulás nem minősülhet szabad akaratból adottnak, amennyiben az érintettnek nincs valódi választása vagy nem tudja hozzájárulását jogsérelem nélkül megtagadni vagy visszavonni".[347]

Példa: Az „A" állam néhány önkormányzata úgy döntött, hogy beépített chipet tartalmazó tartózkodási kártyát fejleszt ki. A lakosok nem kötelesek beszerezni ezt az elektronikus kártyát. Azok a lakosok azonban, akik nem rendelkeznek ilyen kártyával, nem férnek hozzá egy sor fontos közigazgatási szolgáltatáshoz, például nem tudnak online fizetni önkormányzati adókat, nem tudnak elektronikusan panaszt benyújtani, így nem tudják igénybe venni a három napos válaszadási határidőt és elkerülni a sorbanállást, nem tudnak az önkormányzati koncertterembe kedvezményes jegyet vásárolni és használni a bejáratnál elhelyezett szkennereket.

A személyes adatok önkormányzatok általi kezelése ebben a példában nem alapulhatott hozzájáruláson. Mivel a lakosokra legalább közvetett nyomást gyakorolnak az elektronikus kártya beszerzésére és az adatkezelés elfogadásához, a hozzájárulás nem tekinthető szabad akaratból adottnak. Az önkormányzatok elektronikus kártyarendszerének fejlesztését tehát az adatkezelést indokoló másik jogszerű okra kell alapítani. Hivatkozhatnának például arra, hogy az adatkezelés közérdekből végzett feladat teljesítéséhez szükséges, ami az adatkezelés általános adatvédelmi rendelet 6. cikke (1) bekezdésének e) pontja szerinti törvényes jogalapja.[348]

A szabad akaratból tett hozzájárulás olyan alárendelt helyzetekben is kétséges lehet, amikor nincs gazdasági egyensúly a hozzájárulást biztosító adatkezelő és

346 *Uo.*, 7. cikk (4) bekezdés.

347 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

348 Lásd még: 29. cikk szerinti munkacsoport (2011), *15/2011. sz. vélemény (2011) a hozzájárulás fogalmáról*, WP 187, Brüsszel, 2011. július 13., 16. o. További példák olyan esetekre, amikor az adatkezelés nem alapulhat hozzájáruláson, hanem egy másik jogalap szükséges az adatkezelés jogszerűségéhez, a vélemény 14. és 17. oldalán olvashatók.

a hozzájárulást megadó érintett között.[349] Az ilyen egyensúlytalanság és alárendeltség tipikus példája az, amikor a munkáltató a munkaviszonnyal összefüggésben kezel személyes adatokat. A 29. cikk szerinti munkacsoport véleménye szerint „[a] munkavállalók a munkáltató és a munkavállalók közötti függőségi viszonyból eredően szinte soha nincsenek abban a helyzetben, hogy a hozzájárulásukat szabadon adják meg, tagadják meg vagy vonják vissza. Az erőviszonyok egyenlőtlensége miatt a munkavállalók csak kivételes körülmények között képesek az önkéntes hozzájárulásra, akkor, amikor az ajánlat elfogadásához vagy elutasításához semmilyen következmény nem kapcsolódik."[350]

Példa: Egy nagyvállalat – kizárólag a vállalaton belüli kommunikáció javítása céljából – névjegyzék létrehozását tervezi, amely az összes munkavállaló nevét, beosztását és munkahelyi címét tartalmazza. A személyzeti vezető fényképet is szeretne közölni minden munkavállalóról a névjegyzékben azért, hogy a kollégákat könnyebb legyen felismerni az értekezleteken. A munkavállalók képviselői szerint ezt kizárólag az egyes munkavállalók hozzájárulásával lehetne megtenni.

Ilyen helyzetben a munkavállaló hozzájárulását kellene jogalapnak elismerni a névjegyzékben szerepeltetendő fényképek kezeléséhez, mert valószínű, hogy a munkavállaló számára ez semmilyen következménnyel nem jár, függetlenül attól, hogy hozzájárul-e fényképének a névjegyzékben való közléséhez.

Példa: Az „A" vállalat megbeszélést tervez tartani három munkavállalója és a „B" vállalat igazgatói között, hogy egyeztessenek egy projekttel kapcsolatos lehetséges jövőbeli együttműködésről. A megbeszélésre a „B" vállalat épületében fog sor kerülni, amely előírja, hogy az „A" vállalat e-mailben küldje el a megbeszélés résztvevőinek nevét, önéletrajzát és fényképét. A „B" vállalat azzal érvel, hogy a résztvevők nevére és fényképére azért van szükség, hogy az épület bejáratánál a biztonsági

349 Lásd még: 29. cikk szerinti munkacsoport (2001), *8/2001. sz. vélemény a személyes adatok feldolgozásáról a foglalkoztatás kontextusában*, WP 48, Brüsszel, 2001. szeptember 13.; 29. cikk szerinti munkacsoport (2005), *Az 1995. október 24-i 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről szóló munkadokumentum*, WP 114, Brüsszel, 2005. november 25; 29. cikk szerinti munkacsoport (2017), *2/2017. sz. vélemény a munkahelyi adatkezelésről*, WP 249, Brüsszel, 2017. június 8.

350 29. cikk szerinti munkacsoport, *2/2017. sz. vélemény a munkahelyi adatkezelésről*, WP 249, Brüsszel, 2017. június 8.

szolgálat ellenőrizni tudja, hogy ők a megfelelő személyek, míg az önéletrajz lehetővé teszi, hogy az igazgatók jobban felkészüljenek a megbeszélésre. Ebben az esetben a munkavállalók személyes adatainak továbbítása az „A" vállalat által nem alapulhat hozzájáruláson. A hozzájárulás nem tekinthető „szabad akaratból adottnak", mivel előfordulhat, hogy a munkavállalók negatív következményekkel szembesülnek, ha ezt megtagadják (például lecserélik őket, és nem csak a megbeszélésre megy el a másik kolléga, hanem a „B" vállalattal való kapcsolattartást és általában a projektben való részvételt is átveszi). Ezért az adatkezelésnek az adatkezelés egy másik jogalapján kell alapulnia.

Ez nem jelenti azonban azt, hogy a hozzájárulás sosem lehet érvényes olyan körülmények között, amikor a hozzájárulás megtagadása néhány negatív következménnyel járna. Ha például egy áruházi törzsvásárlói kártya visszautasítása csupán azzal a következménnyel jár, hogy az adott személy nem kap egy csekély engedményt bizonyos áruk árából, a hozzájárulás érvényes jogalap lehet azon vásárlók személyes adatainak kezelésére, akik beleegyeztek, hogy ilyen kártyát kapjanak. Nincs alárendeltség a vállalat és a vásárló között, és a hozzájárulás megtagadásának következményei nem elég súlyosak ahhoz, hogy megakadályozzák az érintett szabad döntését (feltéve, hogy az árengedmény elég kicsi ahhoz, hogy ne befolyásolja szabad döntését).

Amennyiben azonban az áruk és szolgáltatások csak akkor szerezhetők meg, ha az érintettnek bizonyos személyes adatokat kell közölnie az adatkezelővel vagy később harmadik felekkel, az érintett hozzájárulása azon adatok közléséhez, amelyek nem szükségesek a szerződéshez, nem tekinthető szabad döntésnek, és ezért nem érvényes az adatvédelmi rendelet értelmében.[351] Az általános adatvédelmi rendelet meglehetősen szigorúan tiltja a hozzájárulás összekapcsolását áruk és szolgáltatások biztosításával.[352]

Példa: Az utasok hozzájárulása, amelyet egy légitársaságnak adtak arra vonatkozóan, hogy a légitársaság utasnyilvántartási adatokat, azaz az utasok személyazonossági adatait, étkezési szokásaival vagy egészségi problémáival kapcsolatos adatokat egy meghatározott külföldi ország bevándorlási hatóságainak továbbítson, az adatvédelmi jog értelmében nem

351 Általános adatvédelmi rendelet, 7. cikk (4) bekezdés.

352 *Uo.*

minősíthető érvényes hozzájárulásnak, mivel az utasoknak nincs választási lehetőségük, ha el szeretnének utazni a szóban forgó országba. Ha ezeket az adatokat jogszerűen szeretnék továbbítani, ahhoz a hozzájáruláson kívül más jogalap szükséges, leginkább egy külön törvény.

Tájékoztatáson alapuló hozzájárulás

Az érintettnek elegendő információval kell rendelkeznie, mielőtt döntését meghozza. A tájékoztatáson alapuló hozzájárulás rendszerint magában foglalja azon tárgy pontos és könnyen érthető leírását, amihez a hozzájárulás szükséges. A 29. cikk szerinti munkacsoport magyarázata szerint a hozzájárulás az érintettnek az adott adatkezelési cselekvéssel kapcsolatos tények és következmények értékelésén és megértésén alapuló hozzájárulását jelenti. Ezért „[a]z érintett egyénnek világos és érthető módon, pontos és teljes körű tájékoztatást kell adni valamennyi [...] releváns kérdésről, például a feldolgozott adatok természetéről, a feldolgozás céljáról, a lehetséges adattovábbítás címzettjeiről, valamint az érintettek jogairól."[353] Ahhoz, hogy a hozzájárulás tájékoztatáson alapuljon, az egyéneknek tisztában kell lenniük azzal, hogy milyen következményei lehetnek, ha valaki nem járul hozzá az adatfeldolgozáshoz.

Figyelemmel a tájékoztatáson alapuló hozzájárulás jelentőségére, az általános adatvédelmi rendelet és a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés megpróbálta tisztázni a fogalmat. Az általános adatvédelmi rendelet preambulumbekezdései kikötik, hogy a tájékoztatáson alapuló hozzájárulás azt jelenti, hogy „az érintettnek legalább tisztában kell lennie az adatkezelő kilétével és a személyes adatok kezelésének céljával".[354]

Abban a kivételes esetben, amikor a hozzájárulást eltérésként használják a nemzetközi adattovábbítás jogalapjaként, ahhoz, hogy a hozzájárulás érvényes legyen, az adatkezelőnek tájékoztatnia kell az érintettet az adattovábbításból eredő – a megfelelőségi határozat és a megfelelő garanciák hiányából fakadó – esetleges kockázatokról.[355]

353 29. cikk szerinti munkacsoport (2007), *Munkadokumentum az elektronikus egészségügyi nyilvántartásban tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról*, WP 131., Brüsszel, 2007. február 15.

354 Általános adatvédelmi rendelet, (42) preambulumbekezdés.

355 *Uo.*, 49. cikk (1) bekezdés a) pont

A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kimondja, hogy tájékoztatást kell adni az érintett döntésének vonzatairól, nevezetesen arról, hogy „mivel jár a hozzájárulás megadása, és mire terjed ki a hozzájárulás".[356]

Fontos a tájékoztatás minősége. A tájékoztatás minősége azt jelenti, hogy a tájékoztatás nyelvezetét a várható címzettekhez kell igazítani. A tájékoztatást zsargon használata nélkül, érthető és egyszerű szövegben kel megadni, amelyet egy átlagos felhasználó képes megérteni.[357] A tájékoztatásnak az érintett számára könnyen elérhetőnek kell lennie, és szóban vagy írásban adható. A tájékoztatás elérhetősége és láthatósága fontos elem: a tájékoztatásnak világosan láthatónak és szembetűnőnek kell lennie. Online környezetben jó megoldás lehet a rétegzett tájékoztató felhívás, mivel ez lehetővé teszi, hogy az érintettek eldöntsék, hogy a tájékoztatás tömör vagy részletesebb verzióját szeretnék elolvasni.

Konkrét hozzájárulás

Ahhoz, hogy a hozzájárulás érvényes legyen, az adatkezelési cél tekintetében konkrétnak is kell lennie, amit világos és egyértelmű kifejezésekkel kell körülírni. Ez együtt jár a hozzájárulás céljáról adott tájékoztatás minőségével. Ebből a szempontból az átlagos érintett észszerű elvárásai lesznek irányadók. Újra kérni kell az érintett hozzájárulását, ha az adatkezelési műveleteket olyan módon bővítik vagy megváltoztatják, ami az eredeti hozzájárulás megadásakor elvárhatóan nem volt előrelátható, és a cél módosulását eredményezi. Amikor az adatkezelésnek több célja van, a hozzájárulást valamennyi cél tekintetében meg kell adni.[358]

Példák: A *Deutsche Telekom AG* ügyben[359] az EUB azt vizsgálta, hogy egy távközlési szolgáltatónak, amely köteles előfizetői személyes adatait továbbítani, ahhoz, hogy azokat telefonkönyvekben tegyék közzé, újabb hozzájárulást kell-e kérnie az érintettektől[360], mivel az eredeti hozzájárulás megadásakor az adatok címzettjei nem voltak megnevezve.

356 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

357 Lásd még: 29. cikk szerinti munkacsoport, *15/2011. sz. vélemény a hozzájárulás fogalmáról*, WP 187, Brüsszel, 2011. július 13., 19. o.

358 Általános adatvédelmi rendelet, (32) preambulumbekezdés.

359 EUB, *Deutsche Telekom AG kontra Bundesrepublik Deutschland*, C-543/09 sz. ügy, 2011. május 5. Lásd különösen az 53. és 54. pontot.

360 Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről, HL L 201., 2002.7.31. („Elektronikus hírközlési adatvédelmi irányelv").

Az EUB megállapította, hogy az elektronikus hírközlési adatvédelmi irányelv 12. cikke alapján nem kell új hozzájárulást kérni az adatok továbbítása előtt. Mivel az érintetteknek csak arra volt lehetőségük, hogy a kezelés céljához – azaz adataik közzétételéhez – járuljanak hozzá, nem választhattak több telefonkönyv között, amelyekben az adatok közzétehetők.

Az EUB kiemelte, hogy „az elektronikus hírközlési adatvédelmi irányelv 12. cikkének összefüggés szerinti és rendszertani értelmezéséből az következik, hogy az e cikk (2) bekezdése alapján a hozzájárulás elsődlegesen a személyes adatok nyilvános telefonkönyvben való megjelentetésének céljára, nem pedig e telefonkönyv szolgáltatójára vonatkozik".[361] Továbbá „maga a személyes adatok valamely sajátos rendeltetésű telefonkönyvben való megjelentetése az, ami az előfizető számára hátrányosnak bizonyulhat",[362] nem pedig a kiadó kiléte.

A *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV kontra Autoriteit Consument en Markt (AMC)* ügy[363] egy belga vállalat azon kérésével foglalkozott, hogy kapjon hozzáférést az előfizetőkhöz telefonszámokat rendelő holland vállalkozások előfizetőinek személyes adataihoz. A belga vállalat egy az egyetemes szolgáltatási irányelv szerinti kötelezettségre támaszkodott.[364] Ez az előfizetőkhöz telefonszámokat rendelő vállalkozásokat arra kötelezi, hogy bocsássák a felperes telefonkönyv szolgáltatók rendelkezésére a telefonszámokat, ha az előfizetők hozzájárultak telefonszámuk közzétételéhez. A holland vállalatok megtagadták ezt arra hivatkozva, hogy ők nem kötelesek kiadni a szóban forgó adatokat egy másik tagállamban székhellyel rendelkező vállalkozás számára. Azzal érveltek, hogy a felhasználók azzal a feltétellel járultak hozzá telefonszámuk közzétételéhez, hogy azt egy holland telefonkönyvben teszik közzé. Az EUB megállapította, hogy az egyetemes szolgáltatási irányelv a telefonkönyv-szolgáltató vállalkozások összes kérésére kiterjed, függetlenül attól, hogy

361 EUB, *Deutsche Telekom AG kontra Bundesrepublik Deutschland*, C-543/09. sz. ügy, 2011. május 5., 61. pont.

362 *Uo.*, 62. pont.

363 EUB, *Tele2 (Netherlands) BV és társai kontra Autoriteit Consument en Markt (AMC)*, C-536/15. sz. ügy, 2017. március 15.

364 Az Európai Parlament és a Tanács 2002/22/EK irányelve (2002. március 7.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról (Egyetemes szolgáltatási irányelv), HL L 108., 2002.4.24., amelyet módosított az Európai Parlament és a Tanács 2009. november 25-i 2009/136/EK irányelve, HL L 337., 2009.12.18.

melyik tagállamban rendelkeznek székhellyel. Az EUB azt is megállapította, hogy ugyanezen adatok továbbítása valamely nyilvános telefonkönyvet megjelentetni szándékozó másik vállalkozáshoz az előfizető újabb hozzájárulása nélkül nem sértheti a személyes adatok védelméhez való jog lényegét.[365] Következésképpen az előfizetőihez telefonszámokat rendelő vállalkozásnak az előfizetőhöz intézett hozzájárulás-kérést nem kell úgy megfogalmaznia, hogy az előfizető ezt a hozzájárulását eltérő módon adja meg azon tagállamtól függően, amelybe az őt érintő adatok továbbíthatók.[366]

Egyértelmű hozzájárulás

A hozzájárulást minden esetben egyértelműen kell megadni.[367] Ez azt jelenti, hogy nem szabad, hogy kétség maradjon afelől, hogy az érintett ki akarta fejezni hozzájárulását adatainak kezeléséhez. Például, az érintett nem cselekvése nem jelent egyértelmű hozzájárulást.

Ez lenne a helyzet akkor, ha az adatkezelők adatvédelmi nyilatkozatukban például a következő megfogalmazással szereznék be a hozzájárulást: „szolgáltatásaink használatával Ön hozzájárul személyes adatainak kezeléséhez". Ebben az esetben az adatkezelőknek biztosítaniuk kellene, hogy a felhasználók kézzel és egyedileg adják hozzájárulásukat az ilyen nyilatkozatokban.

Ha a hozzájárulást egy szerződés részeként írásban adják meg, a személyes adatok kezeléséhez való hozzájárulást személyre kell szabni, és minden esetben „garanciákkal szükséges biztosítani azt, hogy az érintett tisztában legyen azzal a ténnyel, hogy hozzájárulását adta, valamint azzal, hogy ezt milyen mértékben tette."[368]

Gyermekek hozzájárulásával szemben támasztott követelmények

Az általános adatvédelmi rendelet különös védelmet biztosít a gyermekek számára az információs társadalommal összefüggő szolgáltatások nyújtásával kapcsolatban, mivel „ők kevésbé lehetnek tisztában a személyes adatok kezelésével összefüggő kockázatokkal, következményeivel és az ahhoz kapcsolódó garanciákkal és

365 EUB, *Tele2 (Netherlands) BV és társai kontra Autoriteit Consument en Markt (AMC)*, C-536/15. sz. ügy, 2017. március 15., 36. pont.

366 *Uo.*, 40–41. pont.

367 Általános adatvédelmi rendelet, 4. cikk 11. pont.

368 *Uo.*, (42) preambulumbekezdés.

jogosultságokkal".[369] Ezért az **uniós jog** alapján amikor az információs társadalommal összefüggő szolgáltatások nyújtói 16. életévét be nem töltött gyermek személyes adatait kezelik hozzájárulás alapján, a gyermekek személyes adatainak kezelése „csak akkor és olyan mértékben jogszerű, ha a hozzájárulást a gyermek feletti szülői felügyeletet gyakorló adta meg, illetve engedélyezte.[370] A tagállamok nemzeti jogukban alacsonyabb korhatárt is előírhatnak, azonban az nem lehet 13 évnél alacsonyabb.[371] A szülői felelősség gyakorlójának hozzájárulása nem szükséges a „közvetlenül a gyermek részére nyújtott megelőzési és tanácsadási szolgáltatások esetében."[372] Amikor az adatkezelésre vonatkozó tájékoztatás és kommunikáció címzettje gyermek, ezek nyelvezetének világosnak és egyszerűnek, a gyermek számára könnyen érthetőnek kell lennie.[373]

A hozzájárulás bármely időpontban való visszavonásának joga

Az általános adatvédelmi rendelet tartalmaz egy általános jogot a hozzájárulás bármely időpontban való visszavonására.[374] Erről a jogáról az érintettet a hozzájárulás megadása előtt tájékoztatni kell, és ezt a jogot tetszése szerint gyakorolhatja. Nem szabad olyan követelményt előírni, hogy a visszavonást indokolni kell, és a korábbi beleegyezéssel történő adathasználatból következő bármely előny megszűnésén túl semmiféle egyéb negatív következmény nem állhat be. A hozzájárulás visszavonását ugyanolyan egyszerű módon kell lehetővé tenni, mint annak megadását.[375] Nem lehet szó szabad akaratból tett hozzájárulásról, ha az érintett nem tudja anélkül visszavonni hozzájárulását, hogy hátrányt ne szenvedjen, vagy ha a hozzájárulás visszavonása nem olyan egyszerű, mint annak megadása.[376]

Példa: Egy vásárló hozzájárul, hogy az általa az adatkezelőnek megadott címre reklámlevelet kapjon. Ha a vásárló visszavonja hozzájárulását, az adatkezelőnek azonnal le kell állítania a reklámlevél küldését. A leállítás

369 *Uo.*, (38) preambulumbekezdés.

370 *Uo.*, 8. cikk (1) bekezdés első franciabekezdés. Az információs társadalommal összefüggő szolgáltatások fogalmának meghatározását az általános adatvédelmi rendelet 4. cikkének 25. pontja tartalmazza.

371 Általános adatvédelmi rendelet, 8. cikk (1) bekezdés második franciabekezdés.

372 *Uo.*, (38) preambulumbekezdés.

373 *Uo.*, (58) preambulumbekezdés. Lásd még: Korszerűsített 108. Egyezmény, 15. cikk (2) bekezdés e) pont; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 68. és 125. pont.

374 Általános adatvédelmi rendelet, 7. cikk (3) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 45. pont.

375 Általános adatvédelmi rendelet, 7. cikk (3) bekezdés.

376 *Uo.*, (42) preambulumbekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 42. pont.

semmiféle büntető jellegű következménnyel, például díj kiszabásával nem járhat. A visszavonás azonban a jövőre szól, visszamenőleges hatálya nincs. Az az időszak, amely alatt az ügyfél személyes adatait jogszerűen kezelték – mivel ahhoz az ügyfél hozzájárult –, törvényesnek minősül. A hozzájárulás visszavonása megakadályozza az adatok további kezelését, kivéve, ha az adatkezelés a törléshez való jognak megfelelően történik.[377]

Szerződés teljesítésének szükségessége

Az uniós jogban az általános adatvédelmi rendelet 6. cikke (1) bekezdésének b) pontja biztosítja a jogszerű adatkezelés egy másik jogalapját, mégpedig, ha az adatkezelés „olyan szerződés teljesítéséhez szükséges, amelyben az érintett az egyik fél" Ez a rendelkezés a szerződéskötés előtti jogviszonyokra is vonatkozik. Azokban az esetekben például, ahol egy fél szerződést kíván kötni, de még nem kötötte meg – esetleg mert még bizonyos ellenőrzések hátra vannak. Ha ehhez az egyik félnek adatokat kell feldolgoznia, ez az adatfeldolgozás törvényes, amennyiben „az a szerződés megkötését megelőzően az érintett kérésére történő lépések megtételéhez szükséges".[378]

Az adatkezelés fogalma, mint a Korszerűsített 108. Egyezmény 5. cikkének (2) bekezdésében rögzített „törvényben meghatározott jogalap" kiterjed „egy olyan szerződés (vagy előszerződéses intézkedés érintett kérésére történő) teljesítése érdekében végzett adatkezelésre, amelyben az érintett az egyik fél".[379]

Az adatkezelő jogszabályi kötelezettségei

Az **uniós jog** az adatkezelést jogszerűvé tevő másik kritériumot is meghatároz, mégpedig, ha „az adatkezelés az adatkezelőre vonatkozó jogszabályi kötelezettség teljesítéséhez szükséges" (általános adatvédelmi rendelet 6. cikk (1) bekezdésének c) pontja). Ez a rendelkezés a magán és állami szektorban működő adatkezelőkre egyaránt vonatkozik; az állami szektorban működő adatkezelők jogszabályi kötelezettségei szintén az általános adatvédelmi rendelet 6. cikk (1) bekezdésének

377 Általános adatvédelmi rendelet, 17. cikk (1) bekezdés b) pont.

378 *Uo.*, 6. cikk (1) bekezdés b) pont.

379 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 46. pont; Európa Tanács, Miniszteri Bizottság, CM/Rec(2010)13. sz. ajánlás a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről, 2010. november 23., 3.4. cikk b) pont.

e) pontja hatálya alá tartozhatnak. Számos példa létezik az olyan helyzetekre, amikor törvény kötelezi a magánszektorbeli adatkezelőket arra, hogy konkrét érintettekre vonatkozó adatokat kezeljenek. A munkáltatóknak például kezelniük kell munkavállalóik adatait társadalombiztosítási és adózási okokból, és a vállalkozásoknak az ügyfeleikkel kapcsolatos adatokat kell kezelniük adózási célból.

A jogszabályi kötelezettség eredhet uniós vagy tagállami törvényből, ami egy vagy több adatkezelési művelet jogalapjául szolgálhat. Jogszabályban kell meghatározni az adatkezelés célját, az adatkezelő megjelölésére vonatkozó pontos szabályokat, az adatkezelés tárgyát képező személyes adatok típusát, az érintetteket, azokat a szervezeteket, amelyekkel a személyes adatok közölhetők, az adatkezelés céljára vonatkozó korlátozásokat, az adattárolás időtartamát, valamint egyéb, a jogszerű és tisztességes adatkezelés biztosításához szükséges intézkedéseket is.[380] Minden olyan jogszabálynak, amely a személyes adatok kezelésének alapját képezi, összhangban kell lennie a Charta 7. és 8. cikkével, valamint az EJEE 8. cikkével.

Az adatkezelő jogszabályi kötelezettségei is a jogszerű adatkezelés jogalapját képezik **az Európa Tanács szabályozása szerint**.[381] Ahogy arra korábban már rámutattunk, a magánszektorbeli adatkezelő jogi kötelezettségeinek teljesítése csak egy konkrét példa az EJEE 8. cikkének (2) bekezdésében említett mások jogos érdekeire. Ezért az a példa, amelyben a munkáltatók a munkavállalóik adatait kezelik releváns az Európa Tanács szabályozása szempontjából is.

Az érintett vagy más természetes személy létfontosságú érdekei

Az **uniós jogban** az általános adatvédelmi rendelet 6. cikke (1) bekezdésének d) pontja rendelkezik arról, hogy az adatkezelés jogszerű, ha az „az érintett vagy egy másik természetes személy létfontosságú érdekeinek védelme miatt szükséges". Csak akkor lehet hivatkozni a személyes adatok más természetes személy létfontosságú érdekéből történő kezelésének jogszerű okára, ha adatkezelés „egyéb jogalapon nem végezhető".[382] Néha az adatkezelés valamely típusa történhet egyszerre közérdek és az érintett vagy más személy létfontosságú érdekei alapján. Ez a helyzet például járványok és azok alakulásának nyomon követésekor, vagy humanitáriánus vészhelyzet esetén.

380 Általános adatvédelmi rendelet, (45) preambulumbekezdés.

381 Európa Tanács, Miniszteri Bizottság, CM/Rec(2010)13. sz. ajánlás a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről, 2010. november 23., 3.4. cikk a) pont.

382 Általános adatvédelmi rendelet, (46) preambulumbekezdés.

Az **Európa Tanács** szabályozásában az érintett létfontosságú érdekei nem szerepelnek az EJEE 8. cikkében. Az érintett létfontosságú érdekeinek figyelembevétele azonban következik a Korszerűsített 108. Egyezmény 5. cikkének (2) bekezdésében foglalt „jogalap" fogalmából is, amely a személyes adatok kezelésének jogszerűségével foglalkozik.[383]

Közérdek és hivatali hatáskör gyakorlása

Figyelemmel a közügyek szervezésének számos lehetséges módjára, az általános adatvédelmi rendelet 6. cikke (1) bekezdésének e) pontja úgy rendelkezik, hogy személyes adatok akkor is jogszerűen feldolgozhatók, ha „közérdekből elvégzendő feladat végrehajtása vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása érdekében szükséges [...]".[384]

Példa: A *Heinz Huber kontra Bundesrepublik Deutschland* ügyben[385] H. Hube, egy Németországban élő osztrák állampolgár azzal a kéréssel fordult a Szövetségi Bevándorlási és Menekültügyi Hivatalhoz, hogy a külföldiek központi nyilvántartásából („AZR") töröljék a rá vonatkozó adatokat. Ezt a nyilvántartást, amely nem német, de a három hónapnál hosszabb ideig Németországban élő uniós állampolgárok személyes adatait tartalmazza, bűnüldöző és igazságszolgáltatási hatóságok használják statisztikai célokra, amikor bűncselekmények vagy a közbiztonságot veszélyeztető tevékenységek ügyében nyomoznak és emelnek vádat. A kérdést előterjesztő bíróság azt a kérdést tette fel, hogy az olyan nyilvántartásban végzett személyesadat-feldolgozás, mint pl. a külföldiek központi nyilvántartása, amelyhez más hatóságoknak is van hozzáférésük, összhangban áll-e az uniós joggal – tekintettel arra, hogy német állampolgárokra vonatkozóan ilyen nyilvántartás nem létezik.

383 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 46. pont.

384 Lásd az általános adatvédelmi rendelet (45) preambulumbekezdését.

385 EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008. december 16.

Az EUB először is megállapította, hogy az irányelv 7. cikkének e) pontja[386] értelmében személyes adatok csak akkor dolgozhatók fel jogszerűen, ha az adatfeldolgozás közérdekből elvégzendő feladat végrehajtásához vagy hivatali hatáskör gyakorlásához szükséges.

Az EUB szerint „tekintettel arra a célkitűzésre, hogy valamennyi tagállamban azonos védelmi szintet kell biztosítani, a 95/46/EK irányelv 7. cikkének e) pontja[387] szerinti szükségesség fogalma [...] nem lehet eltérő tartalmú az egyes tagállamokban. Ennek következtében önálló közösségi jogi fogalomról van szó, amelyet oly módon kell értelmezni, hogy az maradéktalanul megfeleljen ezen irányelv célkitűzésének, amint az annak 1. cikke (1) bekezdéséből következik. "[388]

Az EUB megállapította, hogy az uniós polgároknak egy olyan másik tagállam területén történő szabad mozgáshoz való joga, amelynek nem állampolgárai, nem feltétlen, hanem az Európai Közösséget létrehozó szerződésben, valamint a végrehajtására hozott rendelkezésekben előírt korlátozások és feltételek betartásához köthető. Ennek megfelelően, ha főszabályként jogszerű, hogy egy tagállam az AZR-hez hasonló nyilvántartással támogassa a tartózkodási joggal kapcsolatos jogszabályok alkalmazásáért felelős hatóságokat, egy ilyen nyilvántartás kizárólag az adott célhoz szükséges információkat tartalmazhatja. Az EUB arra következtetésre jutott, hogy egy ilyen személyesadat-kezelési rendszer akkor felel meg az uniós jognak, ha kizárólag a szóban forgó jogszabályok alkalmazásához szükséges adatokat tartalmazza, és ha központi jellege e jogszabályok alkalmazását hatékonyabbá teszi. A nemzeti bíróság feladata, hogy ezeket a körülményeket a konkrét ügyben megvizsgálja. Semmiképpen sem tekinthető azonban a 95/46/EK irányelv 7. cikkének e) pontja[389] értelmében szükségesnek a névhez kötődő személyes adatoknak az AZR-hez hasonló nyilvántartásban statisztikai célból történő feldolgozása.[390]

386 A korábbi adatvédelmi irányelv 7. cikkének (1) bekezdése, most az általános adatvédelmi rendelet 6. cikkének (1) bekezdése.

387 *Uo.*

388 EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008. december 16., 52. pont.

389 A korábbi adatvédelmi irányelv 7. cikkének e) pontja, most az általános adatvédelmi rendelet 6. cikke (1) bekezdésének e) pontja.

390 EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008. december 16., 54., 58–59. és 66–68. pont.

Végül, a nyilvántartásban szereplő adatoknak a bűnözés elleni küzdelem céljára való felhasználásával kapcsolatban az EUB megállapítja, hogy ez a cél „szükségszerűen a bűncselekményeknek és szabálysértéseknek az elkövetők állampolgárságától független történő üldözését jelenti". A szóban forgó nyilvántartás nem tartalmaz az érintett tagállam állampolgáraira vonatkozó személyes adatokat, ez az eltérő bánásmód viszont kimeríti az EUMSZ 18. cikk által tiltott megkülönböztetés fogalmát. Következésképpen az EUB megállapította, hogy ez a rendelkezés „azzal ellentétes, ha valamely tagállam a bűnözés elleni küzdelem céljából a személyes adatok feldolgozásának olyan rendszerét vezeti be, amely csak azon uniós polgárokra vonatkozik, akik nem e tagállam állampolgárai".[391]

A személyes adatok közügyekben eljáró hatóságok általi felhasználása az **EJEE** 8. cikkének hatálya alá tartozik, valamint – amennyiben megfelelő – vonatkozik rá a Korszerűsített 108. Egyezmény 5. cikk (2) bekezdése..[392]

Az adatkezelő vagy harmadik fél által előmozdított jogos érdekek

Az **uniós jog** értelmében nem az érintett az egyetlen, akinek jogos érdekei vannak. Az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja úgy rendelkezik, hogy személyes adatok akkor kezelhetők jogszerűen, ha „az adatkezelés az adatkezelő vagy egy harmadik fél [kivéve a hatóságokat feladatuk elvégzése során] jogos érdekeinek érvényesítéséhez szükséges, kivéve, ha ezen érdekekkel szemben elsőbbséget élveznek az érintett olyan érdekei vagy alapvető jogai és szabadságai, amelyek személyes adatok védelmét teszik szükségessé [...]".[393]

A jogos érdek fennállását minden egyedi esetben körültekintően kell megvizsgálni.[394] Ha az adatkezelő jogos érdekei meghatározásra kerültek, megfelelő egyensúlyt kell teremteni ezen érdekek és az érintett érdekei, illetve alapvető jogai és szabadságai között.[395] Egy ilyen vizsgálat során mérlegelni kell az érintett észszerű elvárásait annak megállapítására, hogy az adatkezelő érdekei nem élveznek-e

391 *Uo.*, 78. és 81. pont.

392 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 46–47. pont.

393 A 95/46 irányelvvel összehasonlítva az általános adatvédelmi rendelet több példát hoz az olyan esetekre, amelyek jogos érdeknek minősülnek.

394 Általános adatvédelmi rendelet, (47) preambulumbekezdés.

395 29. cikk szerinti munkacsoport (2014), *06/2014. sz. vélemény az adatkezelő 95/46/EK irányelv 7. cikke szerinti jogszerű érdekeinek fogalmáról*, 2014. április 4.

elsőbbséget az érintett alapvető jogaival és érdekeivel szemben.[396] Ha az érintett jogai elsőbbséget élveznek az adatkezelő jogos érdekeivel szemben, az adatkezelő intézkedéseket tehet és garanciákat alkalmazhat annak biztosítására, hogy minimalizálja az érintett jogaira gyakorolt hatást (például az adatok álnevesítése), és megfordítsa az „egyensúlyt" az előtt, hogy jogszerűen támaszkodhatna az adatkezelésnek erre a jogalapjára. Az adatkezelő jogos érdekeinek fogalmára vonatkozó véleményében a 29. cikk szerinti munkacsoport kiemelte az elszámoltathatóság és átláthatóság rendkívül fontos szerepét, valamint az érintett jogát, hogy tiltakozzon adatainak kezelése ellen, illetve, hogy hozzáférjen azokhoz, módosítsa, törölje vagy továbbítsa azokat az adatkezelő jogos érdekeinek és az érintett alapvető jogainak összeegyeztetésekor.[397]

Az általános adatvédelmi rendelet preambulumbekezdései néhány példát szolgáltatnak arra, hogy mi minősül az érintett adatkezelő jogos érdekének. A személyes adatok kezelése például megengedett az érintett hozzájárulása nélkül, ha az közvetlen üzletszerzés érdekében történik, vagy amikor az ilyen adatkezelés „a csalások megelőzése céljából feltétlenül szükséges ".[398]

Ítélkezési gyakorlatában az EUB kiterjesztette annak vizsgálatát, hogy mi minősül jogos érdeknek.

Példa: A *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde* ügy[399] egy rigai tömegközlekedési vállalat trolibuszát ért kárral foglalkozott, amelyet egy taxi ajtajának utas általi hirtelen kinyitása okozott. A Rīgas satiksme be akarta perelni az utast. A rendőrség azonban csak az utas nevét adta ki, és megtagadta az utas személyigazolvány számának és címének kiadását arra hivatkozva, hogy ezen adatok közlése a nemzeti adatvédelmi jogszabályok értelmében törvénytelen lenne.

396 *Uo.*

397 *Uo.*

398 Általános adatvédelmi rendelet, (47) preambulumbekezdés.

399 EUB, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde kontra Rīgas pašvaldības SIA „Rīgas satiksme"*, C-13/16. sz. ügy, 2017. május 4.

Az eljáró lett bíróság előzetes döntéshozatal iránti kérelmet nyújtott be az EUB-nak arra vonatkozóan, hogy az uniós adatvédelmi jog kötelezővé teszi-e a közigazgatási szabálysértésben feltételezetten felelős személy ellen polgári peres eljárás megindításához szükséges valamennyi személyes adat közlését.[400]

Az EUB tisztázta, hogy az uniós adatvédelmi törvény lehetőséget biztosít – nem pedig kötelezettséget ró – valamely harmadik fél jogos érdekének érvényesítéséhez szükséges adatok adott féllel való közlésére.[401] Az EUB három együttes feltételt határozott meg, amelyeknek teljesülniük kell ahhoz, hogy a személyes adatok kezelése a „jogos érdekek" jogalapján jogszerű legyen.[402] Először is, annak a harmadik félnek, akivel az adatokat közlik, jogos érdeket kell érvényesítenie. Ebben a konkrét esetben ez azt jelenti, hogy a személyes adatok kiadásának kérelmezése azért, hogy bepereljenek egy vagyoni kárt okozó személyt, harmadik fél jogos érdekének minősül. Másodszor, a személyes adatok kezelése valamely jogos érdek érvényesítéséhez szükségesnek kell lennie. Ebben az esetben az olyan személyes adatok, mint a cím, és/vagy személyi igazolvány szám feltétlenül szükséges az illető személy azonosításához. Harmadszor pedig az adatvédelemmel érintett személy alapvető jogai és szabadságai nem lehetnek magasabb rendűek az adatkezelő vagy harmadik felek jogos érdekénél. Az érdekek közötti megfelelő egyensúlyt eseti alapon kell megteremteni, figyelembe véve az olyan elemeket, mint az érintett jogai megsértésének súlyossága, vagy – egyes esetekben – akár az érintett életkora. Ebben a konkrét ügyben azonban az EUB nem tekintette indokoltnak az adatok közlésének megtagadását pusztán azért, mert az érintett kiskorú volt.

Az *ASNEF és FECEMD* ítéletben az EUB kifejezetten a „jogos érdek" jogalap alapján végzett adatkezeléssel foglalkozott, amelyet akkoriban az adatvédelmi irányelv 7. cikkének f) pontja rögzített.[403]

400 *Uo.*, 23. pont.

401 *Uo.*, 26. pont.

402 *Uo.*, 28–34. pont.

403 A korábbi adatvédelmi irányelv 7. cikkének f) pontja, most az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja.

Példa: Az *ASNEF és FECEMD* ügyben[404] az EUB tisztázta, hogy a nemzeti jog nem egészítheti ki az irányelv 7. cikkének f) pontjában a jogszerű adatkezelésre vonatkozóan említett feltételeket.[405] Az ügyben az alaphelyzet az volt, hogy a spanyol adatvédelmi törvény olyan rendelkezést tartalmazott, miszerint személyesadat-kezelés kapcsán más magánfelek csak akkor hivatkozhatnak jogos érdekre, ha az adatok a nyilvánosság számára hozzáférhető forrásokban már szerepeltek.

Az EUB először is megállapította, hogy a 95/46/EK irányelv[406] célja, hogy minden tagállamban azonossá tegye az egyének jogai és szabadságai védelmének szintjét a személyes adatok kezelése terén. Ugyanígy, az ezen a területen alkalmazandó nemzeti jogszabályok közelítése nem vezethet az általuk nyújtott védelem szintjének csökkenéséhez. Sőt, magas védelmi szintet kell, hogy biztosítson az Unión belül.[407] Következésképpen az EUB megállapította, hogy „abból a célkitűzésből, amelynek lényege az azonos védelmi szint biztosítása valamennyi tagállamban, az következik, hogy a 95/46 irányelv 7. cikke[408] kimerítő és korlátozó jellegű felsorolását írja elő azon eseteknek, amelyekben a személyes adatok kezelése jogszerűnek minősíthető". Ezenfelül, „a tagállamok nem alkothatnak a személyes adatok kezelésének megengedhetőségére vonatkozó, az ezen irányelv 7. cikkében[409] szereplőkhöz képest új elveket, és olyan további követelményeket sem írhatnak elő, amelyek módosítanák az e cikkben előírt elvek akár egyikének a hatályát".[410] Az EUB elismerte, hogy „a 95/46 irányelv 7. cikkének f) pontja értelmében szükséges súlyozást illetően figyelembe vehető, hogy

404 EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24.

405 A korábbi adatvédelmi irányelv 7. cikkének f) pontja, most az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja.

406 Korábbi adatvédelmi irányelv, most általános adatvédelmi rendelet.

407 EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24., 28. pont. Lásd az adatvédelmi irányelv (8) és (10) preambulumbekezdését.

408 A korábbi adatvédelmi irányelv 7. cikke, most az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja.

409 A korábbi adatvédelmi irányelv 2. cikke, most az általános adatvédelmi rendelet, 6. cikke.

410 *Uo.*

az érintett személy alapvető jogainak a hivatkozott adatkezelés általi sérelme súlyossága azon ténytől függően változhat, hogy a szóban forgó adatok szerepelnek-e már a nyilvánosság által hozzáférhető forrásokban, vagy sem".

Azonban az „irányelv 7. cikkének f) pontjával ellentétes az, ha valamely tagállam bizonyos kategóriákba tartozó személyes adatok tekintetében kategorikusan és általánosan kizárja ezek kezelhetőségét anélkül, hogy lehetővé tenné a szóban forgó ellentétes érdekek és jogok súlyozását az egyes esetekben".

A fenti megfontolásokra figyelemmel az EUB arra a következtetésre jutott, hogy „a 95/46 irányelv 7. cikkének f) pontját[411] úgy kell értelmezni, hogy azzal ellentétes az olyan nemzeti szabályozás, amely az érintett hozzájárulásának hiányában, és annak érdekében, hogy lehetővé tegye az érintett személyes adatainak feldolgozását – ami az adatkezelő vagy azon harmadik személyek jogos érdekének kielégítéséhez szükséges, akikkel az adatokat közlik –, azt is előírja azonfelül, hogy ne sérüljenek a személy alapvető jogai és szabadságai, hogy adatai a nyilvánosság számára hozzáférhető forrásokban szerepeljenek, kategorikusan és általánosan kizárva ily módon az ilyen forrásokban nem szereplő adatok bármely kezelését".[412]

Minden esetben, amikor a személyes adatok kezelése „jogos érdekek" alapján történik, az egyénnek joga van bármikor tiltakozni az adatkezelés ellen a saját egyéni helyzetével kapcsolatos okokból az általános adatvédelmi rendelet 2. cikke (1) bekezdésének megfelelően. Az adatkezelő köteles megszüntetni az adatkezelést, kivéve, ha igazolja, hogy folytatását kényszerítő erejű jogos okok indokolják.

Az **Európa Tanács szabályozását illetően,** a Korszerűsített 108. Egyezményben[413] és az Európa Tanács ajánlásaiban is hasonló megfogalmazások szerepelnek. A profilalkotásra vonatkozó ajánlás akkor ismeri el jogszerűnek a profilalkotási célokra végzett személyesadat-kezelést, ha az mások jogos érdekeinek védelme érdekében szükséges, „kivéve amennyiben az ilyen érdekeket megelőzik az érintett alapvető

411 A korábbi 95/46/EK irányelvadatvédelmi irányelv 7. cikkének f) pontja, most az általános adatvédelmi rendelet 6. cikke (1) bekezdésének f) pontja.

412 EUB, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado*, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24., 40., 44. és 48–49. pont.

413 Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 46. pont.

jogaihoz és szabadságaihoz fűződő érdekek".[414] Ezenkívül az EJEE 8. cikkének (2) bekezdése az adatvédelemhez való jog egyik jogszerű okaként megemlíti a „mások jogainak és szabadságának a védelmét".

Példa: Az *Y kontra Törökország* ügyben[415] a felperes HIV pozitív volt. Mivel kórházba érkezésekor eszméletlen volt, a mentősök tájékoztatták a kórházi dolgozókat arról, hogy HIV pozitív. A felperes az EJEB előtt azzal érvelt, hogy ennek az információnak a közlése megsértette a magánélet tiszteletben tartásához való jogát. Figyelemmel azonban arra, hogy szükséges a kórházi személyzet biztonságának védelme, ezt nem tekintették joga megsértésének.

4.1.2 Különleges adatkategóriák (különleges adatok) kezelése

Az **Európa Tanács joga** a hazai törvényre bízza a különleges adatok használata tekintetében a megfelelő védelem meghatározását, feltéve ha a Korszerűsített 108. Egyezmény 6. cikkében foglalt feltételek teljesülnek, azaz a törvény az egyezmény más rendelkezéseit kiegészítő, megfelelő garanciákat tartalmaz. Az **uniós jog** az általános adatvédelmi rendelet 9. cikkében részletes szabályokat tartalmaz a személyes adatok különleges kategóriáinak (vagy különleges adatok) kezelésére. Ezek az adatok faji eredetre vagy etnikai hovatartozásra, a politikai véleményre, a vallásos vagy filozófiai meggyőződésre, a szakszervezeti tagságra vonatkoznak, valamint a természetes személyek egyedi azonosítását célzó genetikai és biometrikus adatok kezelésére, továbbá az egészségügyi adatok és a természetes személyek szexuális életére vagy szexuális irányultságára vonatkozó személyes adatok tekintetében. Főszabályként a különleges adatok kezelése nem megengedett.[416]

Létezik ugyanakkor egy, az e tilalom alóli kivételeket tartalmazó átfogó lista, amely a rendelet 9. cikkének (2) bekezdésében található, és amely törvényes jogalapul

414 Európa Tanács, Miniszteri Bizottság, CM/Rec(2010)13. sz. ajánlás és magyarázó megjegyzések a tagállamok részére a profilalkotással összefüggésben az egyéneknek a személyes adatok gépi feldolgozása során való védelméről, 2010. november 23., 3.4. cikk b) pont (a profilalkotásra vonatkozó ajánlás).

415 EJEB, *Y kontra Törökország*, 648/10. sz. ügy, 2015. február 17.

416 A korábbi adatvédelmi irányelv 7. cikkének f) pontja, most az általános adatvédelmi rendelet 9. cikkének (1) bekezdése.

szolgál a különleges adatok kezeléshez. Ezek a kivételek azokat a helyzeteket foglalják magukban, amelyekben:

- az érintett kifejezett hozzájárulását adta az adatok kezeléséhez;
- az adatkezelést valamely politikai, világnézeti, vallási vagy szakszervezeti célú nonprofit szervezet végzi jogszerű tevékenysége keretében, és az adatkezelés kizárólag az ilyen szerv jelenlegi (vagy volt) tagjaira, vagy olyan személyekre vonatkozik, akik a szervezettel rendszeres kapcsolatban állnak a szervezet céljaihoz kapcsolódóan;
- az adatkezelés olyan személyes adatokra vonatkozik, amelyeket az érintett kifejezetten nyilvánosságra hozott;
- az adatkezelés szükséges:
  - az adatkezelőnek vagy az érintettnek a foglalkoztatást, valamint a szociális biztonságot és szociális védelmet szabályozó jogi előírásokból fakadó kötelezettségei teljesítése és konkrét jogai gyakorlása érdekében;
  - az adatkezelés az érintett vagy más természetes személy létfontosságú érdekeinek védelméhez szükséges (ha az érintett nem képes a hozzájárulását megadni);
  - jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez szükséges, vagy amikor a bíróságok igazságszolgáltatási feladatkörükben járnak el;
  - megelőző egészségügyi vagy munkahelyi egészségügyi célokból szükséges: „a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében";
  - a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból;
  - a népegészségügy területét érintő közérdekből; vagy

- jelentős közérdek miatt.

A különleges adatkategóriák kezeléséhez az érintettel fennálló szerződéses jogviszony tehát nem minősül a különleges adatok kezelése törvényes jogalapjának, kivéve a szakmai titoktartás alá tartozó egészségügyi szakemberrel kötött szerződést.[417]

Az érintett kifejezett hozzájárulása

Az **uniós jog** értelmében bármely adat jogszerű kezelésének első feltétele – függetlenül attól, hogy különleges vagy nem különleges adatról van-e szó – az érintett hozzájárulása. Különleges adatok esetében a hozzájárulásnak kifejezettnek kell lennie. Uniós vagy tagállami jog azonban rendelkezhet úgy, hogy a különleges adatkategóriák kezelésére vonatkozó tilalom nem oldható fel az érintett hozzájárulásával.[418] Ez a helyzet áll fenn például, ha az adatkezelés az érintettre nézve szokatlan kockázattal jár.

A foglalkoztatást, illetve a szociális biztonságot és szociális védelmet szabályozó jogi előírások

Az **uniós jog** alapján a 9. cikk (1) bekezdése alól felmentés adható, ha az adatkezelés szükséges az adatkezelő vagy az érintett kötelezettségei teljesítése és jogai gyakorlása érdekében a foglalkoztatás vagy társadalom biztosítás területén. Az adatkezelés szükségességét azonban az uniós jognak, nemzeti jognak vagy a nemzeti jog alá tartozó kollektív szerződésnek kell lehetővé tennie, amely garanciákat biztosít az érintett alapvető jogai és érdekei védelmére.[419] Valamely szervezet által vezetett foglalkoztatási nyilvántartás az általános adatvédelmi rendeletben és a vonatkozó nemzeti jogban meghatározott feltételek mellett tartalmazhat különleges adatokat. A különleges adatok közé tartozhat a szakszervezeti tagság vagy egészségügyi információ.

Az érintett vagy más személy létfontosságú érdekei

Az **uniós jog** értelmében,akárcsak a nem különleges adatok esetében, a különleges adatok is kezelhetők az érintett vagy más természetes személy létfontosságú

417 Általános adatvédelmi rendelet, 9. cikk (2) bekezdés h) és i) pont.

418 *Uo.*, 9. cikk (2) bekezdés a) pont.

419 *Uo.*, 9. cikk (2) bekezdés b) pont.

érdekeinek védelmében.[420] Amennyiben az adatkezelés más személy létfontosságú érdekei alapján történik, erre a jogszerű okra csak akkor lehet hivatkozni, hogy az adatkezelés „egyéb jogalapon nem végezhető".[421] Néhány esetben a személyes adatok kezelése egyéni és közérdeket is védhet, például akkor, amikor az adatkezelés humanitárius célokból történik.[422]

Ahhoz, hogy a különleges adatok e jogcímen való kezelése jogszerű legyen, szükséges, hogy a hozzájárulásra irányuló kérdést ne lehessen feltenni az érintettnek például azért, mert nem volt tudatánál, távol volt vagy nem volt elérhető. Más szavakkal, a személy fizikailag vagy jogilag képtelen hozzájárulását adni.

Jótékony vagy nonprofit szervezetek

A személyes adatok kezelése alapítványok, egyesületek vagy egyéb nonprofit szervezetek jogszerű tevékenysége során is megengedett valamely politikai, világnézeti, vallási vagy szakszervezeti célból. Az adatkezelés azonban kizárólag a szervezet jelenlegi vagy volt tagjaira vonatkozhat, akik a szervezettel rendszeres kapcsolatban állnak.[423] A különleges adatok az érintett hozzájárulása nélkül nem tehetők hozzáférhetővé a szervezeten kívül.

Az érintett által kifejezetten nyilvánosságra hozott adatok

Az általános adatvédelmi rendelet 9. cikke (2) bekezdésének e) pontja úgy rendelkezik, hogy az adatkezelés nem tilos, ha olyan adatokra vonatkozik, amelyeket az érintett egyértelműen nyilvánosságra hozott. Annak ellenére, hogy a rendelet nem határozza meg a „kifejezetten nyilvánosságra hozott" jelentését, mivel ez kivételt képez a különleges adatok kezelésének tilalma alól, szigorúan kell értelmezni, és akként, hogy ehhez az szükséges, hogy az érintett szándékosan nyilvánosságra hozza személyes adatait. Akkor tehát, amikor a televízió egy biztonsági kamera felvételét teszi közzé, amelyben többek között az látható, hogy egy tűzoltó megsérül, miközben megpróbál kiüríteni egy ingatlant, nem tekinthető úgy, hogy a tűzoltó kifejezetten közzétette az adatokat. Másrészt viszont, ha a tűzoltó úgy dönt, hogy ismerteti az incidenst és egy nyilvános internetes oldalon videót és fényképeket tesz közzé, ezzel szándékos, megerősítő cselekedetet tesz a személyes adatok

420 *Uo.*, 9. cikk (2) bekezdés c) pont.

421 *Uo.*, (46) preambulumbekezdés.

422 *Uo.*

423 *Uo.*, 9. cikk (2) bekezdés d) pont.

nyilvánosságra hozatalára. Fontos megjegyezni, hogy egy személy adatainak nyilvánosságra hozatala nem jelent hozzájárulást, azonban egy további engedélyt jelent az adatok különleges kategóriáinak kezelésére.

Annak ténye, hogy az érintett nyilvánosságra hozta a kezelt személyes adatokat, nem mentesíti az adatkezelőket az adatvédelmi törvény szerinti kötelezettségei alól. A célhoz kötöttség elve például folyamatosan vonatkozik a személyes adatokra akkor is, ha az érintett adatokat nyilvánosan hozzáférhetővé tették.[424]

Jogi igények

A különleges adatkategóriák azon kezelése, amely „jogi igények előterjesztése, érvényesítése és védelme miatt szükséges" akár bírósági eljárásban, közigazgatási vagy bíróságon kívüli eljárásban,[425] szintén megengedett az általános adatvédelmi rendelet értelmében.[426] Ebben az esetben az adatkezelésnek egy konkrét jogi igényre, annak érvényesítésére vagy védelmére kell vonatkoznia, és a vitás felek bármelyike kérheti.

A bíróságok igazságszolgáltatási feladatkörükben eljárva a jogvita megoldásával összefüggésben kezelhetik a különleges adatkategóriákat.[427] Az ebben az összefüggésben kezelt különleges adatok például – többek között – a genetikai adatok a származás megállapítása során, vagy az egészségügyi állapot, amikor a bizonyíték egy része bűncselekmény áldozata által elszenvedett sérülés részleteit érinti.

Alapvető közérdek

Ezenkívül az adatvédelmi irányelv 9. cikkének (2) bekezdése szerint a tagállamok további célokat is megállapíthatnak, amelyek érdekében különleges adatok kezelhetők, amennyiben:

- az adatkezelés alapvető közérdekből történik;
- európai jog vagy tagállami jog írja elő;

424 29. cikk szerinti munkacsoport (2013), *3/2013. sz. vélemény a célhoz kötöttségről*, WP 203, Brüsszel, 2013. április 2., 14. o.

425 Általános adatvédelmi rendelet, (52) preambulumbekezdés.

426 *Uo.*, 9. cikk (2) bekezdés.

427 *Uo.*

- az uniós jog vagy tagállami jog arányos, tiszteletben tartja a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket ír elő.[428]

Kiváló példa erre az elektronikus egészségügyi dokumentum-nyilvántartó rendszer. Az ilyen rendszerek nagymértékben, rendszerint országos szinten lehetővé teszik, hogy a beteg kezelése során az egészségügyi szolgáltatók által gyűjtött egészségügyi adatokhoz a beteg más egészségügyi szolgáltatói is hozzáférjenek.

A 29. cikk szerinti munkacsoport arra a következtetésre jutott, hogy az adatkezelésre vonatkozó meglévő jogszabályok szerint ilyen rendszereket nem volna szabad létrehozni.[429] Létezhetnek azonban elektronikus egészségügyi dokumentum-nyilvántartó rendszerek, ha azok „jelentős közérdek miatt" szükségesek.[430] Eszerint a létrehozásukhoz kifejezett jogalap lenne szükséges, amely tartalmazná a rendszer biztonságos működtetéséhez szükséges garanciákat is.[431]

A különleges adatok kezelésének egyéb jogalapja

Az általános adatvédelmi rendelet előírja, hogy különleges adatok akkor kezelhetők, ha a kezelés a következők miatt szükséges:[432]

- megelőző orvoslás vagy foglalkozás-egészségügy, a munkavállaló munkavégzési képességének felmérése, orvosi diagnózis felállítása, egészségügyi vagy szociális ellátás vagy kezelés nyújtása, illetve egészségügyi vagy szociális rendszerek és szolgáltatások irányítása érdekében szükséges, uniós vagy tagállami jog alapján vagy egészségügyi szakemberrel kötött szerződés értelmében;

- népegészségügy területét érintő olyan közérdekből szükséges, mint a határokon át terjedő súlyos egészségügyi veszélyekkel szembeni védelem vagy az egészségügyi ellátás, a gyógyszerek és az orvostechnikai eszközök magas

428 *Uo.*, 9. cikk (2) bekezdés f) pont.

429 29. cikk szerinti munkacsoport (2007), *Munkadokumentum az elektronikus egészségügyi nyilvántartásban tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról*, WP 131., Brüsszel, 2007. február 15. Lásd még: általános adatvédelmi rendelet, 9. cikk (3) bekezdés.

430 Általános adatvédelmi rendelet, 9. cikk (2) bekezdés g) pont.

431 29. cikk szerinti munkacsoport (2007), *Munkadokumentum az elektronikus egészségügyi nyilvántartásban tárolt, egészségi állapotra vonatkozó személyes adatok feldolgozásáról*, WP 131., Brüsszel, 2007. február 15.

432 Általános adatvédelmi rendelet, 9. cikk (2) bekezdés h), i) és j) pont.

színvonalának és biztonságának a biztosítása, uniós vagy tagállami jog alapján. A jognak biztosítania kell megfelelő és konkrét intézkedéseket az érintett jogait és szabadságait védő garanciák biztosítására;

- archiválás, tudományos vagy történelmi kutatási célból vagy statisztikai célból uniós vagy tagállami jog alapján. A jognak az követett céllal arányosnak kell lennie, tiszteletben kell tartania a személyes adatok védelméhez való jog lényeges tartalmát, és az érintett alapvető jogainak és érdekeinek biztosítására megfelelő és konkrét intézkedéseket kell előírnia.

További feltételek a nemzeti jog értelmében

Az általános adatvédelmi rendelet lehetővé teszi a tagállamok számára, hogy további feltételeket – köztük korlátozásokat – vezessenek be a genetikai adatok, a biometrikus adatok és az egészségügyi adatok kezelésére vonatkozóan.[433]

4.2 Az adatkezelés biztonságosságára vonatkozó szabályok

Főbb pontok

- Az adatkezelés biztonságosságára vonatkozó szabályok kötelezik az adatkezelőt és az adatfeldolgozót, hogy megfelelő technikai és szervezési intézkedéseket hajtsanak végre az adatkezelési műveletekbe való jogosulatlan beavatkozás megakadályozására.
- Az adatbiztonság szükséges szintjét a következők határozzák meg:
  - az adott típusú feldolgozás esetében a piacon elérhető biztonsági funkciók;
  - a költségek;
  - az adatkezeléssel járó kockázatok az érintettek alapvető jogaira és szabadságaira nézve.
- A személyes adatok bizalmas jellegének biztosítása az általános adatvédelmi rendeletben elismert egyik általános elv részét képezi.

433 *Uo.*, 9. cikk (2) bekezdés h) pont és 9. cikk (4) bekezdés.

Az uniós és Európa tanácsi jog szerint is az adatkezelőkkel szemben támasztott általános kötelezettség, hogy átláthatók és elszámoltathatók legyenek a személyes adatok kezelése során, és különösen az adatvédelmi incidensek vonatkozásában, amennyiben ilyen incidens történik. Adatvédelmi incidensek esetén az adatkezelők kötelesek értesíteni a felügyeleti hatóságot, kivéve, ha az adatvédelmi incidens valószínűsíthetően nem jár kockázattal a természetes személyek jogaira és szabadságaira nézve. Az érintetteket is tájékoztatni kell az adatvédelmi incidensről, ha az valószínűsíthetően a természetes személyek jogaira és szabadságaira nézve nagy kockázattal jár.

4.2.1 Az adatbiztonság elemei

Az **uniós jog** vonatkozó rendelkezései szerint:

> *„Az adatkezelő és az adatfeldolgozó a tudomány és technológia állása és a megvalósítás költségei, továbbá az adatkezelés jellege, hatóköre, körülményei és céljai, valamint a természetes személyek jogaira és szabadságaira jelentett, változó valószínűségű és súlyosságú kockázat figyelembevételével megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja [...].“*[434]

Ezek az intézkedések többek között a következők lehetnek:

- a személyes adatok álnevesítése és titkosítása;[435]
- az adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítása, integritása, rendelkezésre állása és ellenálló képessége;[436]
- a személyes adatokhoz való hozzáférés és az adatok rendelkezésre állásának kellő időben történő visszaállítása;[437]

434 *Uo.*, 32. cikk (1) bekezdés.

435 *Uo.*, 32. cikk (1) bekezdés a) pont.

436 *Uo.*, 32. cikk (1) bekezdés b) pont.

437 *Uo.*, 32. cikk (1) bekezdés c) pont.

- az adatkezelés biztonságának garantálására hozott technikai és szervezési intézkedések hatékonyságának tesztelésére, felmérésére és értékelésére szolgáló eljárás.[438]

Hasonló rendelkezés az **Európa Tanács jogában** is létezik:

> *„Minden fél biztosítja, hogy az adatkezelő, és adott esetben az adatfeldolgozó megfelelő biztonsági intézkedéseket hozzon olyan kockázatokkal szemben, mint a személyes adatokhoz való véletlen vagy jogosulatlan hozzáférés, a személyes adatok megsemmisülése, elvesztése, felhasználása, módosítása vagy nyilvánosságra hozatala."*[439]

Az **Unió és az Európa Tanács jogában** az adatkezelők kötelesek értesíteni a felügyeleti hatóságot az egyének jogait vagy szabadságait befolyásoló adatvédelmi incidensekről (lásd a 4.2.3 szakaszt).

A biztonságos adatkezelés érdekében számos esetben ágazati, nemzeti és nemzetközi normákat dolgoztak ki. Az európai adatvédelmi bizalompecsét (EuroPriSe) például az EU egyik eTEN (transzeurópai távközlési hálózatokra vonatkozó) projektje, amely a termékek, különösen szoftverek adatvédelmi tanúsításával – azaz az európai adatvédelmi jogszabályoknak való megfelelés megkönnyítésével – kapcsolatos lehetőségeket tártja fel. Az Európai Uniós Hálózat- és Információbiztonsági Ügynökséget (ENISA) azért hozták létre, hogy fokozzák a Közösség, a tagállamok, és következésképpen az üzleti szféra képességét a hálózat- és információbiztonsággal kapcsolatos problémák megelőzésére, kezelésére és az azokra történő reagálásra.[440] Az ENISA rendszeresen közzétesz elemzéseket az aktuális biztonsági fenyegetésekről, és tanácsokat ad azok kezelésével kapcsolatban.[441]

Az adatbiztonság nem pusztán a megfelelő berendezések – hardver és szoftver – meglétével érhető el. Megfelelő belső szervezeti szabályok is szükségesek hozzá. A belső szabályok ideális esetben a következő kérdéseket érintik:

438 *Uo.*, 32. cikk (1) bekezdés d) pont.

439 Korszerűsített 108. Egyezmény, 7. cikk (1) bekezdés.

440 Az Európai Parlament és a Tanács 526/2013/EU rendelete (2013. május 21.) az Európai Uniós Hálózat- és Információbiztonsági Ügynökségről (ENISA) és a 460/2004/EK rendelet hatályon kívül helyezéséről, HL L 165., 2013.6.18.

441 Például: ENISA (2016), *Kiberbiztonság és az intelligens autók ellenállóképessége. Ajánlások és bevált gyakorlatok*; ENISA (2016), *A mobil fizetések és digitális pénztárcák biztonsága*.

- valamennyi munkavállaló rendszeres tájékoztatása az adatbiztonsági szabályokról, valamint a munkavállalóknak az adatvédelmi jog alapján fennálló kötelezettségeiről, különösen a titoktartási kötelezettségről;

- világos feladatkör-megosztás és a hatáskörök egyértelmű meghatározása adatkezelési kérdésekben, különösen a személyes adatok kezelésére és harmadik feleknek vagy érintetteknek történő továbbítására irányuló döntésekkel kapcsolatban;

- a személyes adatok kizárólag az illetékes személy utasításai vagy az általánosan elfogadott szabályok szerinti felhasználása;

- az adatkezelő, illetve az adatfeldolgozó telephelyeihez és hardveréhez, szoftveréhez való hozzáférés védelme, a hozzáférési engedélyek ellenőrzését is beleértve;

- annak biztosítása, hogy a személyes adatokhoz való hozzáférési engedélyt az illetékes személy adja ki, és az engedély megadásához megfelelő dokumentáció szükséges;

- automatizált protokollok a személyes adatokhoz elektronikus úton történő hozzáféréshez, és e protokollok belső felügyeleti részleg általi rendszeres ellenőrzése (ami valamennyi adatkezelési tevékenység rögzítését teszi szükségessé);

- az automatizált hozzáférésen kívüli más közlési formák alapos dokumentálása annak igazolására, hogy nem történt jogellenes adattovábbítás.

Az adatbiztonsággal kapcsolatos megfelelő betanítás és képzés a személyzet tagjai számára szintén a hatékony biztonsági óvintézkedések egyik fontos eleme. Ellenőrzési eljárásokat is alkalmazni kell annak biztosítására, hogy a megfelelő intézkedések ne csupán papíron létezzenek, hanem a gyakorlatban is végrehajtják őket és működnek (pl. belső vagy külső ellenőrzések).

Az adatkezelő vagy -feldolgozó biztonsági szintjének javítását célzó intézkedések közé tartoznak az személyesadatvédelmi tisztviselők megléte, a munkavállalók biztonsággal kapcsolatos oktatása, a rendszeres ellenőrzések, penetrációs tesztek és minőségi tanúsítványok.

Példa: Az *I. kontra Finnország* ügyben[442] a felperes nem tudta bizonyítani, hogy orvosi adataihoz a munkahelyéül szolgáló kórház más alkalmazottai jogellenesen hozzáfértek. Ezért a hazai bíróságok elutasították az adatvédelemhez való jogának megsértése miatt benyújtott keresetét. Az EJEB megállapította, hogy megsértették az EJEE 8. cikkét, mivel a kórház kórlap-nyilvántartási rendszere „úgy volt kialakítva, hogy visszamenőlegesen nem lehetett tisztázni a betegek adatainak felhasználását, mivel a rendszer csupán az öt legutóbbi konzultációt mutatta ki, és ezt az információt törölte, amint a fájl visszakerült az archívumba". A Bíróság számára az volt a döntő, hogy a kórházban alkalmazott nyilvántartási rendszer egyértelműen nem állt összhangban a hazai jog által előírt jogi követelményekkel – aminek a hazai bíróságok nem tulajdonítottak kellő jelentőséget.

Az EU elfogadta a hálózati és információs rendszerek biztonságáról szóló irányelvet (a kiberbiztonsági irányelv),[443] amely az első Unió-szerte érvényes kiberbiztonsági jogi eszköz. Ennek az irányelvnek a célja, hogy egyrészt nemzeti szinten javítsa a kiberbiztonságot, másrészt pedig, hogy fokozza az együttműködés szintjét az Unión belül. Ezenkívül kötelezettségeket ró az alapvető szolgáltatásokat nyújtókra (ideértve az energia-, egészségügyi, banki, szállítási, digitális infrastruktúra ágazatok stb. szereplőit), valamint a digitális szolgáltatókra, hogy kezeljék a kockázatokat, biztosítsák hálózatuk és információs rendszereik biztonságát, valamint jelentsék a biztonsági incidenseket.

Kilátások

2017 szeptemberében az Európai Bizottság javaslatot tett egy rendelettervezetre, amelynek célja megreformálni az ENISA megbízatását úgy, hogy az figyelembe vegye az ügynökség kiberbiztonsági irányelvben megállapított új hatáskörét és felelősségeit. A javasolt rendelet célja, hogy kidolgozza az ENSA feladatait és megerősítse szerepét „az Unió kiberbiztonsági ökoszisztémájának referenciapontjaként".[444] A javasolt rendelet nem sértené az általános adatvédelmi rendelet elveit,

442 EJEB, *I. kontra Finnország*, 20511/03. sz. ügy, 2008. július 17.

443 Az Európai Parlament és a Tanács (EU) 2016/1148 irányelve (2016. július 6.) a hálózati és információs rendszerek biztonságának az egész Unióban egységesen magas szintjét biztosító intézkedésekről, HL L 194., 2016.7.19.

444 Javaslat – Az Európai Parlament és a Tanács rendelete az ENISA-ról, az „Európai Uniós kiberbiztonsági ügynökségről", az 526/2013/EU rendelet hatályon kívül helyezéséről és az információs és kommunikációs technológiák biztonsági tanúsításáról („kiberbiztonsági jogszabály"), COM(2017) 477, 2017. szeptember 13., 6. o.

és az európai kiberbiztonsági tanúsítási rendszereket alkotó szükséges elemek tisztázásával várhatóan erősíteni fogja a személyes adatok biztonságát is. Ezzel párhuzamosan, 2017 szeptemberében az Európai Bizottság javaslatot tett egy végrehajtási rendelettervezetre, amely meghatározza azokat az elemeket, amelyeket a digitális szolgáltatóknak figyelembe kell venniük annak biztosítására, hogy hálózatuk és információs rendszereik biztonságosak legyenek a kiberbiztonsági irányelv 16. cikkének (8) bekezdésében említetteknek megfelelően. A kézikönyv összeállításának idején folyamatban voltak az egyeztetések e két javaslatra vonatkozóan.

4.2.2 Bizalmas jelleg

Az uniós jog szerint az általános adatvédelmi rendelet egy általános elv részeként ismeri el a személyes adatok bizalmas jellegét.[445] A nyilvánosan elérhető elektronikus hírközlési szolgáltatóknak biztosítaniuk kell a titoktartást. Emellett kötelesek biztosítani szolgáltatásaik biztonságát is.[446]

Példa: Egy biztosítótársaság alkalmazottja a munkahelyén telefonhívást kap, és a hívó, aki önmagáról azt állítja, hogy ügyfél, a biztosítási szerződésével kapcsolatban kér tájékoztatást.

Az ügyfelek adatainak bizalmas kezelésére vonatkozó kötelezettség miatt az alkalmazottnak legalább minimális biztonsági intézkedéseket kell alkalmaznia, mielőtt személyes adatokat közöl. Ez történhet például úgy, hogy visszahívást ajánl az ügyfél aktájában szereplő telefonszámon.

Az 5. cikk (1) bekezdésének f) pontja értelmében a személyes adatok kezelését oly módon kell végezni, hogy megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve („integritás és bizalmas jelleg”).

A 32. cikk alapján az adatkezelő és az adatfeldolgozó megfelelő technikai és szervezési intézkedéseket hajt végre annak érdekében, hogy a kockázat mértékének megfelelő szintű adatbiztonságot garantálja. Az ilyen intézkedések többek között

445 Általános adatvédelmi rendelet, 5. cikk (1) bekezdés f) pont.

446 Elektronikus hírközlési adatvédelmi irányelv, 5. cikk (1) bekezdés.

magukban foglalják a személyes adatok álanomizálását és titkosítását, az adatok kezelésére használt rendszerek és szolgáltatások folyamatos bizalmas jellegének biztosítását, integritását, rendelkezésre állását és ellenálló képességét, az intézkedések hatékonyságának rendszeres tesztelésére, felmérésére és értékelésére szolgáló eljárást, valamint fizikai vagy műszaki incidens esetén az arra való képességet, hogy a vissza lehessen állítani az adatkezelést. Ezenkívül egy jóváhagyott magatartási kódexhez vagy tanúsítási mechanizmushoz való csatlakozással igazolható az integritás és bizalmas jelleg elvének való megfelelés. Az általános adatvédelmi rendelet 28. cikkével összhangban az adatfeldolgozót az adatkezelővel szemben kötő szerződésnek ki kell kötnie, hogy a személyes adatok kezelésére feljogosított személyek titoktartási kötelezettséget vállalnak,vagy jogszabályon alapuló megfelelő titoktartási kötelezettség alatt állnak.

A titkos kezelési kötelezettség nem terjed ki olyan helyzetekre, amikor az adatok magánszemélyként, nem pedig valamely adatkezelő vagy -feldolgozó alkalmazottjaként jutnak a személy tudomására. Ebben az esetben az általános adatvédelmi rendelet 32. és 28. cikke nem alkalmazandó, mivel a személyes adatok magánszemélyek általi felhasználása egyáltalán nem tartozik a rendelet hatálya alá, amennyiben a felhasználás az úgynevezett otthoni tevékenységre vonatkozó mentesség körébe esik.[447] Az otthoni tevékenységre vonatkozó mentesítés a „természetes személy által kizárólag személyes célra, vagy otthoni tevékenysége keretében végzett" személyesadat-kezelést jelenti.[448] Az EUB-nak a *Bodil Lindqvist* ügyben[449] hozott ítélete óta azonban ezt a mentességet szűken kell értelmezni, különösen adatok közzétételével kapcsolatban. Konkrétan, az otthoni tevékenységre vonatkozó mentesség nem terjed ki személyes adatoknak az interneten, korlátlan számú címzett részére történő közzétételére, illetve szakmai vagy kereskedelmi vonatkozású adatkezelésre (az ügy további részleteit lásd a 2.1.2, 2.2.2, és 2.3.1 szakaszban).

„A közlések titkossága" a bizalmas jelleg egy másik szempontja, amely különös szabályok alá tartozik. Az elektronikus közlések titkosságát biztosító különös szabályok az elektronikus hírközlési adatvédelmi irányelv értelmében előírják a tagállamok számára, hogy tiltsák meg a közlések és az azokra vonatkozó forgalmi adatok felhasználókon kívüli személyek által történő, az érintett felhasználó hozzájárulása nélküli meghallgatását, lehallgatását, tárolását vagy más módon történő elfogását

447 Általános adatvédelmi rendelet, 2. cikk (2) bekezdés c) pont.

448 *Uo.*

449 EUB, *Bodil Lindqvist elleni büntetőeljárás*, C-101/01. sz. ügy, 2003. november 6.

vagy megfigyelését.[450] A nemzeti jog ezen elv alóli kivételek alkalmazását kizárólag akkor teheti lehetővé, ha az szükséges és arányos intézkedésnek minősül a nemzetbiztonság, a nemzetvédelem és a közbiztonság védelme érdekében, valamint a bűncselekmények, illetve az elektronikus hírközlési rendszer jogosulatlan használata megelőzésének, kivizsgálásának, felderítésének és üldözésének a biztosítása érdekében.[451] Ugyanezek a szabályok lesznek érvényesek a jövőbeli elektronikus hírközlési adatvédelmi rendelet alapján is, az elektronikus hírközlési adatvédelemre vonatkozó jogi aktus hatálya azonban a nyilvánosan elérhető elektronikus hírközlési szolgáltatások mellett az over the top szolgáltatásokra is (például a mobilalkalmazásokat) ki fog terjedni.

Az **Európa Tanács joga** szerint a Korszerűsített 108. Egyezmény 7. cikkének (1) bekezdésében szereplő „adatbiztonság" fogalma magában foglalja a titoktartási kötelezettséget.

Az adatfeldolgozók számára a titoktartási kötelezettség azt jelenti, hogy az adatokat engedély nélkül nem közölhetik harmadik felekkel vagy más címzettekkel. Az adatkezelők vagy -feldolgozók alkalmazottai – a titoktartási kötelezettség miatt – a személyes adatokat kizárólag illetékes feletteseik utasításainak megfelelően használhatják fel.

A titoktartási kötelezettséget az adatkezelők a feldolgozóikkal kötött szerződésekben is kötelesek feltüntetni. Ezenkívül az adatkezelőknek és -feldolgozóknak egyedi intézkedésekkel – általában a munkaszerződésben egy titoktartási záradék szerepeltetésével – a munkavállalóik számára is elő kell írniuk a bizalmas kezelésre vonatkozó jogszabályi kötelezettséget.

A szakmai titoktartási kötelezettség megszegése több uniós tagállam és a 108. Egyezmény részes országainak büntetőjoga szerint is büntetendő.

4.2.3 Adatvédelmi incidens bejelentése

Az adatvédelmi incidens a biztonság olyan sérülése, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, megváltoztatását,

450 Elektronikus hírközlési adatvédelmi irányelv, 5. cikk (1) bekezdés.

451 *Uo.*, 15. cikk (1) bekezdés.

jogosulatlan közlését vagy az azokhoz való jogosulatlan hozzáférést eredményezi.[452] Bár az új technológiák, például a titkosítás, mára több lehetőséget biztosítanak az adatkezelés biztonságának biztosítására, az adatvédelmi incidensek még mindig gyakori jelenségnek számítanak. Az adatvédelmi incidens oka a szervezeten belül dolgozók véletlen hibáitól a külső fenyegetettségig (hekkerek és kiberbűnszervezetek) terjedhetnek.

Az adatvédelmi incidensek nagyon károsak lehetnek az egyének magánélethez és adatvédelemhez való jogaira nézve, akik az incidens eredményeképp elveszítik az ellenőrzést a személyes adataik felett. Az incidensek személyazonosság-lopást vagy csalást, pénzügyi veszteséget vagy vagyoni károkat, a szakmai titoktartás által védett személyes adatok bizalmas jellegének elvesztését, és az érintett hírnevének csorbulását eredményezhetik. Az adatvédelmi incidensekkel kapcsolatos, (EU) 2016/679 sz. rendelet értelmében vett értesítésről szóló iránymutatásában a 29. cikk szerinti munkacsoport kifejti, hogy az incidensek három hatást gyakorolhatnak a személyes adatokra: nyilvánosságra hozatal, elvesztés és/vagy módosítás.[453] Az adatkezelés biztonságosságát biztosító intézkedések megtételére vonatkozó, a 4.2 szakaszban kifejtett kötelezettség mellett ugyanilyen fontos biztosítani, hogy incidens megtörténtekor az adatkezelők megfelelően és kellő időben kezeljék azokat.

A felügyeleti hatóságok és egyének gyakran nincsenek tisztában az adatvédelmi incidensek megtörténtével, és ez megakadályozza, hogy az egyének megtegyék a szükséges lépéseket, hogy megvédjék magukat annak negatív következményeitől. Az egyének jogainak erősítése és az adatvédelmi incidensek hatásának korlátozása érdekében az **EU** és az **Európa Tanács** bizonyos körülmények között értesítési kötelezettséget ír elő az adatkezelő számára.

Az **Európa Tanács** Korszerűsített 108. Egyezménye alapján a részes felek kötelesek előírni az adatkezelők számára, hogy értesítsék az illetékes felügyeleti hatóságot legalább azon adatvédelmi incidensekről, amelyek súlyosan megsértik az érintettek jogait. Az ilyen értesítést „haladéktalanul" meg kell tenni.[454]

452 Általános adatvédelmi rendelet, 4. cikk 12. pont. Lásd még: 29. cikk szerinti munkacsoport (2017), *Iránymutatások az adatvédelmi incidensekkel kapcsolatos, az (EU) 2016/679 sz. rendelet értelmében vett értesítésről*, WP 250, 2017. október 3., 8. o.

453 29. cikk szerinti munkacsoport (2017), *Iránymutatások az adatvédelmi incidensekkel kapcsolatos, az (EU) 2016/679 sz. rendelet értelmében vett értesítésről*, WP 250, 2017. október 3., 6. o.

454 Korszerűsített 108. Egyezmény, 7. cikk (2) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 64–66 pont.

Az uniós jog részletes szabályokat állapít meg az értesítések időzítésére és tartalmára vonatkozóan.[455] Ennek megfelelően az adatkezelők kötelesek bizonyos incidenseket indokolatlan késedelem nélkül, ha lehetséges, legkésőbb 72 órával azután, hogy az adatvédelmi incidens a tudomásukra jutott, bejelenteni az illetékes hatóságnak. Ha a bejelentés 72 órán belül nem tehető meg, abban meg kell jelölni a késedelem okát. Az adatkezelők kizárólag akkor mentesülnek a bejelentési kötelezettség alól, ha igazolni tudják, hogy az adatvédelmi incidens valószínűsíthetően nem jár kockázattal az érintett személyek jogaira és szabadságaira nézve.

A rendelet megállapítja a bejelentésben közlendő információk minimális körét, amely szükséges ahhoz, hogy a felügyeleti hatóság megtehesse a szükséges intézkedéseket.[456] A bejelentésnek tartalmazni kell többek között az adatvédelmi incidens jellegének, valamint az érintettek kategóriáinak és hozzávetőleges számának ismertetését, az incidensből eredő, valószínűsíthető következmények leírását és az adatkezelő által az adatvédelmi incidensből eredő következmények kezelésére és enyhítésére tett intézkedéseket. Ezen kívül meg kell adni az adatvédelmi tisztviselő vagy a további tájékoztatást nyújtó egyéb kapcsolattartó nevét és elérhetőségeit, hogy az illetékes felügyeleti hatóság szükség esetén további információkat szerezhessen be.

Ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, az adatkezelő indokolatlan késedelem nélkül tájékoztatja ezeket a személyeket (az érintetteket) az adatvédelmi incidensről.[457] Az érintettek tájékoztatását, beleértve az adatvédelmi incidens ismertetését, világosan és közérthetően kell megfogalmazni, és a tájékoztatásnak a felügyeleti hatóságok részére küldött tájékoztatásban foglaltakhoz hasonló információkat kell tartalmaznia. Bizonyos körülmények között az adatkezelők mentesülhetnek az érintettek tájékoztatására vonatkozó kötelezettség alól. A tájékoztatás alól az adatkezelő akkor mentesülhet, ha megfelelő technikai és szervezési védelmi intézkedéseket hajtott végre, és ezeket az intézkedéseket az adatvédelmi incidens által érintett adatok tekintetében alkalmazták, különösen azokat az intézkedéseket – mint például a titkosítás alkalmazása –, amelyek a személyes adatokhoz való hozzáférésre fel nem jogosított személyek számára értelmezhetetlenné teszik az adatokat. Az adatkezelő szintén mentesül az érintettek tájékoztatásának kötelezettsége alól, ha az adatvédelmi incidenst követően olyan intézkedéseket tett, amelyek

455 Általános adatvédelmi rendelet, 33. és 34. cikk.

456 *Uo.*, 33. cikk (3) bekezdés.

457 *Uo.*, 34. cikk.

biztosítják, hogy az érintettek jogaira jelentett veszély a továbbiakban ne valósuljon meg. Végezetül pedig, ha a tájékoztatás aránytalan erőfeszítést tenne szükségessé az adatkezelő részéről, az érintetteket más módon, például nyilvánosan közzétett információk útján vagy olyan hasonló intézkedésekkel is lehet tájékoztatni az incidensről.[458]

Az adatvédelmi incidensek felügyeleti hatóságok részére történő bejelentése és az érintettek tájékoztatásának kötelezettsége az adatkezelőket terheli. Adatvédelmi incidensek azonban bekövetkezhetnek függetlenül attól, hogy az adatkezelést az adatkezelő vagy az adatfeldolgozó végezte-e. Ezért rendkívül fontos biztosítani, hogy az adatfeldolgozók is kötelesek legyenek bejelenteni az adatvédelmi incidenseket. Ebben az esetben adatfeldolgozó az adatvédelmi incidenst indokolatlan késedelem nélkül bejelenti az adatkezelőnek.[459] Ezt követően az adatkezelő felelős azért, hogy értesítse a felügyeleti hatóságot és az érintetteket, a fenti szabályok és határidők függvényében.

4.3 Az elszámoltathatóságra vonatkozó szabályok és a megfelelőség előmozdítása

Főbb pontok

- A személyes adatok kezelése során az elszámoltathatóság biztosítása érdekében az adatkezelőknek és az adatfeldolgozóknak nyilvántartást kell vezetniük a felelősségi körükben elvégzett adatkezelési tevékenységekről, és azokat kérésre át kell adniuk a felügyeleti hatóságoknak.
- Az általános adatvédelmi rendelet számos eszközt határoz meg a szabályok betartásának előmozdítására:
  - adatvédelmi tisztviselő kinevezése bizonyos helyzetekben;
  - hatásvizsgálat végzése azon adatkezelési tevékenységek megkezdése előtt, amelyek valószínűsíthetően magas kockázattal járnak a természetes személyek jogaira és szabadságaira nézve;

458 *Uo.*, 34. cikk (3) bekezdés c) pont.

459 *Uo.*, 33. cikk (2) bekezdés.

  - előzetes konzultáció az érintett felügyeleti hatósággal, ha a hatásvizsgálat azt jelzi, hogy valamely adatkezelési tevékenység olyan kockázatokat jelez, amelyek nem csökkenthetők;
  - a rendelet különféle adatkezelési ágazatokban történő alkalmazását előíró magatartási kódexek az adatkezelők és adatfeldolgozók számára;
  - tanúsítási mechanizmusok, védjegyek, illetve jelölések.
- Az Európa Tanács a Korszerűsített 108. Egyezményben hasonló eszközöket javasol az előírások betartásának előmozdítására.

Az elszámoltathatóság elve különösen fontos az adatvédelmi szabályok érvényre juttatásához Európában. Az adatkezelő felelős az adatvédelmi szabályok betartásáért, és tudnia kell ezt bizonyítani. Nem szabad hagyni, hogy csak az után kapjon szerepet az elszámoltathatóság, amikor már megtörtént egy szabálysértés. Az adatkezelőknek proaktív kötelezettséggel kell rendelkezniük az adatkezelési szabályzatok betartására vonatkozóan az adatkezelés valamennyi szakaszában. Az európai adatvédelmi jog előírja, hogy az adatkezelők hajtsanak végre technikai és szervezési intézkedéseket annak biztosítására és bizonyítására, hogy az adatkezelést a törvénynek megfelelően végzik. Ezen intézkedések között szerepel adatvédelmi tisztviselő kinevezése, nyilvántartás és dokumentáció vezetése az adatkezeléshez kapcsolódóan, valamint adatvédelmi hatásvizsgálat végzése.

4.3.1 Adatvédelmi tisztviselők

Az adatvédelmi tisztviselő (DPO) az a személy, aki tanácsot ad az adatkezelést végző szervezetekben az adatvédelmi szabályoknak való megfelelést illetően. Ő az elszámoltathatóság alapköve, mivel elősegíti a megfelelőséget, miközben közvetítőként is eljár a felügyeleti hatóságok, érintettek és az őt kijelölő szervezet között.

Az **Európa Tanács jogában** a Korszerűsített 108. Egyezmény 10. cikkének (1) bekezdése az elszámoltathatóság általános felelősségét az adatkezelőkre és adatfeldolgozókra testálja. Ez előírja, hogy az adatkezelők és adatfeldolgozók tegyenek meg minden megfelelő intézkedést az egyezményben kikötött adatvédelmi szabályoknak való megfelelés érdekében, és hogy legyenek képesek igazolni, hogy az ellenőrzésük alatt végzett adatkezelés megfelel az egyezmény rendelkezéseinek. Annak ellenére, hogy az egyezmény nem határoz meg az adatkezelők és adatfeldolgozók által elvégzendő konkrét intézkedéseket, a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés jelzi, hogy adatvédelmi tisztviselő kinevezése az egyik lehetséges intézkedés a megfelelőség bizonyítására. Az adatvédelmi

tisztviselők számára biztosítani kell a megbízatásuk ellátásához szükséges összes eszközt.[460]

Az Európa Tanács jogával szemben az **EU-ban** az adatvédelmi biztos kinevezése nem minden esetben az adatkezelők és adatfeldolgozók döntése, viszont bizonyos körülmények között kötelező. Az általános adatvédelmi rendelet elismeri, hogy az adatvédelmi tisztviselő kiemelt szerepet játszik az új irányítási rendszerben, és tartalmaz rendelkezéseket a tisztviselő kinevezését, beosztását, kötelezettségeit és feladatait illetően.[461]

Az általános adatvédelmi rendelet kötelezővé teszi az adatvédelmi tisztviselő kinevezését, ha az adatkezelést közhatalmi szervek végzik; az adatkezelő vagy az adatfeldolgozó fő tevékenységei olyan adatkezelési műveleteket foglalnak magukban, amelyek az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé, vagy ha a fő tevékenységek a büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó különleges kategóriák vagy személyes adatok nagy számban történő kezelését foglalják magukban.[462] Bár a rendelet nem definiálja az olyan kifejezéseket, mint a „szisztematikus, nagymértékű megfigyelés" és a „fő tevékenységek", a 29. cikk szerinti munkacsoport iránymutatást adott ki ezek értelmezésére vonatkozóan.[463]

Példa: A közösségi média vállalkozások és keresőmotorok alkalmasak arra, hogy olyan adatkezelőnek minősüljenek, amelyek adatkezelési műveletei az érintettek rendszeres és szisztematikus, nagymértékű megfigyelését teszik szükségessé. Az ilyen vállalkozások üzleti modellje nagy mennyiségű személyesadat-kezelésén alapul, és jelentős bevételt termelnek célzott reklámszolgáltatások kínálásával, valamint azzal, hogy lehetővé teszik, hogy a vállalatok weboldalakon helyezzenek el hirdetéseket. A célzott reklám a demográfiai adatok, valamint a vásárló korábbi vásárlásai és szokásai alapján történő hirdetés elhelyezés. Ezért ehhez az érintettek online szokásainak és viselkedésének szisztematikus megfigyelése szükséges.

460 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 87. pont.

461 Általános adatvédelmi rendelet, 37–39. cikk.

462 *Uo.*, 37. cikk (1) bekezdés.

463 29. cikk szerinti munkacsoport (2017), *Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban*, WP 243 rev.01, a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5.

Példa: A kórházak és egészségbiztosítók tipikus példa azon adatkezelőkre, amelyek tevékenysége különleges adatkategóriák nagy mértékű kezelését teszi szükségessé. Egy egyén egészségére vonatkozó információkat feltáró adatok az Európa Tanács és az Unió joga értelmében egyaránt a személyes adatok különleges kategóriáját képezik, ezért fokozott védelemben részesülnek. Az uniós jog továbbá különleges adatkategóriaként ismeri el a genetikai és biometrikus adatokat. Amennyiben egészségügyi létesítmények és biztosító vállalatok ilyen adatokat kezelnek nagy mértékben, az általános adatvédelmi rendelet értelmében adatvédelmi tisztviselőt kell kijelölniük.

Ezenkívül az általános adatvédelmi rendelet 37. cikkének (4) bekezdése kiköti, hogy a 37. cikk (1) bekezdésében előírt három kötelező eseten kívül az adatkezelő vagy az adatfeldolgozó, illetve az adatkezelők vagy adatfeldolgozók kategóriáit képviselő egyesületek és egyéb szervezetek adatvédelmi tisztviselőt jelölhetnek ki, vagy ha ezt uniós vagy tagállami jog írja elő, kötelesek kijelölni.

Az összes többi szervezet törvényileg nem köteles adatvédelmi tisztviselőt kijelölni. Az általános adatvédelmi rendelet azonban kimondja, hogy az adatkezelők és adatfeldolgozók önkéntesen jelölhetnek ki adatvédelmi tisztviselőt, miközben lehetővé teszi a tagállamok számára, hogy a rendeletben előírtnál több szervezettípus esetén kötelezővé tegyék adatvédelmi tisztviselő kijelölését.[464]

Miután az adatkezelő kinevezett egy adatvédelmi tisztviselőt, biztosítja, hogy a szervezeten belül „az adatvédelmi tisztviselő a személyes adatok védelmével kapcsolatos összes ügybe megfelelő módon és időben bekapcsolódjon”.[465] Az adatvédelmi tisztviselőknek részt kellene venniük az adatvédelmi hatásvizsgálat elvégzésére vonatozó tanácsadásban és a szervezet adatkezelési tevékenységeire vonatkozó nyilvántartás elkészítésében és vezetésében. Ahhoz, hogy az adatvédelmi tisztviselő hatékonyan tudja feladatait ellátni, az adatkezelő és adatfeldolgozó biztosítja számára azokat az erőforrásokat, köztük a pénzügyi forrásokat és felszereléseket, amelyek e feladatok hatékony végrehajtásához szükségesek. További követelmény, hogy például elegendő időt biztosítsanak az adatvédelmi tisztviselő számára feladatai ellátására, továbbá folyamatos képzést, hogy fejleszthesse

464 Általános adatvédelmi rendelet, 37. cikk (3) és (4) bekezdés.

465 *Uo.*, 38. cikk (1) bekezdés.

szakértelmét, és napra kész ismeretekkel rendelkezzen az adatvédelmi törvény fejleményeit illetően.[466]

Az általános adatvédelmi rendelet létrehoz néhány alapvető garanciát annak biztosítására, hogy az adatvédelmi tisztviselő függetlenül járhasson el. Az adatkezelők és adafeldolgozók kötelesek biztosítani, hogy az adatvédelmi tisztviselő a feladatai ellátásával kapcsolatban utasításokat senkitől ne kapjon a vállalatnál, beleértve a legmagasabb szintű vezetőket is. Ezenkívül az adatvédelmi tisztviselő feladatai ellátásával összefüggésben nem bocsátható el és szankcióval nem sújtható.[467] Vegyük például azt az esetet, amikor az adatvédelmi tisztviselő azt tanácsolja az adatkezelőnek vagy adatfeldolgozónak, hogy végezzen adatvédelmi hatásvizsgálatot, mert úgy véli, hogy az adatkezelés az érintettek számára magas kockázattal járhat. A vállalat nem ért egyet az adatvédelmi tisztviselő tanácsával, nem gondolja ezt megalapozottnak, következésképpen úgy dönt, hogy nem végez hatásvizsgálatot. A vállalat figyelmen kívül hagyhatja a tanácsot, azonban ezért nem bocsáthatja el vagy sújthatja szankcióval az adatvédelmi tisztviselőt.

Végezetül az adatvédelmi tisztviselő feladatait és kötelezettségeit az általános adatvédelmi rendelet 39. cikke részletezi. Ide tartozik a tájékoztatási és szakmai tanácsadási kötelezettség az adatkezelő vagy az adatfeldolgozó vállalat, továbbá az adatkezelést végző alkalmazottak részére a jogszabály, valamint az egyéb uniós vagy tagállami adatvédelmi rendelkezések szerinti kötelezettségeikkel kapcsolatban. Az adatvédelmi tisztviselő köteles együttműködni a felügyeleti hatósággal és az adatkezeléssel összefüggő ügyekben, például adatvédelmi incidensnél, kapcsolattartó pontként szolgál a felügyeleti hatóság felé.

Az uniós intézmények és szervek által kezelt személyes adatok vonatkozásában a 45/2001 rendelet kimondja, hogy az egyes uniós intézmények és szervek kötelesek adatvédelmi tisztviselőt kijelölni. Az adatvédelmi tisztviselő feladata biztosítani, hogy a rendelet rendelkezéseit megfelelően hajtsák végre az uniós intézményeken és szerveken belül, és, hogy az érintetteket és adatkezelőket egyaránt tájékoztassa jogaikról és kötelezettségeikről.[468] Feladata továbbá, hogy válaszoljon az európai adatvédelmi biztos megkereséseire, és szükség esetén együttműködjön vele. Az általános adatvédelmi rendelethez hasonlóan a 45/2001 rendelet is tartalmaz

466 29. cikk szerinti munkacsoport (2017), *Iránymutatás az adatvédelmi tisztviselőkkel kapcsolatban*, WP 243 rev.01, a legutóbbi felülvizsgálat és elfogadás időpontja: 2017. április 5., 3.1. pont.

467 Általános adatvédelmi rendelet, 38. cikk (2) és (3) bekezdés.

468 Lásd az adatvédelmi tisztviselő feladatainak teljese listáját a 45/2001/EK rendelet 24. cikkének (1) bekezdésében.

rendelkezéseket az adatvédelmi tisztviselő függetlenségére vonatkozóan feladatai ellátása során, valamint a feladatai elvégzéséhez szükséges személyi és anyagi erőforrások biztosításának szükségességére vonatkozóan.[469] Az adatvédelmi tisztviselőt értesíteni kell mielőtt egy uniós intézmény vagy szerv (vagy ezen szervezetek valamely szervezeti egysége) adatvédelmi műveleteket kezdene végezni, és a bejelentett adatkezelési műveletekről nyilvántartást kell vezetnie.[470]

4.3.2 A feldolgozási tevékenységek nyilvántartása

Azért, hogy bizonyítani tudják megfelelősségüket és elszámoltathatók legyenek, a vállalatok számára gyakran törvényi kötelezettség, hogy dokumentálják tevékenységeiket és nyilvántartást vezessenek róluk. Fontos példa erre az adótörvény és a könyvvizsgálat, amely előírja valamennyi vállalat számára, hogy vezessenek átfogó dokumentációt és nyilvántartást. Hasonló kötelezettségek előírása a jog egyéb területein – különösen az adatvédelmi jogban – is fontos, mivel a nyilvántartás-vezetés fontos az adatvédelmi szabályok betartásának megkönnyítése szempontjából. Az **uniós jog** ezért előírja, hogy az adatkezelők vagy képviselőik vezessenek nyilvántartást a felelősségi körükben elvégzett adatkezelési tevékenységekről.[471] Ennek a kötelezettségnek a szándéka biztosítani – szükség esetén –, hogy a felügyeleti hatóságok rendelkezzenek az adatkezelés jogszerűségének megállapításához szükséges dokumentációval.

A dokumentálandó információk a következőket tartalmazzák:

- az adatkezelő neve és elérhetősége, valamint – ha van ilyen – a közös adatkezelőnek, az adatkezelő képviselőjének és az adatvédelmi tisztviselőnek a neve és elérhetősége;
- az adatkezelés célja;
- az érintettek kategóriáinak, valamint a személyes adatok kategóriáinak ismertetése;

469 45/2001/EK rendelet, 24. cikk (6) és (7) bekezdés.

470 *Uo.*, 25. és 26. cikk.

471 Általános adatvédelmi rendelet, 30. cikk.

- olyan címzettek kategóriái, akikkel a személyes adatokat közlik vagy közölni fogják, ideértve a harmadik országbeli címzetteket vagy nemzetközi szervezeteket;

- arra vonatkozó információ, hogy a személyes adatokat továbbítják-e, vagy fogják-e továbbítani harmadik országba vagy nemzetközi szervezet részére;

- ha lehetséges, a különböző adatkategóriák törlésére előirányzott határidők, valamint az adatkezelés biztonságosságának garantálása érdekében alkalmazott technikai és szervezési intézkedések általános leírása.[472]

Az általános adatvédelmi rendelet értelmében az adatkezelési tevékenységek nyilvántartására vonatkozó kötelezettség nem csak az adatkezelőkre, hanem az adatfeldolgozókra is vonatkozik. Ez egy fontos fejlemény, mivel a rendelet elfogadása előtt az adatkezelő és az adatfeldolgozó között létrejött szerződés elsődlegesen az adatfeldolgozó kötelezettségeit tartalmazta. Nyilvántartás-vezetési kötelezettségüket most a törvény közvetlenül is előírja.

Az általános adatvédelmi rendelet tartalmaz egy kivételt e kötelezettség alól. A nyilvántartás-vezetési kötelezettség nem vonatkozik a 250 főnél kevesebb személyt foglalkoztató vállalkozásra vagy szervezetre (adatkezelő vagy adatfeldolgozó). A kivétel feltétele azonban, hogy az érintett szervezet által végzett adatkezelés ne járjon az érintettek jogaira és szabadságaira nézve valószínűsíthetően kockázattal, hogy az adatkezelés alkalmi jellegű legyen, és hogy az adatkezelés ne terjedjen ki a személyes adatok 9. cikk (1) bekezdésében említett különleges kategóriáinak vagy a 10. cikkben említett, büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatoknak a kezelésére.

Az adatkezelési tevékenységek nyilvántartása lehetővé teszi az adatkezelők és adatfeldolgozók számára, hogy bizonyítsák a rendeletnek való megfelelőségüket. Lehetővé teszi továbbá a felügyeleti hatóságok számára, hogy ellenőrizzék az adatkezelés jogszerűségét. Amennyiben a felügyeleti hatóságok hozzáférést kérnek e nyilvántartásokhoz, az adatkezelők és adatfeldolgozók kötelesek együttműködni, és a nyilvántartást a hatóság rendelkezésére bocsátani.

472 *Uo.*, 30. cikk (1) bekezdés.

4.3.3 Adatvédelmi hatásvizsgálat és előzetes konzultáció

Az adatkezelési tevékenységek némi kockázattal járnak az egyének jogaira nézve. A személyes adatok elveszhetnek, jogosulatlan felek tudomására juthatnak vagy előfordulhat jogszerűtlen kezelésük. Természetesen a kockázatok az adatezelés jellegétől és körétől függően változnak. A különleges adatokra is kiterjedő, nagymértékben történő adatkezelés például nagyobb kockázatot hordoz az érintettekre nézve ahhoz képest, amikor egy kisvállalat kezeli munkavállalóinak címét és személyes telefonszámát.

Az új technológiák megjelenésével és az adatkezelés egyre összetettebbé válásával az adatkezelőknek nagyobb kockázatokat kell kezelniük a tervezett adatkezelés valószínűsíthető hatásainak vizsgálatával még az adatkezelési művelet megkezdése előtt. Ez lehetővé teszi a szervezetek számára, hogy megfelelően azonosítsák, kezeljék és csökkentsék már előzetesen a kockázatokat, jelentősen csökkentve ezzel az adatkezelés egyénekre gyakorolt negatív hatásainak valószínűségét.

Adatvédelmi hatásvizsgálat végzését az **Európa Tanács és az EU joga** egyaránt előírja. Az Európa Tanács jogi keretrendszerében a Korszerűsített 108. Egyezmény 10. cikkének (2) bekezdése előírja, hogy a részes felek biztosítsák, hogy az adatkezelők és adatfeldolgozók „megvizsgálják a tervezett adatkezelés érintettek jogaira és alapvető szabadságaira gyakorolt hatását az adatkezelés megkezdése előtt", és a hatásvizsgálat elvégzését követően úgy tervezik meg az adatkezelést, hogy megakadályozzák vagy minimálisra csökkentsék az adatkezeléshez kapcsolódó kockázatokat.

Az uniós jog hasonló, ám részletesebb kötelezettséget ró az általános adatvédelmi rendelet hatálya alá tartozó adatkezelőkre. A 35. cikk előírja, hogy hatásvizsgálatot kell végezni, amennyiben az adatkezelés valószínűsíthetően az egyén jogaira és szabadságaira nézve nagy kockázattal jár. A rendelet nem határozza meg a kockázat valószínűsége mérésének módját, hanem helyette azt mondja meg, hogy melyek lehetnek ezek a kockázatok.[473] Egy felsorolást tartalmaz a magas kockázatúnak minősülő adatkezelési műveletekről, illetve azokról, amelyek esetében különösen szükség van előzetes hatásvizsgálatra. Ezek a következők:

473 Általános adatvédelmi rendelet, (75) preambulumbekezdés.

- természetes személyekre vonatkozó személyes adatok döntéshozatal céljából történő kezelése az egyénre vonatkozó személyes jellemzők módszeres és kiterjedt értékelését követően (profilalkotás);

- különleges adatok, vagy büntetőjogi felelősség megállapítására vonatkozó határozatokra és bűncselekményekre vonatkozó személyes adatok nagy számban történő kezelése;

- az adatkezelés nyilvános helyek nagymértékű, módszeres megfigyelésére terjed ki.

A felügyeleti hatóságnak össze kell állítania és nyilvánosságra kell hoznia az olyan adatkezelési műveletek típusainak a jegyzékét, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni. Azon adatkezelési műveletekre vonatkozó jegyzéket is összeállíthat, amelyekre vonatkozóan nem kell adatvédelmi hatásvizsgálatot végezni.[474]

Azokban az esetekben, amikor hatásvizsgálatot kell végezni, az adatkezelőknek meg kell vizsgálniuk az adatkezelés szükségességét és arányosságát, valamint az egyének jogaira gyakorolt lehetséges kockázatokat. A hatásvizsgálatnak tartalmaznia kell az azonosított kockázatok kezelését szolgáló tervezett biztonsági intézkedéseket. A jegyzékek összeállítása érdekében a tagállamok felügyeleti hatóságainak együtt kell működniük egymással és az Európai Adatvédelmi Testülettel. Ez biztosítja Unió-szerte a következetes megközelítést az adatvédelmi hatásvizsgálatot igénylő műveletekre vonatkozóan, és azt, hogy az adatkezelőknek székhelyüktől függetlenül hasonló kötelezettségeket kelljen teljesíteniük.

Ha a hatásvizsgálatot követően úgy tűnik, hogy az adatkezelés valószínűsíthetően magas kockázattal jár az egyének jogaira nézve, és nem tettek intézkedéseket a kockázat mérséklése céljából, az adatkezelő a személyes adatok kezelését megelőzően konzultál a felügyeleti hatósággal.[475]

A 29. cikk szerinti munkacsoport iránymutatást adott ki az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés

474 *Uo.*, 35. cikk (4) és (5) bekezdés.

475 *Uo.*, 36. cikk (1) bekezdés; 29. cikk szerinti munkacsoport (2017), *Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e*, WP 248 rev.01, Brüsszel, 2017. október 4.

valószínűsíthetően magas kockázattal jár-e.[476] Kilenc kritériumot dolgozott ki, amelyek segítenek meghatározni, hogy egy adott esetben szükség van-e adatvédelmi hatásvizsgálatra:[477] (1) értékelés vagy pontozás (2) joghatással vagy hasonló jelentős hatással járó automatizált döntéshozatal; (3) módszeres megfigyelés; (4) különleges adatok; (5) nagy számban kezelt adatok; (6) adatkészletek egymással való megfeleltetése vagy összevonása; (7) kiszolgáltatott helyzetben lévő érintettekkel kapcsolatos adatok; (8) technológiai vagy szervezési megoldások innovatív használata vagy alkalmazása; (9) amikor az adatkezelés önmagában „megakadályozza, hogy az érintett a jogait gyakorolja vagy szolgáltatást vegyen igénybe vagy szerződést érvényesítsen". A 29. cikk szerinti munkacsoport bevezetett egy ökölszabályt, amely szerint a kevesebb, mint két kritériumnak megfelelő adatkezelési műveletek alacsonyabb szintű kockázatot jelentenek, és ezek esetében nem szükséges adatvédelmi hatásvizsgálatot végezni, ugyanakkor a kettő vagy annál több kritériumnak megfelelő műveleteknél kötelező a vizsgálat elvégzése. Azokban az esetekben, ahol nem egyértelmű, hogy szükség van-e adatvédelmi hatásvizsgálatra, a 29. cikk szerinti munkacsoport ajánlja az ilyen vizsgálat elvégzését, mert azok „hasznosak a tekintetben, hogy segítségükkel az adatkezelők az általános adatvédelmi rendeletnek megfelelő adatkezelési rendszereket vezethetnek be".[478] Különösen új adatkezelési technológiák bevezetésekor lényeges, hogy elvégezzék az adatvédelmi hatásvizsgálatot.[479]

4.3.4 Magatartási kódexek

A magatartási kódexek számos iparágban használatosak arra, hogy kidolgozzák és konkretizálják az általános adatvédelmi rendelet alkalmazását saját ágazatukban. A személyes adatok kezelői és feldolgozói számára egy ilyen kódex létrehozása nagymértékben javíthatja a megfelelést és fokozhatja az uniós adatvédelmi szabályok végrehajtását. Az ágazatban tevékenységet folytatók szakmai tudásuk alapján olyan megoldásokat fognak előnyben részesíteni, amelyek gyakorlatiasak, azaz amelyeket minden valószínűség szerint követni fognak. Az általános adatvédelmi rendelet elismeri az ilyen kódexek jelentőségét az adatvédelmi törvény hatékony alkalmazása szempontjából, ezért a tagállamokat, a felügyeleti hatóságokat, a Bizottságot és az Európai Adatvédelmi Testületet olyan magatartási kódexek

476 29. cikk szerinti munkacsoport (2017), *Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár"-e*, WP 248 rev.01, Brüsszel, 2017. október 4.

477 *Uo.*, 9–15. oldal.

478 *Uo.*, 12. oldal.

479 *Uo.*

kidolgozására ösztönzi, amelyek Unió-szerte segítik a rendelet helyes alkalmazását.[480] A kódex meghatározhatja a rendelet alkalmazását konkrét ágazatokban, például a személyes adatok gyűjtését, az érintetteknek és a nyilvánosságnak adandó tájékoztatást, valamint az érintettek jogainak gyakorlását illetően.

Annak biztosítására, hogy a magatartási kódexek megfeleljenek az általános adatvédelmi rendeletben megállapított szabályoknak, a kódexeket azok elfogadása előtt meg kell küldeni az illetékes felügyeleti hatóságnak. A felügyeleti hatóság ezt követően véleményt bocsát ki arról, hogy a kódextervezet összhangban van-e a rendelettel, és jóváhagyja a kódextervezetet, a módosítást vagy a kiegészítést, amennyiben megállapítja, hogy az elegendő és megfelelő garanciát nyújt.[481] A felügyeleti hatóságok kötelesek közzétenni a jóváhagyott magatartási kódexeket, valamint a jóváhagyás alapját képező kritériumokat. Azokban az esetekben, amikor a magatartási kódex tervezete több tagállamban végzett adatkezelési tevékenységet érint, az illetékes hatóság a kódextervezet, a módosítás vagy a kiegészítés jóváhagyását megelőzően azt továbbítja az Európai Adatvédelmi Testületnek, amely véleményt bocsát ki arról, hogy a kódextervezet, a módosítás vagy a kiegészítés összhangban van-e az általános adatvédelmi rendelettel. A Bizottság végrehajtási jogi aktusok útján határozhat arról, hogy a jóváhagyott magatartási kódex, módosítás vagy kiegészítés az Unió területén általános érvényű hatállyal rendelkezik.

Valamely jóváhagyott magatartási kódex betartása fontos előnyöket biztosít az érintetteknek, az adatkezelőknek és adatfeldolgozóknak egyaránt. Az ilyen kódexek részletes útmutatást nyújtanak, amely a jogszabályi követelményeket egy konkrét ágazatra igazítja, és elősegíti az adatkezelési tevékenységek átláthatóságát. Az adatkezelők és adatfeldolgozók arra is használhatják a kódexek betartását, hogy bizonyítsák az uniós jognak való megfelelőségüket, illetve ezáltal olyan szervezet képét alakíthatják ki magukról a nyilvánosság előtt, amely tevékenysége során kiemelt figyelmet szentel az adatvédelemnek és elkötelezett mellette. A jóváhagyott magatartási kódexek kötelező érvényű és érvényesíthető kötelezettségvállalásokkal megfelelő garanciaként használhatók az adatok harmadik országokba való továbbításakor. Annak biztosítására, hogy a magatartási kódexeket követő szervezetek be is tartsák azokat, egy külön testület (amelyet az illetékes felügyeleti hatóság erre akkreditál) jelölhető ki a megfelelőség ellenőrzésére és biztosítására. Ahhoz, hogy feladatait hatékonyan lássa el, a testületnek függetlennek kell lennie, igazolt szakértelemmel kell rendelkeznie a magatartási kódexszel szabályozott

480 Általános adatvédelmi rendelet, 40. cikk (1) bekezdés.

481 *Uo.*, 40. cikk (5) bekezdés.

ügyekben, és átlátható eljárásokkal és struktúrákkal kell rendelkeznie, amelyek révén kezelni tudja a kódex megsértésével kapcsolatos panaszokat.[482]

Az **Európa Tanács jogában** a Korszerűsített 108. Egyezmény rendelkezik arról, hogy az adatvédelem nemzeti jogban garantált szintje eredményesen fokozható önkéntes szabályozó intézkedésekkel, például bevált gyakorlatok kódexével vagy szakmai magatartási kódexekkel. Ezek ugyanakkor csak önkéntes intézkedéseknek minősülnek a Korszerűsített 108. Egyezmény értelmében: törvényileg nem kötelezhető senki ilyen intézkedések alkalmazására, noha az tanácsos, és az ilyen intézkedések önmagukban nem elegendőek ahhoz, hogy biztosítsák az egyezménynek való megfelelést.[483]

4.3.5 Tanúsítás

A magatartási kódexek mellett a tanúsítási mechanizmusok és adatvédelmi védjegyek, illetve jelölések képezik a másik módját, amivel az adatkezelők és adatfeldolgozók bizonyítani tudják az általános adatvédelmi rendeletnek való megfelelőségüket. Ebből a célból a szabályozás önkéntes tanúsítási rendszerről rendelkezik, amellyel egyes testületek vagy a felügyeleti ihatóságok tanúsítványokat adhatnak ki. Valamely tanúsítási mechanizmushoz csatlakozni kívánó adatkezelők és adatfeldolgozók nagyobb láthatóságra és szavahihetőségre tehetnek szert, mivel a védjegyek, illetve jelölések lehetővé teszik az érintettek számára, hogy gyorsan felmérjék az adott szervezet védelmi szintjét adatkezelés tekintetében. Fontos, hogy attól, hogy egy adatkezelő vagy adatfeldolgozó rendelkezik ilyen tanúsítvánnyal, azzal még nem csökken arra irányuló kötelezettsége és felelőssége, hogy megfeleljen a rendelet követelményeinek.

4.4 Beépített és alapértelmezett adatvédelem

Beépített adatvédelem

Az **uniós jog** előírja, hogy az adatkezelők megfelelő intézkedéseket hajtsanak végre az adatvédelmi elvek hatékony megvalósítása, és a rendeletben foglalt követelmények teljesítéséhez és az érintettek jogainak védelméhez szükséges garanciák

482 *Uo.*, 41. cikk (1) és (2) bekezdés.

483 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 33. pont.

adatkezelés folyamatába történő beépítése érdekében.[484] Ezeket az intézkedéseket mind az adatkezelés módjának meghatározásakor, mind pedig az adatkezelés során alkalmazni kell. Ezen intézkedések megtétele során az adatkezelőnek figyelembe kell vennie a tudomány és technológia állását, a megvalósítás költségeit, továbbá az adatkezelés jellegét, hatókörét és céljait, valamint az érintett jogaira és szabadságaira jelentett kockázatot és annak súlyosságát.[485]

Az **Európa Tanács joga** előírja az adatkezelők és adatfeldolgozók számára, hogy az adatkezelés megkezdése előtt értékeljék az adatkezelés érintettek jogaira és szabadságaira gyakorolt valószínűsíthető hatásait. Ezenkívül az adatkezelők és adatfeldolgozók kötelesek úgy megtervezni az adatkezelést, hogy megakadályozzák vagy minimálisra csökkentsék az e jogokba és szabadságokba való beavatkozás kockázatát, valamint olyan technikai és szervezeti intézkedéseket hajtsanak végre, amelyek az adatkezelés minden fázisában figyelemmel vannak az adatvédelemhez való jog vonzataira.[486]

Alapértelmezett adatvédelem

Az **uniós jog** előírja, hogy az adatkezelő megfelelő technikai és szervezési intézkedéseket hajtson végre annak biztosítására, hogy alapértelmezés szerint kizárólag olyan személyes adatok kezelésére kerüljön sor, amelyek az adott konkrét adatkezelési cél szempontjából szükségesek. Ez a kötelezettség vonatkozik a gyűjtött személyes adatok mennyiségére, kezelésük mértékére, tárolásuk időtartamára és hozzáférhetőségükre.[487] Ezeknek az intézkedéseknek azt kell például biztosítaniuk, hogy az érintettek személyes adataihoz alapértelmezés szerint ne legyen az adatkezelő valamennyi alkalmazottjának hozzáférése. További iránymutatást az európai adatvédelmi biztos dolgozott ki a *Szükségességi eszköztárban*.[488]

484 Általános adatvédelmi rendelet, 25. cikk (1) bekezdés.

485 29. cikk szerinti munkacsoport (2017), *Iránymutatás az adatvédelmi hatásvizsgálat elvégzéséhez és annak megállapításához, hogy az adatkezelés az (EU) 2016/679 rendelet alkalmazásában „valószínűsíthetően magas kockázattal jár”-e*, WP 248 rev.01, 2017. október 4. Lásd még: ENISA (2015), *Beépített adatvédelem – a politikától a tervezésig*, 2015. január 12.

486 Korszerűsített 108. Egyezmény, 10. cikk (2)–(3) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 89. pont.

487 Általános adatvédelmi rendelet, 25. cikk (2) bekezdés.

488 Európai adatvédelmi biztos (EDPS) (2017), *Necessity Toolkit*, Brüsszel, 2017. április 11.

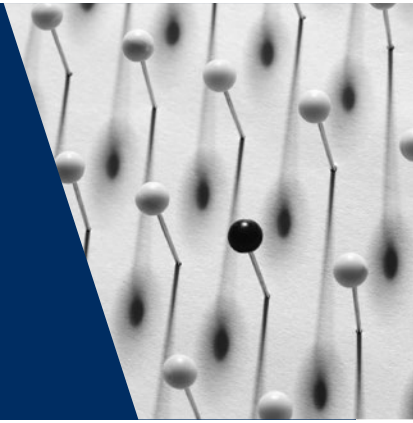
Az **Európa Tanács joga** előírja, hogy az adatkezelők és az adatfeldolgozók technikai és szervezési intézkedéseket hajtsanak végre az adatvédelemhez való jog vonzatainak figyelembevétele érdekében.[489]

2016-ban az ENISA egy jelentést tett közzé a rendelkezésre álló adatvédelmi eszközökről és szolgáltatásokról.[490] Egyéb megfontolások mellett ez a jelentés egy mutatószámot határoz meg azon kritériumokat és paramétereket illetően, amelyek a jó vagy rossz adatvédelmi gyakorlatokat jelzik. Bár néhány kritérium közvetlenül kapcsolódik az általános adatvédelmi rendelet rendelkezéseihez – mint például az álnevesítés vagy a jóváhagyott tanúsítási mechanizmusok használata – mások innovatív kezdeményezéseket kínálnak a beépített és alapértelmezett adatvédelem biztosításához. A használhatóságra vonatkozó kritérium például, bár közvetlenül nem kapcsolódik az adatvédelemhez, fokozhatja azt, mivel lehetővé teheti valamely adatvédelmi eszköz vagy szolgáltatás szélesebb körben való elfogadását. Előfordulhat, hogy a gyakorlatban nehezen alkalmazható adatvédelmi eszközöket a nyilvánosság nehezen fogadja el, még akkor is, ha azok nagyon erős garanciákat biztosítanak. Ezenkívül az adatvédelmi eszköz érettségére és stabilitására vonatkozó kritérium – ami azt jelenti, hogy egy eszköz miként változik az idők folyamán és hogyan reagál az adatvédelemhez kapcsolódó meglévő vagy új kihívásokra – döntő fontosságú. Az adatvédelmet erősítő egyéb technológiák, például a biztonságos kommunikáció összefüggésében, a következőket foglalják magukban: végpontok közötti titkosítás (olyan kommunikáció, ahol kizárólag az egymással kommunikáló személyek képesek olvasni az üzeneteket), kliens-szerver titkosítás (a kliens és a szerver között létrehozott kommunikációs csatorna titkosítása); hitelesítés (a kommunikáló felek személyazonosságának ellenőrzése); és az anonim kommunikáció (a kommunikáló feleket harmadik személy nem képes azonosítani).

489 Korszerűsített 108. Egyezmény, 10. cikk (3) bekezdés; a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 89. pont.

490 ENISA, *PET ellenőrzések mátrixa: Szisztematikus megközelítés az online és mobil adatvédelmi eszközökhöz*, 2016. december 26.

5 Független felügyelet



EU	Tárgyalt kérdések	Európa Tanács
Charta, 8. cikk (3) bekezdés Az EU működéséről szóló szerződés, 16. cikk (2) bekezdés Általános adatvédelmi rendelet, 51–59. cikk EUB, *Európai Bizottság kontra Németországi Szövetségi Köztársaság* [nagytanács], C-518/07. sz. ügy, 2010 EUB, *Európai Bizottság kontra Osztrák Köztársaság* [nagytanács], C-614/10. sz. ügy, 2012 EUB, *Európai Bizottság kontra Magyarország* [nagytanács], C-288/12. sz. ügy, 2014 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015	**Felügyeleti hatóságok**	Korszerűsített 108. Egyezmény, 15. cikk
Általános adatvédelmi rendelet, 60–67. cikk	**Együttműködés a felügyeleti hatóságok között**	Korszerűsített 108. Egyezmény, 16–21. cikk
Általános adatvédelmi rendelet, 68–76. cikk	**Európai Adatvédelmi Testület**	

Főbb pontok

- Az európai adatvédelmi jog elengedhetetlen eleme a független felügyelet, és ezt a Charta 8. cikkének (3) bekezdése is rögzíti.
- A hatékony adatvédelem biztosítása érdekében a nemzeti jogszabályokban független felügyeleti hatóságokat kell létrehozni.
- A felügyeleti hatóságoknak teljes függetlenséggel kell eljárniuk, amit az őket létrehozó törvénynek garantálnia kell, és aminek a felügyeleti hatóság egyedi szervezeti struktúrájában is tükröződnie kell.
- A felügyeleti hatóságoknak speciális hatáskörük és feladataik vannak. Ezek többek között a következők:
  - nemzeti szinten nyomon követik és előmozdítják az adatvédelmet;
  - tanácsadással segítik az érintetteket és az adatkezelőket, valamint a kormányt és a nagyközönséget;
  - megtárgyalják a panaszokat, és segítséget nyújtanak az érintetteknek az állítólagos adatvédelmi jogsértésekkel kapcsolatban;
  - felügyelik az adatkezelőket és az adatfeldolgozókat.
- A felügyeleti hatóságok hatáskörrel rendelkeznek, hogy szükség esetén beavatkozzanak a következőkkel:
  - figyelmeztetésben vagy megrovásban részesíthetik, sőt akár meg is bírságolhatják az adatkezelőket és az adatfeldolgozókat;
  - elrendelhetik adatok helyesbítését, zárolását vagy törlését;
  - elrendelhetik az adatfeldolgozás tilalmát, vagy közigazgatási bírságot szabhatnak ki;
  - ügyeket bíróság elé utalhatnak.
- Mivel a személyes adatok kezelése gyakran azzal jár, hogy az adatkezelők, az adatfeldolgozók és az érintettek eltérő országokban találhatók, a felügyeleti hatóságok kötelesek együttműködni egymással a határokon átnyúló kérdések tekintetében az egyének hatékony európai védelmének biztosítása érdekében.
- Az EU-ban az általános adatvédelmi rendelet egy egységességi mechanizmust hoz létre a határokon átnyúló adatkezelési ügyek tekintetében. Néhány vállalat határokon átnyúló adatkezelési tevékenységeket folytat vagy az egynél több tagállamban adatkezelést végző leányvállalatai révén, vagy azért, mert noha csak egy tevékenységi hellyel rendelkezik az Unióban, de tevékenysége jelentős hatással van egynél több tagállamban található érintettekre. A mechanizmus keretében az ilyen vállalatoknak egyetlen nemzeti adatvédelmi felügyeleti hatósággal lesz dolguk.

- Az együttműködés és az egységességi mechanizmus lehetővé teszi a koordinált megközelítést az ügyben érintett valamennyi felügyeleti hatóság számára. A – fő vagy egyetlen tevékenységi hely szerinti – fő felügyeleti hatóság konzultál a többi érintett felügyeleti hatósággal és határozattervezetet nyújt be e hatóságokhoz.
- A jelenlegi 29. cikk szerinti munkacsoporthoz hasonlóan az egyes tagállamok felügyeleti hatóságai és az európai adatvédelmi biztos (EDPS) alkotják majd az Európai Adatvédelmi Testületet.
- Az Európai Adatvédelmi Testület feladatai közé tartozik például a rendelet megfelelő alkalmazásának ellenőrzése, tanácsadás a Bizottságnak a vonatkozó kérdésekkel kapcsolatban, továbbá vélemények, iránymutatások vagy bevált gyakorlatok kiadása egy sor témában.
- A fő különbség az, hogy az Európai Adatvédelmi Testület nem csak véleményeket ad ki, mint a 95/46/EK irányelv értelmében. Kötelező érvényű határozatokat is kiad olyan eseteket illetően, ahol valamely érintett felügyeleti hatóság releváns és megalapozott kifogást emelt az egységességgel kapcsolatban; ahol véleménykülönbség van a tekintetben, hogy melyik felügyeleti hatóság a „fő", végezetül pedig, ahol a felügyeleti hatóság nem kéri ki, vagy nem követi az európai adatvédelmi biztos véleményét. A cél annak biztosítása, hogy a rendeletet valamennyi tagországban egységesen alkalmazzák.

A független felügyelet az európai adatvédelmi jog elengedhetetlen eleme. Az EU és az Európa Tanács joga egyaránt elengedhetetlennek tekinti a független felügyeleti hatóságokat az egyének jogainak és szabadságainak hatékony védelmében személyes adataik kezelését illetően. Mivel az adatkezelés mára mindenütt jelen van és egyre összetettebb ahhoz, hogy az egyének megértsék, e hatóságok a digitális kor megfigyelői. Az EU-ban a független felügyeleti hatóságok létezését tekintik az elsődleges uniós jogban biztosított személyes adatok védelméhez való jog egyik legfontosabb elemének. Az EU Alapjogi Chartája 8. cikkének (3) bekezdése és az EUMSZ 16. cikk (2) bekezdése alapvető jogként ismeri el a személyes adatok védelmét, és megerősíti, hogy az adatvédelmi szabályoknak való megfelelést független hatóságoknak kell ellenőrizniük.

Az adatvédelmi törvény betartásának független felügyeletét az ítélkezési gyakorlatban is elismerték már.

Példa: A *Schrems* ügyben[491] az EUB azt vizsgálta, hogy a személyes adatok továbbítása az Egyesült Államokba az EU és az Egyesült Államok közötti első biztonságos kikötő megállapodás keretében összeegyeztethető-e az uniós

491 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

adatvédelmi joggal, figyelemmel az Edward Snowden által az Egyesült Államok Nemzetbiztonsági Ügynöksége (National Security Agency) által végzett tömeges megfigyelésre vonatkozóan kiszivárogtatott információkra. A személyes adatok továbbítására az Egyesült Államokba egy 2000-ben elfogadott európai bizottsági határozat alapján került sor, amely lehetővé tette a személyes adatok továbbítását az EU-ból olyan egyesült államokbeli szervezeteknek, amelyek a biztonságos kikötő megállapodás keretében önmaguk tanúsították a megfelelést, azon a jogcímen, hogy a megállapodás megfelelő szintű védelmet biztosít a személyes adatok tekintetében. Amikor az ír felügyeleti hatóságot felkérték, hogy vizsgálja ki a felperes panaszát az adattovábbítások jogszerűségét illetően Snowden kiszivárogtatásait követően, a hatóság a panaszt elutasította arra hivatkozva, hogy mivel a „biztonságos kikötő" adatvédelmi elvek (a biztonságos kikötőre vonatkozó határozat) tükrözték a Bizottság határozatának meglétét az amerikai adatvédelmi rendszer megfelelőségét illetően, ez megakadályozza, hogy tovább vizsgálja a panaszt.

Az EUB azonban megállapította, hogy egy olyan bizottsági határozat, amely engedélyezi az adattovábbítást a megfelelő védelmi szinttel rendelkező harmadik országokba, nem szünteti meg vagy csökkenti a nemzeti felügyeleti hatóságok hatáskörét. Az EUB megjegyezte, hogy e hatóságoknak az a hatásköre, hogy ellenőrizzék és biztosítsák az uniós adatvédelmi szabályoknak való megfelelést, az EU elsődleges jogából, mégpedig a Charta 8. cikkének (3) bekezdéséből, és az EUMSZ 16. cikk (2) bekezdéséből származik. „Következésképpen a független felügyelő hatóságok [...] létrehozatala [...] lényeges eleme az egyének személyes adatok kezelése tekintetében való védelmének."[492]

Az EUB ezért úgy határozott, hogy annak ellenére, hogy a személyes adatok továbbítása egy bizottsági megfelelőségi határozat alá tartozik, amennyiben egy nemzeti felügyeleti hatósághoz panaszt nyújtanak be, a hatóság köteles kellő gondossággal megvizsgálni a panaszt. A hatóság elutasíthatja a panaszt, ha arra a következtetésre jut, hogy az megalapozatlan. Ebben az esetben, hangsúlyozta az EUB, a hatékony bírósági jogorvoslati lehetőséghez való jog megköveteli, hogy az egyén a nemzeti bíróságok előtt vitassa az ilyen döntést, amely bíróságok a bizottsági határozat érvényességére

492 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6., 41. pont.

vonatkozóan előzetes döntéshozatal iránti kérelemmel fordulhatnak az EUB-hoz. Amennyiben a felügyeleti hatóság a panaszt megalapozottnak ítéli, lehetőséggel kell rendelkeznie ahhoz, hogy az ügyet a nemzeti bíróságok elé vigye. A nemzeti bíróságok az üggyel az EUB-hoz fordulhatnak, mivel az az egyetlen olyan testület, amely hatáskörrel rendelkezik ahhoz, hogy döntsön a bizottsági határozat érvényességére vonatkozóan.[493]

Az EUB ezt követően megvizsgálta a biztonságos kikötő határozatot annak megállapítására, hogy az adattovábbítási rendszer megfelelt-e az uniós adatvédelmi szabályoknak. Azt állapította meg, hogy a biztonságos kikötő határozat 3. cikke korlátozta a nemzeti felügyeleti hatóságok (adatvédelmi irányelvben biztosított) hatáskörét, hogy megakadályozza az Egyesült Államokba történő adattovábbítást, amennyiben a személyes adatok védelmének szintje nem megfelelő. Figyelemmel a független felügyeleti hatóságok fontosságára az adatvédelmi irányelvnek való megfelelés biztosítása tekintetében, az EUB azt állapította meg, hogy az adatvédelmi irányelvet a Charta összefüggésében úgy kell értelmezni, hogy a Bizottság nem rendelkezik a független felügyeleti hatóságok hatáskörét ilyen módon korlátozó hatáskörrel. A felügyeleti hatóságok hatáskörének korlátozása volt az egyik ok, ami miatt az EUB a biztonságos kikötő határozatot érvénytelennek nyilvánította.

Az európai jog tehát a független felügyeletet a hatékony adatvédelem biztosításához szükséges fontos mechanizmusnak tartja. A független felügyeleti hatóságok jelentik az első kapcsolattartót az érintettek számára adatvédelmi incidensek esetén.[494] Az uniós és az Európa tanácsi jog szerint a felügyeleti hatóságok létrehozása kötelező. Mindkét jogi keretrendszer az általános adatvédelmi rendeletben foglaltakhoz hasonlóan ismerteti e hatóságok feladatait és hatásköreit. Elvileg tehát a felügyeleti hatóságoknak az uniós jog és az Európa Tanács joga szerint azonos módon kellene működniük.[495]

493 *Uo.*, 53–66. pont.

494 Általános adatvédelmi rendelet, 13. cikk (2) bekezdés d) pont.

495 *Uo.*, 51. cikk; Korszerűsített 108. Egyezmény, 15. cikk.

5.1 Függetlenség

Az **EU** és az **Európa Tanács** joga előírja, hogy minden egyes felügyeleti hatóság feladatai teljesítése és hatáskörének gyakorlása során teljes függetlenséggel járjon el.[496] A felügyeleti hatóság és tagjainak, valamint alkalmazottainak közvetlen vagy közvetett külső befolyásokkal szembeni függetlensége alapvető a teljes objektivitás garantáláshoz az adatvédelmi ügyekben való döntések során. Nemcsak a felügyeleti hatóság létrehozását megalapozó jogszabálynak kell a függetlenséget kifejezetten garantáló rendelkezéseket tartalmaznia, hanem a hatóság szervezeti felépítésének is mutatnia kell a függetlenséget. 2010-ben az EUB azt vizsgálta – első alkalommal – meg, hogy a felügyeleti hatóságoknak milyen mértékben kell függetlennek lenniük.[497] A kiemelt példák a „teljes függetlenség" jelentésének EUB általi meghatározását szemléltetik.

Példa: Az *Európai Bizottság kontra Németországi Szövetségi Köztársaság* ügyben[498] az Európai Bizottság annak megállapítására kérte az EUB-t, hogy Németország helytelenül ültette át az adatvédelem biztosításáért felelős hatóságok „teljes függetlenségére" vonatkozó követelményt, azaz nem teljesítette a 95/46/EK irányelv 28. cikke (1) bekezdéséből eredő kötelezettségeit. A Bizottság álláspontja szerint az a tény, hogy Németország a különböző tartományokban (*Länder*) végzett személyesadat-kezelést ellenőrző felügyeleti hatóságokat állami ellenőrzés alá vonta az adatvédelmi törvénynek való megfelelés biztosítása érdekében, megsértette a függetlenségre vonatkozó követelményt.

Az EUB kiemelte, hogy a „teljes függetlenséggel" kifejezést a szóban forgó rendelkezés tényleges megszövegezése, valamint az uniós adatvédelmi törvény céljai és szerkezete alapján kell értelmezni.[499] Az EUB hangsúlyozta, hogy a felügyeleti hatóságok a személyes adatok kezeléséhez kapcsolódó jogok „őrzői". Ezért létrehozásuk a tagállamokban „alapvető eleme az egyének védelmének a személyes adatok kezelése tekintetében".[500]

496 Általános adatvédelmi rendelet, 52. cikk (1) bekezdés; Korszerűsített 108. Egyezmény, 15. cikk (5) bekezdés.

497 FRA (2010), *Alapvető jogok: kihívások és eredmények 2010-ben – Az FRA éves jelentése*, 59. o.; FRA (2010), *Adatvédelem az Európai Unióban: az országos adatvédelmi hatóságok szerepe*, 2010. május.

498 EUB, *Európai Bizottság kontra Németországi Szövetségi Köztársaság* [nagytanács], C-518/07. sz. ügy, 2010. március 9., 27. pont.

499 *Uo.*, 17. és 29. pont.

500 *Uo.*, 23. pont.

Az EUB megállapította, hogy „feladataik gyakorlása során a felügyeleti hatóságoknak objektíven és pártatlanul kell eljárniuk. Ezért minden külső befolyástól mentesnek kell lenniük, ideértve az állam vagy a tartományok által gyakorolt közvetlen vagy közvetett befolyást is”.[501]

Az EUB azt is megállapította, hogy a „teljes függetlenséget” az európai adatvédelmi biztosnak az uniós intézmények adatvédelmi rendeletében meghatározott függetlensége fényében kell értelmezni. Ebben a rendeletben a függetlenség fogalma megköveteli, hogy az európai adatvédelmi biztos senkitől ne kérhessen és fogadhasson el utasításokat.

Ennek megfelelően az EUB megállapította, hogy a németországi felügyeleti hatóságok – az állami hatóságok felügyelete miatt – nem élveztek az uniós adatvédelmi törvény értelmében vett teljes függetlenséget.

Példa: Az *Európai Bizottság kontra Osztrák Köztársaság* ügyben[502] az EUB hasonló problémákra világított rá az osztrák adatvédelmi hatóság (Adatvédelmi Bizottság, DSK) egyes tagjainak és munkatársainak függetlenségével kapcsolatban. Az EUB arra a következtetésre jutott, hogy az a tény, hogy a szövetségi kancellária biztosította a munkaerőt a felügyeleti hatóság számára, aláásta az uniós adatvédelmi törvényben meghatározott függetlenségi követelményt. Az EUB azt is megállapította, hogy az az előírás, miszerint a kancelláriát mindenkor tájékoztatni kell a munkájáról, ellehetetlenítette a felügyeleti hatóság teljes függetlenségét.

Példa: Az *Európai Bizottság kontra Magyarország* ügyben[503] az EUB a munkaerő függetlenségét érintő hasonló nemzeti gyakorlatot tiltott be. Rámutatott, hogy „azon követelmény, amely szerint biztosítani kell, hogy a rájuk ruházott feladatok gyakorlása során minden egyes hatóság teljes függetlenségben járjon el, magában foglalja azt a kötelezettséget […], hogy az érintett tagállamnak e hatóság megbízatását az eredetileg megállapított időtartam leteltéig tiszteletben kell tartania”. Az EUB azt is megállapította,

501 *Uo.*, 25. pont.

502 EUB, *Európai Bizottság kontra Osztrák Köztársaság* [nagytanács], C-614/10. sz. ügy, 2012. október16., 59. és 63. pont.

503 EUB, *Európai Bizottság kontra Magyarország* [nagytanács], C-288/12. sz. ügy, 2014. április 8., 50. és 67. pont.

hogy „Magyarország – mivel idő előtt megszüntette a személyes adatok védelmét felügyelő felügyeleti hatóság megbízatását, nem teljesítette a[z] [...] 1995. október 24-i 95/46/EK [...] irányelvből eredő kötelezettségeit".

A „teljes függetlenség" fogalma és kritériuma kifejezetten meghatározásra kerül az általános adatvédelmi rendeletben, amely beépíti az ismertetett EUB ítéleteken keresztül létrehozott elveket. A rendelet értelmében a teljes függetlenség a feladatainak ellátása, illetve hatásköreinek gyakorlása során a következőket jelenti:[504]

- minden egyes felügyeleti hatóság tagjainak védelmet kell élvezniük minden – akár közvetlen, akár közvetett – külső befolyástól, és nem kérhetnek, és nem fogadhatnak el senkitől utasítást;

- minden egyes felügyeleti hatóság tagjainak tartózkodniuk kell a feladataikkal össze nem egyeztethető cselekedetektől az összeférhetetlenség megelőzése érdekében;

- a tagállamok kötelesek biztosítani minden egyes felügyeleti hatóság számára a szükséges emberi, műszaki és pénzügyi erőforrásokat és infrastruktúrát a feladataik hatékony ellátása érdekében;

- a tagállamok kötelesek biztosítani, hogy minden egyes felügyeleti hatóság maga válassza ki a saját személyzetét;

- az a pénzügyi ellenőrzés, amely alá a nemzeti jog értelmében az egyes felügyeleti hatóságok tartoznak, nem befolyásolhatja azok függetlenségét. A felügyeleti hatóságoknak a megfelelő működésüket lehetővé tevő külön és nyilvános éves költségvetéssel kell rendelkezniük.

A felügyeleti hatóságok függetlenségét az Európa Tanács joga is alapvető követelménynek tekinti. A Korszerűsített 108. Egyezmény előírja, hogy a felügyeleti hatóságok „teljesen pártatlanul és függetlenül járjanak el feladataik ellátása és hatáskörük gyakorlása során", anélkül, hogy utasításokat kérnének vagy fogadnának el.[505] Ilyen módon az egyezmény elismeri, hogy ezek a hatóságok csak akkor tudják hatékonyan védeni az egyének adatkezeléshez kapcsolódó jogait és szabadságait, ha feladataik ellátása során teljes függetlenséget élveznek. A Korszerűsített

504 Általános adatvédelmi rendelet, 52. cikk.

505 Korszerűsített 108. Egyezmény, 15. cikk (5) bekezdés.

108. Egyezményhez fűzött Magyarázó Jelentés számos olyan elemet határoz meg, amelyek hozzájárulnak e függetlenség megőrzéséhez. Ilyen elemek például a felügyeleti hatóságok azon lehetősége, hogy saját maguk vegyék fel személyzetük tagjait, és hogy külső beavatkozás nélkül fogadhassanak el határozatokat, valamint a feladataik ellátásának időtartamára vonatkozó tényezők, és azon feltételek, amelyek mellett szolgálati jogviszonyuk megszűnik.[506]

5.2 Joghatóság és hatáskör

Az **uniós jogban** az általános adatvédelmi rendelet meghatározza a felügyeleti hatóságok joghatóságát és szervezeti felépítését, és előírja, hogy a hatóságoknak joghatósággal és hatáskörrel kell rendelkezniük ahhoz, hogy a rendeletben meghatározott feladataikat elláthassák.

A felügyeleti hatóság a nemzeti jogban az a fő szerv, amely biztosítja az uniós adatvédelmi törvénynek való megfelelést. A felügyeleti hatóságok az ellenőrzésen túl átfogó feladatokkal és hatáskörrel rendelkeznek, amely tartalmaz proaktív és megelőző felügyeleti tevékenységeket is. E feladatok ellátásához a felügyeleti hatóságoknak az általános adatvédelmi rendelet 58. cikkében felsorolt megfelelő vizsgálati, korrekciós és tanácsadási hatáskörrel kell rendelkezniük, ami például a következőkre terjed ki:[507]

- tanácsot adhatnak az adatkezelőknek és az érintetteknek adatvédelmi kérdésekben;
- általános szerződési feltételeket, kötelező erejű vállalati szabályokat vagy közigazgatási megállapodásokat engedélyezhetnek;
- vizsgálhatják az adatkezelési műveleteket, és ennek megfelelően beavatkozhatnak;
- elrendelhetik az adatkezelői tevékenységek felügyelete szempontjából releváns információk benyújtását;

506 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés.

507 Általános adatvédelmi rendelet, 58. cikk. Lásd még a 108. Egyezmény kiegészítő jegyzőkönyvének 1. cikkét.

- figyelmeztethetik vagy megrovásban részesíthetik az adatkezelőket, és elrendelhetik, hogy az adatvédelmi incidensekről tájékoztassák az érintetteket;
- elrendelhetik adatok helyesbítését, zárolását, törlését vagy megsemmisítését;
- elrendelheti az adatfeldolgozás átmeneti vagy végleges tilalmát, vagy közigazgatási bírságot szabhat ki ;
- ügyet bíróság elé utalhatnak.

Feladatainak gyakorlásához a felügyeleti hatóságnak a vizsgálathoz szükséges valamennyi személyes adathoz és információhoz hozzáféréssel kell rendelkeznie, továbbá belépési joggal kell rendelkeznie minden olyan telephelyre, ahol az adatkezelő releváns információkat tárol. Az EUB véleménye szerint a felügyeleti hatóság hatáskörét tágan kell értelmezni az adatvédelem teljes körű hatékonyságának biztosítására az uniós érintettek számára.

Példa: A *Schrems* ügyben az EUB azt vizsgálta, hogy a személyes adatok továbbítása az Egyesült Államokba az EU és az Egyesült Államok közötti első biztonságos kikötő megállapodás keretében összeegyeztethető-e az uniós adatvédelmi törvénnyel, figyelemmel az Edward Snowden által kiszivárogtatott információkra. Az EUB indokolása szerint – az adatkezelők adatkezelési tevékenységét ellenőrző független szervként eljárva – a nemzeti felügyeleti hatóságok egy megfelelőségi határozat léte ellenére is megakadályozhatják a személyes adatok harmadik országba történő továbbítását, ha van észszerű bizonyíték arra, hogy a harmadik ország már nem garantálja a megfelelő védelmet.[508]

Minden egyes felügyeleti hatóság rendelkezik hatáskörrel ahhoz, hogy területén belül vizsgálati és beavatkozási jogkört gyakoroljon. Mivel azonban az adatkezelők és adatfeldolgozók tevékenységei gyakran határokon átnyúlnak, és az adatkezelés több tagállamban lévő érintettet érint, felmerül a kérdés, hogy miként lehet megosztani a joghatóságot a különböző felügyeleti hatóságok között. Az EUB-nek lehetősége volt megvizsgálni ez a kérdést a *Weltimmo* ügyben.

508 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6., 26–36. és 40–41. pont.

Példa: A *Weltimmo* ügyben[509] az EUB azt vizsgálta, hogy a nemzeti felügyeleti hatóságoknak van-e hatáskörük nem a joghatóságukban székhellyel rendelkező szervezeteket érintő ügyekkel foglalkozni. A Weltimmo egy Szlovákiában bejegyzett vállalat volt, amely magyarországi ingatlanokra vonatkozó hirdetéseket megjelentető weboldalt üzemeltetett. A hirdetők panaszt nyújtottak be a magyar adatvédelmi felügyeleti hatóságnál a magyar adatvédelmi törvény megsértése miatt, és a hatóság megbírságolta a Weltimmot. A vállalat a bírságot megtámadta a nemzeti bíróságokon, és az ügyet az EUB elé terjesztették annak megállapítására, hogy az uniós adatvédelmi irányelv lehetővé teszi-e valamely tagállam számára, hogy nemzeti adatvédelmi törvényét alkalmazza egy másik tagállamban székhellyel rendelkező vállalatra.

Az EUB az adatvédelmi irányelv 4. cikke (1) bekezdésének a) pontját úgy értelmezte, hogy az lehetővé teszi az attól eltérő tagállam személyes adatok védelmére vonatkozó szabályozásának alkalmazását, mint ahol ezen adatok kezelője be van jegyezve, „amennyiben ezen adatkezelő tartós jelleggel olyan, akár csekély mértékű valós és tényleges tevékenységet folytat e tagállam területén, amelynek keretében ezen adatkezelésre sor kerül". Az EUB megállapította, hogy a rendelkezésére álló információk alapján a Weltimmo valós és tényleges tevékenységet folytatott Magyarországon, mivel a vállalat a szlovák cégjegyzékbe bejegyzett képviselővel rendelkezett Magyarországon, valamint rendelkezett magyarországi bankszámlaszámmal és postafiókkal, és magyarul megírt tevékenységeket folytatott Magyarországon. Ez az információ egy „tevékenységi hely" létét jelezte, és a Weltimmo tevékenységét a magyar adatvédelmi törvény hatálya, valamint a magyar felügyeleti hatóság joghatósága alá tartozóvá tette. Az EUB ugyanakkor a nemzeti bíróságra bízta az információk ellenőrzését és annak eldöntését, hogy a Weltimmo ténylegesen rendelkezett-e tevékenységi hellyel Magyarországon.

Ha az eljáró bíróság azt állapítja meg, hogy a Weltimmo rendelkezik tevékenységi hellyel Magyarországon, a magyar felügyeleti hatóság hatásköre kiterjed arra, hogy bírságot vessen ki. Mindazonáltal ha a nemzeti bíróság ennek ellenkezőjét állapítja meg, vagyis azt, hogy a Weltimmo nem rendelkezik tevékenységi hellyel Magyarországon, következésképp annak

509 EUB, *Weltimmo s. r. o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság*, C-230/14. sz. ügy, 2015. október 1.

a tagállam(ok)nak a jogát kell alkalmazni, ahol a vállalatot bejegyezték. Ebben az esetben, mivel a felügyeleti hatóságok hatásköreit a másik tagállam területi szuverenitásával összhangban kell alkalmazni, a magyar hatóság nem vethet ki bírságot. Mivel az adatvédelmi irányelv a felügyeleti hatóságok tekintetében együttműködési kötelezettséget ír elő, a magyar hatóság azonban megkérheti szlovák társát, hogy vizsgálja ki az ügyet, állapítsa meg a szlovák törvény megsértését, és vesse ki a szlovák jogszabályokban meghatározott bírságot.

Az általános adatvédelmi rendelet elfogadásával a felügyeleti hatóságok határon átnyúló esetekre vonatkozó joghatóságát illetően mára részletes szabályok kerültek kialakításra. A rendelet egy „egységességi" mechanizmust hoz létre, és tartalmaz a különböző felügyeleti hatóságok közötti együttműködést előíró rendelkezéseket. A határokon átnyúló esetekben a hatékony együttműködés érdekében az általános adatvédelmi rendelet előírja az adatkezelő vagy adatfeldolgozó tevékenységi központja vagy egyetlen tevékenységi helye felügyeleti hatóságaként egy fő felügyeleti hatóság létrehozását.[510] A fő felügyeleti hatóság felelős a határokon átnyúló esetekért, az adatkezelő vagy adatfeldolgozó egyetlen kapcsolattartója, és konszenzusra törekedve koordinálja az együttműködést az egyéb felügyeleti hatóságok között. Az együttműködés magában foglalja az információk cseréjét, a kölcsönös segítségnyújtást az ellenőrzés és vizsgálat, valamint kötelező érvényű határozatok elfogadása terén.[511]

Az Európa Tanács jogában a felügyeleti hatóságok jogköréről és hatásköréről a Korszerűsített 108. Egyezmény 12a cikke rendelkezik. Ezek a hatáskörök megegyeznek a felügyeleti hatóságok uniós jogban biztosított hatásköreivel, ideértve a vizsgálati és beavatkozási hatáskört, a hatáskört határozatok elfogadására és közigazgatási szankciók kiszabására az egyezmény rendelkezéseinek megsértéséért, valamint a hatáskört bírósági eljárás kezdeményezésére. A független felügyeleti hatóságok szintén rendelkeznek jogkörrel ahhoz, hogy érintettek megkereséseivel és panaszaival foglalkozzanak, tájékoztassák a nyilvánosságot az adatvédelmi törvényről, és tanácsot adjanak a nemzeti döntéshozóknak bármely, a személyes adatok kezelését szabályozó jogalkotási vagy közigazgatási intézkedés tekintetében.

510 Általános adatvédelmi rendelet, 56. cikk (1) bekezdés.

511 *Uo.*, 60. cikk.

5.3 Együttműködés

Az általános adatvédelmi rendelet egy általános keretet határoz meg a felügyeleti hatóságok közötti együttműködésre, és konkrétabb szabályokat állapít meg a felügyeleti hatóságok közötti együttműködésre a határokon átnyúló adatkezelési tevékenységeket illetően.

Az általános adatvédelmi rendelet értelmében a felügyeleti hatóságok a rendelet egységes végrehajtása és alkalmazása érdekében megosztják egymással a releváns információkat, és kölcsönösen segítséget nyújtanak egymásnak.[512] Ide tartozik, amikor a megkeresett felügyeleti hatóság konzultációt, ellenőrzéseket és vizsgálatokat folytat. A felügyeleti hatóságok közös műveleteket hajthatnak végre, ideértve a közös vizsgálatokat és a közös végrehajtási intézkedéseket is, amelyekben az összes felügyeleti hatóság alkalmazottai részt vesznek.[513]

Az EU-ban az adatkezelők és adatfeldolgozók egyre inkább transznacionális szinten dolgoznak. Ez az illetékes felügyeleti hatóságok közötti szoros együttműködést tesz szükségessé a tagállamokban annak biztosítására, hogy az adatkezelés megfeleljen az általános adatvédelmi rendelet követelményeinek. A rendelet „egységességi" mechanizmusa értelmében, ha egy adatkezelő vagy adatfeldolgozó több tagállamban rendelkezik tevékenységi hellyel, vagy ha egy tevékenységi hellyel rendelkezik, azonban az adatkezelési műveletek az érintetteket egynél több tagállamban jelentős mértékben érintik, fő hatóságként az adatkezelő vagy az adatfeldolgozó tevékenységi központja (vagy egyetlen tevékenységi helye) szerinti felügyeleti hatósága jár el. A fő hatóságok az adatkezelő vagy adatfeldolgozó ellen kényszerítő intézkedéseket hozhatnak. Az egységességi mechanizmus célja javítani a harmonizációt és az uniós adatvédelmi törvény egységes alkalmazását a különböző tagállamokban. Előnyös továbbá az üzleti vállalkozások számára is, mivel csak egy vezető hatósággal kell foglalkozniuk, nem pedig több felügyeleti hatósággal. Ez fokozza a jogbiztonságot a vállalkozások számára, és a gyakorlatban azt is jelenti, hogy a határozatokat gyorsabban meghozzák, és a vállalkozásoknak nem kell azzal szembesülniük, hogy a különböző felügyeleti hatóságok egymásnak ellentmondó követelményeket írnak számukra elő.

A fő felügyeleti hatóság azonosításához meg kell határozni a vállalkozás tevékenységi központját az EU-ban. A „tevékenységi központ" meghatározását az általános adatvédelmi rendelet tartalmazza. Ezenkívül a 29. cikk szerinti munkacsoport

512 *Uo.*, 61. cikk (1)–(3) bekezdés és 62. cikk (1) bekezdés.

513 *Uo.*, 62. cikk (1) bekezdés.

iránymutatást adott ki az adatkezelő és az adatfeldolgozó fő felügyeleti hatóságának azonosításához, amely tartalmazza a tevékenységi központ azonosításának kritériumait is.[514]

A magas szintű adatvédelem biztosításához az egész Unióban a fő felügyeleti hatóság nem egyedül jár el. Együtt kell működnie a többi érintett felügyeleti hatósággal az adatkezelők és adatfeldolgozók által végzett személyesadat-kezelési tevékenységekre vonatkozó határozatok elfogadása során, konszenzusra törekedve és a következetesség biztosítása érdekében. Az érintett felügyeleti hatóságok közötti együttműködés kiterjed az információcserére, kölcsönös segítségnyújtásra, közös vizsgálatok és ellenőrzési tevékenységek végzésére.[515] A kölcsönös segítségnyújtás során a felügyeleti hatóságok kötelesek pontosan kezelni a más felügyeleti hatóságtól érkező információkéréseket, és felügyeleti intézkedéseket kell tenniük, például előzetes engedélyezés és egyeztetés az adatkezelővel az adatkezelési tevékenységét illetően, ellenőrzések és vizsgálatokat lefolytatása. A kölcsönös segítségnyújtás keretében a más tagállamok felügyeleti hatóságától érkező megkereséseket indokolatlan késedelem nélkül, de legkésőbb a megkeresés kézhezvételétől számított egy hónapon belül meg kell válaszolni.[516]

Ha az adatkezelő több tagállamban is rendelkezik tevékenységi hellyel, a felügyeleti hatóságok közös műveleteket hajthatnak végre, ideértve a közös vizsgálatokat és a közös végrehajtási intézkedéseket is, amelyekben más tagállamok felügyeleti hatóságainak alkalmazottai is részt vesznek.[517]

Az Európa Tanács jogában is fontos követelmény a különböző felügyeleti hatóságok közötti együttműködés. A Korszerűsített 108. Egyezmény előírja, hogy a felügyeleti hatóságoknak a feladatuk ellátásához szükséges mértékben együtt kell működniük egymással.[518] Ez történhet például úgy, hogy biztosítják egymás számára az összes szükséges és hasznos információt, koordinálják a vizsgálatokat és közös intézkedéseket tesznek.[519]

514 29. cikk szerinti munkacsoport (2016), *Iránymutatás az adatkezelő vagy az adatfeldolgozó fő felügyeleti hatóságának meghatározásához*, WP 244, Brüsszel, 2016.december 13., felülvizsgálat időpontja: 2017. április 5.

515 Általános adatvédelmi rendelet, 60. cikk (1)–(3) bekezdés.

516 *Uo.*, 61. cikk (1) és (2) bekezdés.

517 *Uo.*, 62. cikk (1) bekezdés.

518 Korszerűsített 108. Egyezmény, 16–17. cikk.

519 *Uo.*, 17. cikk (1) bekezdés.

5.4 Az Európai Adatvédelmi Testület

A független felügyeleti hatóságok jelentőségét és az őket az európai adatvédelmi jog alapján megillető fő jogköröket az előzőekben ismertettük. Az Európai Adatvédelmi Testület (EDPB) egy másik fontos szereplő annak biztosítása során, hogy az adatvédelmi szabályokat az egész Unióban hatékonyan és következetesen alkalmazzák.

Az általános adatvédelmi rendelet létrehozta az Európai Adatvédelmi Testületet, amely egy jogi személyiséggel rendelkező uniós szerv.[520] A 29. cikk szerinti munkacsoport jogutódja,[521] amelyet az adatvédelmi irányelv hozott létre annak érdekében, hogy tanáccsal lássa el a Bizottságot az egyéneknek az adatkezeléshez és magánélethez fűződő jogait érintő minden uniós intézkedés tekintetében, előmozdítsa az irányelv egységes alkalmazását, valamint, hogy szakvéleményt biztosítson a Bizottság számára az adatvédelemhez kapcsolódó kérdésekben. A 29. cikk szerinti munkacsoport az uniós tagállamok felügyeleti hatóságainak képviselőiből állt, valamint a Bizottság képviselőiből és az európai adatvédelmi biztosból.

A munkacsoporthoz hasonlóan az Európai Adatvédelmi Testületet az egyes tagállamok felügyeleti hatóságainak vezetői és az európai adatvédelmi biztos, vagy ezek képviselői alkotják.[522] Az európai adatvédelmi biztos egyenlő szavazati jogot élvez, kivéve a vitarendezéssel kapcsolatos kérdéseket, amelyek esetén kizárólag az uniós intézményekre alkalmazandó elvekre és szabályokra vonatkozóan szavazhat, amelyek lényegében megegyeznek az általános adatvédelmi rendeletben foglalt elvekkel és szabályokkal. A Bizottságnak joga van részt venni az Európai Adatvédelmi Testület tevékenységeiben és ülésein, azonban nincs szavazati joga.[523] A Testület tagjai közül egyszerű többséggel öt évre elnököt (aki a Testület képviseletét látja el) és két elnökhelyettest választ. A Testület továbbá titkársággal rendelkezik, amelyet az európai adatvédelmi biztos biztosít, hogy a Testületnek legyen elemzési, igazgatási és logisztikai támogatása.[524]

520 Általános adatvédelmi rendelet, 68. cikk.

521 A 95/46/EK irányelv értelmében a 29. cikk szerinti munkacsoport feladatai közé a következők tartoztak: tanácsadás a Bizottság számára az egyéneknek a személyesadat-kezeléshez fűződő jogait érintő minden uniós intézkedés tekintetében, az irányelv egységes alkalmazásának előmozdítása, továbbá szakvélemény biztosítása a Bizottság számára az adatvédelemhez kapcsolódó kérdésekben. A 29. cikk szerinti munkacsoport az uniós tagállamok felügyeleti hatóságainak képviselőiből állt, valamint képviseltette magát benne a Bizottság és az európai adatvédelmi biztos is.

522 Általános adatvédelmi rendelet, 68. cikk (3) bekezdés.

523 *Uo.*, 68. cikk (4) és (5) bekezdés.

524 *Uo.*, 73. és 75. cikk.

Az Európai Adatvédelmi Testület feladatait az általános adatvédelmi rendelet 64., 65. és 70. cikkei ismertetik részletesen.

- **Következetesség:** Az Európai Adatvédelmi Testület három esetben kötelező érvényű határozatokat is kiad: amennyiben az érintett felügyeleti hatóság releváns és megalapozott kifogást emelt az egységességgel kapcsolatban; amennyiben véleménykülönbség van a tekintetben, hogy melyik felügyeleti hatóság a „fő"; végezetül pedig, amennyiben a felügyeleti hatóság nem kéri ki, vagy nem követi az európai adatvédelmi biztos véleményét.[525] Az Európai Adatvédelmi Testület fő felelőssége az általános adatvédelmi rendelet egységes alkalmazása az egész EU-ban, és kiemelt szerepet játszik az 5.5 szakaszban ismertetett egységességi mechanizmusban.

- **Konzultáció:** Az Európai Adatvédelmi Testület feladatai közé tartozik, hogy tanácsot adjon a Bizottságnak a személyes adatok uniós védelméhez kapcsolódó bármely kérdés vonatkozásában, így például az általános adatvédelmi rendelet módosításai, az adatkezelést érintő és az uniós adatvédelmi szabályokkal esetlegesen ellentétes uniós jogszabályok átdolgozása vagy a személyes adatok harmadik országba vagy nemzetközi szervezeteknek való továbbítását lehetővé tevő bizottsági megfelelőségi határozatok kiadása tekintetében.

- **Iránymutatás:** A Testület iránymutatásokat, ajánlásokat és bevált gyakorlatokat is közzétesz a rendelet egységes alkalmazásának ösztönzésére, és előmozdítja az együttműködést, valamint az ismeretek megosztását a felügyeleti hatóságok között. Emellett ösztönöznie kell az adatkezelői vagy adatfeldolgozói egyesületeket, hogy dolgozzanak ki magatartási kódexeket, továbbá hozzanak létre adatvédelmi tanúsítási mechanizmusokat és védjegyeket.

A Testület határozatai megtámadhatók az EUB előtt.

5.5 Az általános adatvédelmi rendelet egységességi mechanizmusa

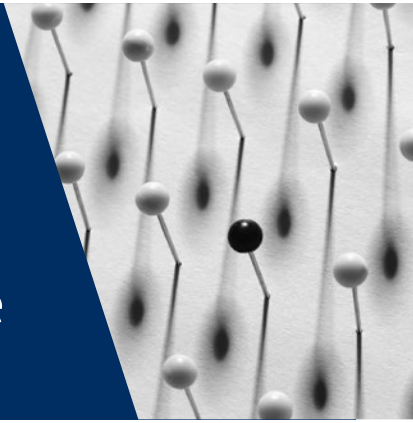
Az általános adatvédelmi rendelet létrehoz egy egységességi mechanizmust a rendelet egységes alkalmazásának biztosítására valamennyi tagállamban, amely során a felügyeleti hatóságok együttműködnek egymással, és adott esetben

525 *Uo.*, 65. cikk.

a Bizottsággal. Az egységességi mechanizmus alkalmazására két szituációban kerül sor. Az egyik az Európai Adatvédelmi Testület véleményeit érinti olyan esetekben, amikor az illetékes felügyeleti hatóság intézkedéseket szándékozik elfogadni. Ilyen például azon adatkezelési műveletek jegyzékének összeállítása, amelyekre vonatkozóan adatvédelmi hatásvizsgálatot kell végezni, vagy általános szerződési feltételek meghatározása. A második az Európai Adatvédelmi Testületnek a felügyeleti hatóságok számára az egységességi ügyekben, valamint olyan esetekben kiadott kötelező érvényű határozatait érinti, amikor a felügyeleti hatóság nem követi vagy nem kéri ki a Testület véleményét.

6

Az érintettek jogai és e jogok érvényesítése



EU	Tárgyalt kérdések	Európa Tanács
Tájékoztatáshoz való jog		
Általános adatvédelmi rendelet, 12. cikk EUB, *Institut professionnel des agents immobiliers (IPI) kontra Englebert*, C-473/12. sz. ügy, 2013 EUB, *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015	**Az adatok átláthatósága**	Korszerűsített 108. Egyezmény, 8. cikk
Általános adatvédelmi rendelet, 13. cikk (1) és (2) bekezdés és 14. cikk (1) és (2) bekezdés	**A tájékoztatás tartalma**	Korszerűsített 108. Egyezmény, 8. cikk (1) bekezdés
Általános adatvédelmi rendelet, 13. cikk (1) bekezdés és 14. cikk (3) bekezdés	**A tájékoztatás határideje**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés b) pont
Általános adatvédelmi rendelet, 12. cikk (1), (5) és (7) bekezdés	**Az információk rendelkezésre bocsátásának eszközei**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés b) pont
Általános adatvédelmi rendelet, 13. cikk (2) bekezdés d) pont és 14. cikk (2) bekezdés e) pont, 77., 78. és 79. cikk	**Panasz benyújtásának joga**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés f) pont

EU	Tárgyalt kérdések	Európa Tanács
Hozzáféréshez való jog		
Általános adatvédelmi rendelet, 15. cikk (1) bekezdés EUB, *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer*, C-553/07. sz. ügy, 2009	**Hozzáférés a személy saját adataihoz**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés b) pont EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987
EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel* és *Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014 EUB, *Peter Nowak kontra Data Protection Commissioner*, C-434/16. sz. ügy, 2017		
Helyesbítéshez való jog		
Általános adatvédelmi rendelet, 16. cikk	**A pontatlan személyes adatok helyesbítése**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés e) pont EJEB, *Cemalettin Canli kontra Törökország*, 22427/04. sz. ügy, 2008 EJEB, *Ciubotaru kontra Moldova*, 27138/04. sz. ügy, 2010
Törléshez való jog		
Általános adatvédelmi rendelet, 17. cikk (1) bekezdés	**A személyes adatok törlése**	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés e) pont EJEB, *Segerstedt-Wiberg és társai kontra Svédország*, 62332/00. sz. ügy, 2006
EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017	**Az elfeledtetéshez való jog**	

EU	Tárgyalt kérdések	Európa Tanács
Az adatkezelés korlátozásához való jog		
Általános adatvédelmi rendelet, 18. cikk (1) bekezdés	A személyes adatok felhasználásának korlátozásához való jog	
Általános adatvédelmi rendelet, 19. cikk	Értesítési kötelezettség	
Az adathordozhatósághoz való jog		
Általános adatvédelmi rendelet, 20. cikk	Az adathordozhatósághoz való jog	
A tiltakozáshoz való jog		
Általános adatvédelmi rendelet, 21. cikk (1) bekezdés EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017	Tiltakozáshoz való jog az érintett konkrét helyzete alapján	A profilalkotásra vonatkozó ajánlás, 5.3. cikk Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés d) pont
Általános adatvédelmi rendelet, 21. cikk (2) bekezdés	Tiltakozáshoz való jog az adatok üzletszerzési célokra történő felhasználásával kapcsolatban	A közvetlen üzletszerzésre vonatkozó ajánlás, 4.1. cikk
Általános adatvédelmi rendelet, 21. cikk (5) bekezdés	Tiltakozáshoz való jog az automatizált eszközökkel kapcsolatban	
Az automatizált döntéshozatallal és profilalkotással kapcsolatos jogok		
Általános adatvédelmi rendelet, 22. cikk	Az automatizált döntéshozatallal és profilalkotással kapcsolatos jogok	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés a) pont
Általános adatvédelmi rendelet, 21. cikk	Tiltakozáshoz való jog az automatizált döntéshozatallal kapcsolatban	
Általános adatvédelmi rendelet, 13. cikk (2) bekezdés f) pont	Érthető magyarázathoz való jog	Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés c) pont

EU	Tárgyalt kérdések	Európa Tanács
Jogorvoslat, felelősség, szankciók és kártérítés		
Charta, 47. cikk EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015 Általános adatvédelmi rendelet, 77–84. cikk	**A nemzeti adatvédelmi jogszabályok megsértése esetén**	EJEE, 13. cikk (csak az Európa Tanács tagállamai számára) Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés f) pont, 12., 15., 16–21. cikk EJEB, *K.U. kontra Finnország*, 2872/02. sz. ügy, 2008 EJEB, *Biriuk kontra Litvánia*, 23373/03. sz. ügy, 2008
Uniós intézmények adatvédelmi rendelete, 34. és 49. cikk EUB, *Európai Bizottság kontra The Bavarian Lager Co. Ltd.* [nagytanács], C-28/08. P. sz. ügy, 2010	**Az uniós jog uniós intézmények és szervek általi megsértése esetén**	

Általánosságban a jogi előírások és konkrétan az érintettek jogainak hatékonysága jelentős mértékben attól függ, hogy léteznek-e megfelelő mechanizmusok ezen előírások, illetve jogok érvényesítésére. A digitális korszakban az adatkezelés mindenütt jelen levővé vált és egyre nehezebben érthető az egyének számára. Az érintettek és az adatkezelők közötti nem egyenlő erőviszonyok csökkentése érdekében az egyéneket bizonyos jogokkal ruházták fel, hogy személyes adataik felett nagyobb ellenőrzést gyakorolhassanak. Az egyén saját személyes adataihoz való hozzáférési jogát és azok helyesbítéséhez való jogát az EU elsődleges jogát megtestesítő dokumentum, az EU Alapjogi Chartája 8. cikkének (2) bekezdése rögzíti, amely alapvető értékkel bír az Unió jogrendjében. A másodlagos jog – különösen az általános adatvédelmi rendelet – koherens jogi keretet teremtett, amely felhatalmazza az érintetteket azáltal, hogy jogokat biztosít számukra az adatkezelők tekintetében. A saját személyes adatokhoz való hozzáféréshez és azok helyesbítéséhez való jog mellett az általános adatvédelmi rendelet elismer egy sor egyéb jogot is, mint például a törléshez való jogot („az elfeledtetéshez való jog”), a tiltakozáshoz való jogot vagy az adatkezelés korlátozásához való jogot, továbbá az automatizált döntéshozatallal és profilalkotással kapcsolatos jogokat. A Korszerűsített 108. Egyezmény is tartalmaz hasonló garanciákat, amelyek lehetővé teszik az érintettek számára, hogy hatékony ellenőrzést gyakoroljanak adataik felett. A 9. cikk felsorolja azokat a jogokat, amelyeket az egyéneknek tudniuk kell gyakorolni személyes adataik

kezelésével kapcsolatban. A részes felek kötelesek biztosítani, hogy ezek a jogok joghatóságukban minden érintett számára rendelkezésre álljanak, és ezekhez hatékony jogi és gyakorlati eszközök társuljanak, amelyek lehetővé teszik az érintettek számára e jogok gyakorlását.

Az egyének számára biztosított jogok mellett ugyanolyan fontos olyan mechanizmusok kidolgozása is, amelyek lehetővé teszik az érintettek számára, hogy megtámadják jogaik megsértését, az adatkezelőket felelősségre vonják, és kártérítést követeljenek. Az EJEE-ben és a Chartában is garantált hatékony jogorvoslathoz való jog megköveteli, hogy a bírósági jogorvoslat lehetősége mindenki számára rendelkezésre álljon.

6.1 Az érintettek jogai

Főbb pontok

- Minden érintettnek joga van ahhoz, hogy bármely adatkezelőtől tájékoztatást kérjen – korlátozott számú mentesség mellett – arról, hogy az adatkezelő kezel-e rá vonatkozó adatokat.
- Az érintetteknek joga van ahhoz, hogy:
  - saját adataikhoz hozzáférjenek, és bizonyos tájékoztatást kérjenek azok kezeléséről;
  - adataikat az adatkezelővel helyesbíttessék, ha az adatok nem pontosak;
  - adataikat adott esetben töröltessék az adatkezelővel, ha az adatkezelő adataikat jogellenesen kezeli;
  - átmenetileg korlátozza az adatkezelést;
  - adataikat meghatározott feltételek mellett másik adatkezelőhöz vigyék át.
- Ezenfelül az érintett kifogásolhatja az adatkezelést a következők tekintetében:
  - konkrét helyzetével kapcsolatos okok;
  - adatai közvetlen üzletszerzési célokra való felhasználása esetén.
- Az érintettnek joga van ahhoz, hogy mentesüljön azon kizárólag automatizált adatkezelésen – ideértve a profilalkotást is – alapuló döntések alól, amelyek joghatással járnak vagy őt jelentős mértékben érintik. Az érintettnek joga van továbbá ahhoz, hogy:

- emberi beavatkozást kérjen és kapjon az adatkezelő részéről;
- kifejtse álláspontját, és hogy megtámadja az automatizált adatkezelésen alapuló döntést.

6.1.1 A tájékoztatáshoz való jog

A kezelési műveletek adatkezelői az **Európa Tanács** és az **EU joga** szerint is kötelesek a tervezett adatkezelésről az adatgyűjtés időpontjában tájékoztatni az érintettet. Ez a kötelezettség nem függ az érintett kérésétől, az adatkezelőnek inkább proaktívan kell eleget tennie e kötelezettségnek függetlenül attól, hogy az érintett érdeklődést mutat-e a tájékoztatás iránt.

Az Európa Tanács joga szerint a Korszerűsített 108. Egyezmény 8. cikke értelmében a részes felek kötelesek előírni, hogy az adatkezelők tájékoztassák az érintetteket kilétükről és szokásos tartózkodási helyükről, az adatkezelés jogalapjáról és céljáról, a kezelt személyes adatok kategóriáiról, a személyes adatok címzettjeiről (ha van ilyen) és arról, hogy gyakorolhatják a 9. cikk szerinti jogaikat, amelyek magukban foglalják a saját adataikhoz való hozzáféréshez, azok helyesbítéséhez és jogorvoslathoz való jogot. Minden további, a tisztességes és átlátható adatkezelés biztosításához szükségesnek tartott információt is közölni kell az érintettekkel. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés tisztázza, hogy az érintetteknek adott tájékoztatásnak „könnyen hozzáférhetőnek, olvashatónak és érthetőnek kell lennie, és a vonatkozó érintettekhez kell igazítani”.[526]

Az uniós jogban az átláthatóság elve megköveteli, hogy minden személyesadat-kezelés általánosságban legyen átlátható az egyének számára. Az egyéneknek joguk van tudni, hogy a rájuk vonatkozó személyes adatok közül melyeket és hogyan gyűjtik, használják fel, valamint tájékoztatást kell adni számukra a személyes adatok kezelésével összefüggő kockázatokról, garanciákról és jogaikról.[527] Az általános adatvédelmi rendelet tehát egy tág, átfogó kötelezettséget hoz létre az adatkezelők számára az átlátható tájékoztatás biztosítását és/vagy az érintettek arra vonatkozó tájékoztatását illetően, hogy miként tudják gyakorolni jogaikat.[528] A tájékoztatásnak tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek, világosan és közérthetően megfogalmazottnak kell lennie. A tájékoztatást írásban – ideértve adott esetben az elektronikus utat is – kell megadni, és az érintett kérésére akár

526 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 68. pont.

527 Általános adatvédelmi rendelet, (39) preambulumbekezdés.

528 *Uo.*, 13. és 14. cikk; Korszerűsített 108. Egyezmény, 8. cikk (1) bekezdés b) pont.

szóbeli tájékoztatás is adható, feltéve, hogy az érintett személyazonosságát kétséget kizáróan azonosították. A tájékoztatást túlzott késedelem vagy költségek nélkül kell megadni.[529]

Az általános adatvédelmi rendelet 13. és 14. cikke az érintettek tájékoztatáshoz való jogával foglalkozik, vagy olyan helyzetekben, amikor a személyes adatokat közvetlenül tőlük gyűjtötték, vagy olyan helyzetekben, amikor az adatokat nem az érintettől szerezték meg.

A tájékoztatáshoz való jog terjedelmét és korlátozását az uniós jog értelmében az EUB ítélkezési gyakorlatában tisztázta.

Példa: Az *Institut professionnel des agents immobiliers (IPI) kontra Englebert* ügyben[530] az EUB-t a 95/46 irányelv 13. cikke (1) bekezdésének értelmezésére kérték. Ez a cikk választási lehetőséget biztosított a tagállamok számára jogalkotási intézkedések elfogadásához az érintett tájékoztatáshoz való joga terjedelmének korlátozására, amennyiben az szükséges többek között mások jogainak és szabadságainak védelme, illetve bűncselekmények vagy a szabályozott foglalkozások etikai vétségeinek megelőzése és vizsgálata érdekében. Az IPI egy belga ingatlanügynököket tömörítő szakmai szervezet, amelynek feladata biztosítani az ingatlanügynöki foglalkozás megfelelő gyakorlásához szükséges feltételek tiszteletben tartását. Azzal a kéréssel fordult a nemzeti bírósághoz, hogy mondja ki, hogy a vádlottak megsértették a szakmai szabályokat, és rendelje el, hogy szüntessék be különféle ingatlanügynöki tevékenységüket. Az eljárás az IPI által megbízott magánnyomozók által szolgáltatott bizonyítékon alapult.

A nemzeti bíróságnak kétségei voltak a nyomozók bizonyítékainak értékével kapcsolatban, figyelemmel annak lehetőségére, hogy azokat a belga jog adatvédelmi követelményeinek, különösen pedig azon kötelezettség betartása nélkül szerezték be, hogy tájékoztassák az érintetteket az adatgyűjtés előtt a személyes adatok kezeléséről. Az EUB megjegyezte, hogy a 13. cikk (1) bekezdése kimondja, hogy a tagállamok jogszabályokat „fogadhatnak el", nem pedig kötelesek elfogadni annak

529 Általános adatvédelmi rendelet, 12. cikk (5) bekezdés; Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés b) pont.

530 EUB, *Institut professionnel des agents immobiliers (IPI) kontra Geoffrey Englebert és társai*, C-473/12. sz. ügy, 2013. november 7.

érdekében, hogy mentességet biztosítsanak az érintettek személyes adataik kezelésére vonatkozó tájékoztatási kötelezettség alól. Mivel a 13. cikk (1) bekezdése tartalmazza a bűncselekmények vagy a szabályozott foglalkozások etikai vétségeinek megelőzése, vizsgálata, felderítése és az ezekkel kapcsolatos eljárások lefolytatásának jogalapját, amely alapján a tagállamok korlátozhatják az egyének jogait. Egy olyan szervezet, mint amilyen az IPI és a nevében eljáró magánnyomozók támaszkodhatnak erre a rendelkezésre. Azonban ha valamely tagállam nem rendelkezett ilyen kivételről, az érintetteket tájékoztatni kell.

Példa: A *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai* ügyben[531] az EUB tisztázta, hogy az uniós jog tiltja-e, hogy egy nemzeti közigazgatási hatóság személyes adatokat továbbítson egy másik közigazgatási hatóságnak további kezelés céljából anélkül, hogy az érintetteket tájékoztatná-e az adattovábbításról és a kezelésről. Ebben az ügyben a nemzeti közigazgatási ügynökség az adattovábbítás előtt nem tájékoztatta a felpereseket arról, hogy adataikat továbbították a nemzeti egészségbiztosítási alapnak.

Az EUB megállapította, hogy a személyes adataik kezelése által érintett személyek tájékoztatására vonatkozó uniós jog szerinti kötelezettség „annál is inkább fontos, mivel az határozza meg az érintettek részéről a kezelt adatokhoz való hozzáférésre és helyesbítésre irányuló […] joguk, illetve az említett adatok kezelésével szembeni tiltakozáshoz való […] joguk gyakorlását". A tisztességes adatkezelés elve megköveteli az érintettek tájékoztatását adataik másik közigazgatási hatóságnak való továbbításáról abból a célból, hogy ez utóbbi tovább kezelje azokat. A 95/46 irányelv 13. cikkének (1) bekezdése szerint a tagállamok korlátozhatják a tájékoztatáshoz való jogot, amennyiben az az állam fontos gazdasági érdekének – beleértve az adózási ügyeket is –védelme miatt szükséges. Az ilyen korlátozások elfogadására azonban jogszabályok útján kell, hogy sor kerüljön. Mivel sem a továbbítandó adatok, sem az adattovábbítás részletes feltételei nem kerültek jogszabályban meghatározásra, hanem csak a két hatóság közötti jegyzőkönyv rögzítette azt, az uniós jog szerinti eltérés feltétele

531 EUB, *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015. október 1.

nem teljesültek. A felpereseket előzetesen tájékoztatni kellett volna adataik nemzeti egészségbiztosítási alapnak történő továbbításáról, és adataik szerv általi további kezeléséről.

A tájékoztatás tartalma

A Korszerűsített 108. Egyezmény 8. cikkének (1) bekezdése alapján az adatkezelő köteles minden olyan tájékoztatást megadni az érintettnek, ami biztosítja a személyes adatok tisztességes és átlátható kezelését, ideértve a következőket:

- az adatkezelő kiléte és szokásos lakóhelye vagy tevékenységi helye;
- a tervezett adatkezelés jogalapja és céljai;
- a kezelt személyes adatok kategóriái;
- a személyes adatok címzettei vagy címzetteinek kategóriái, ha van ilyen;
- az érintettek lehetőségei, hogy gyakorolják jogaikat.

Az általános adatvédelmi rendelet értelmében, ha az érintettre vonatkozó személyes adatokat az érintettől gyűjtik, az adatkezelő a személyes adatok megszerzésének időpontjában az érintett rendelkezésére bocsátja a következő információk mindegyikét:[532]

- az adatkezelőnek és – ha van ilyen – az adatvédelmi tisztviselőnek a kiléte és elérhetőségei;
- a személyes adatok tervezett kezelésének célja, valamint az adatkezelés jogalapja, vagyis egy szerződés vagy jogszabályi kötelezettség;
- az adatkezelő jogos érdekei, amennyiben ez jelenti az adatkezelés jogalapját;
- adott esetben a személyes adatok címzettjei, illetve a címzettek kategóriái;

532 Általános adatvédelmi rendelet, 13. cikk (1) bekezdés.

- annak ténye, hogy az adatkezelő harmadik országba vagy nemzetközi szervezet részére kívánja-e továbbítani a személyes adatokat, továbbá hogy ez a Bizottság megfelelőségi határozatán alapul-e, illetve hogy megfelelő garanciákra támaszkodik;

- a személyes adatok tárolásának időtartama, vagy ha ez nem lehetséges, az adattárolás időtartama meghatározásának szempontjai;

- az érintett adatkezeléssel kapcsolatos jogai, vagyis hogy kérelmezheti a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását, és tiltakozhat az adatok kezelése ellen;

- annak ténye, hogy a személyes adat szolgáltatása jogszabályon vagy szerződéses kötelezettségen alapul vagy szerződés kötésének előfeltétele-e, valamint hogy az érintett köteles-e a személyes adatokat megadni, továbbá hogy milyen lehetséges következményeikkel járhat az adatszolgáltatás elmaradása;

- automatizált döntéshozatal ténye, ideértve a profilalkotást is;

- a felügyeleti hatósághoz címzett panasz benyújtásának joga;

- a hozzájárulás visszavonásához való jog.

Automatizált döntéshozatal esetén, ideértve a profilalkotást is, az érintetteknek az alkalmazott logikára és arra vonatkozóan érthető információkat kell biztosítani, hogy az ilyen adatkezelés milyen jelentőséggel, és az érintettre nézve milyen várható következményekkel jár.

Azokban az esetekben, amikor a személyes adatokat nem közvetlenül az érintettektől szerzi be, az adatkezelő köteles tájékoztatni az egyént a személyes adatainak eredetéről. Ilyen esetekben az adatkezelő köteles tájékoztatni az érintetteket többek között az automatizált döntéshozatal tényéről, ideértve a profilalkotást is.[533] Végezetül pedig, ha az adatkezelő a személyes adatokat az eredetileg megjelölt céloktól eltérő célból kívánja kezelni, a célhoz kötöttség és az átláthatóság elve megköveteli, hogy az adatkezelő tájékoztassa az érintetteket az új célról. Az adatkezelőknek a további adatkezelést megelőzően tájékoztatnia kell az érintettet. Más szóval, azokban az esetekben, amikor az érintett hozzájárulását adta személyes adatainak

533 *Uo.*, 13. cikk (2) bekezdés és 14. cikk (2) bekezdés.

kezeléséhez, az adatkezelőnek be kell szereznie az érintett új hozzájárulását, ha az adatkezelés célja megváltozott, vagy ha további célokkal egészült ki.

A tájékoztatás határideje

Az általános adatvédelmi rendelet különbséget tesz két forgatókönyv és két olyan időbeli pont között, amikor az adatkezelőnek tájékoztatnia kell az érintettet.

- Amennyiben a személyes adatokat közvetlenül az érintettől szerzi be, az adatkezelőnek a személyes adatok megszerzésének időpontjában tájékoztatnia kell az érintettet valamennyi kapcsolódó információról és az általános adatvédelmi rendelet szerinti jogairól.[534]

  Ha az adatkezelő a személyes adatokat más célra tovább kívánja kezelni, a további kezelés előtt meg kell adnia minden vonatkozó tájékoztatást.

- Ha a személyes adatokat nem közvetlenül az érintettől szerezték meg, az adatkezelő köteles az érintett rendelkezésére bocsátani a kezelésre vonatkozó információkat „a személyes adatok megszerzésétől számított észszerű határidőn, de legkésőbb egy hónapon belül", vagy mielőtt az adatokat harmadik féllel közölné.[535]

A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kiköti, hogy amennyiben nem lehetséges az érintettek tájékoztatása az adatkezelés megkezdése előtt, azt később is meg lehet tenni, például akkor, amikor az adatkezelő valamilyen okból kapcsolatba kerül az érintettel.[536]

A tájékoztatás különböző módjai

Mind az Európa tanácsi, mind az uniós jog szerint az adatkezelő érintettnek adott tájékoztatásának tömörnek, átláthatónak, érthetőnek és könnyen hozzáférhetőnek kell lennie. A tájékoztatást írásban – ideértve adott esetben az elektronikus utat is

534 *Uo.*, 13. cikk (1) és (2) bekezdés, bevezető szöveg, ahol az általános adatvédelmi rendelet arra hivatkozik, hogy a tájékoztatási kötelezettség „a személyes adatok megszerzésének időpontjá[ra]" vonatkozik.

535 *Uo.*, 13. cikk (3) bekezdés és 14. cikk (3) bekezdés; lásd még az észszerű intervallumokra és a túlzott késedelem nélkül kikötésre tett hivatkozásokat a Korszerűsített 108. Egyezmény 8. cikke (1) bekezdésének b) pontjában.

536 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 70. pont.

– kell megadni, világosan, közérthető és könnyen érthető nyelvezet használatával. Tájékoztatás megadása során az adatkezelő használhat szabványosított ikonokat, hogy a tájékoztatást könnyen látható és érthető módon nyújtsa.[537] Egy lakatot jelképező ikon használható például annak jelzésére, hogy az adatok gyűjtése biztonságos és/vagy az adatok titkosítottak. Az érintettek kérhetik a szóbeli tájékoztatást. A tájékoztatás térítésmentes, kivéve, ha az érintett kérései egyértelműen megalapozatlanok vagy túlzók (pl. ismétlődő jellegük miatt).[538] Az adott tájékoztatás könnyű hozzáférhetősége kiemelkedően fontos az érintett azon képessége szempontjából, hogy gyakorolhassa az uniós adatvédelmi törvényben biztosított jogait.

A tisztességes adatkezelés elve megköveteli, hogy a tájékoztatás az érintettek számára könnyen érthető legyen. A címzettek számára megfelelő nyelvezetet kell használni. A nyelvezet szintjét és típusát szükség szerint a célközönségtől függően differenciálni kell, más-más nyelvezetet kell használni például felnőttek és gyermekek, a nagyközönség vagy tudományos szakértők esetében. A 29. cikk szerinti munkacsoport foglalkozott az összehangoltabb tájékoztatási rendelkezésekről szóló véleményében azzal, hogyan lehet megfelelő egyensúlyt teremteni az érthető tájékoztatás e szempontjai között. A munkacsoport az úgynevezett rétegzett tájékoztatás gondolatát[539] ösztönzi, amely lehetővé teszi, hogy az érintett eldöntse, milyen részletességű tájékoztatást szeretne kapni. A tájékoztatás ilyen megadása azonban nem mentesíti az adatkezelőt az általános adatvédelmi rendelet 13. és 14. cikke szerinti kötelezettsége alól. Az adatkezelőnek így is minden információt biztosítania kell az érintett számára.

A tájékoztatás egyik leghatékonyabb módja a megfelelő információs közlemények közzététele az adatkezelő honlapján, például internetes adatvédelmi politika formájában. A lakosság jelentős hányada azonban nem használja az internetet, és egy vállalat vagy hatóság tájékoztatási politikájának figyelembe kell ezt vennie.

Egy weboldalon a személyes adatok kezelésére vonatkozó tájékoztatás például a következő lehet:

537 Az Európai Bizottság felhatalmazáson alapuló jogi aktusok útján részletesebben ki fogja dolgozni az ikonok által jelzett információkat és az egységes ikonok biztosítására vonatkozó eljárásokat; lásd: általános adatvédelmi rendelet, 12. cikk (8) bekezdés.

538 Általános adatvédelmi rendelet, 12. cikk (1), (5) és (7) bekezdés; Korszerűsített 108. Egyezmény, 8. cikk (1) bekezdés b) pont.

539 29. cikk szerinti munkacsoport (2004), *10/2004 sz. vélemény az összehangoltabb tájékoztatási rendelkezésekről*, WP 100, Brüsszel, 2004. november 25.

Kik vagyunk mi?

Az adatokat kezelő „adatkezelő" a Bed and Breakfast C&U, székhelye: [Cím: xxx], Tel: xxx; Fax: xxx; E-mail: info@c&u.com; Adatvédelmi tisztviselő elérhetőségei: [xxx].

A személyes adatokra vonatkozó tájékoztatást a hotelünk szolgáltatásaira irányadó szolgáltatási feltételek tartalmazzák.

Milyen adatokat gyűjtünk?

A következő személyes adatokat gyűjtjük öntől: az ön neve, postacíme, telefonszáma, e-mail címe, tartózkodási helye, hitelkártya és betéti kártyaszám, valamint a weboldalunkra való csatlakozáshoz használt számítógépek IP címei vagy domain nevei.

Miért gyűjtjük az adatait?

Az ön személyes adatait az ön hozzájárulása alapján gyűjtjük a következő célokból: foglalás lebonyolítása, szerződés megkötése és teljesítése az általunk önnek kínált szolgáltatásokra vonatkozóan, illetve a törvény által előírt kötelezettségek teljesítése érdekében. Ilyen például a helyi adókról szóló törvény, amely értelmében azért kell személyes adatokat gyűjtenünk, hogy vendégeink megfizessék a városi idegenforgalmi adót.

Hogyan kezeljük az ön adatait?

Személyes adatait három hónapig őrizzük meg. Az ön adatai nem képezik automatizált döntéshozatal tárgyát.

Bed and Breakfast C&U hotelünk szigorú biztonsági eljárásokat követ annak biztosítására, hogy személyes adatai ne sérüljenek, ne semmisüljenek meg vagy jussanak harmadik fél tudomására az ön engedélye nélkül, illetve hogy megakadályozzuk a jogosulatlan hozzáférést adataihoz. Az adatokat tároló számítógépeket biztonságos környezetben tartjuk korlátozott fizikai hozzáférési lehetőséggel. Biztonságos tűzfalakat és egyéb intézkedéseket használunk az elektronikus hozzáférés korlátozására. Ha az adatokat harmadik félnek kell továbbítanunk, előírjuk számukra, hogy hasonló intézkedéseket alkalmazzanak személyes adatainak védelme érdekében.

Az általunk gyűjtött vagy rögzített összes információ irodáinkra korlátozódik. Az ön személyes adataihoz csak azok a személyek férhetnek hozzá, akiknek feladataik ellátásához szükségük van az adatokra. Amikor az ön azonosításához van szükségünk adatokra, azokat kifejezetten kérni fogjuk öntől. Felkérhetjük arra, hogy mielőtt információt adnánk ki önnek, működjön együtt biztonsági ellenőrzésünk során. A megadott személyes adatait bármikor aktualizálhatja, ha felveszi velünk közvetlenül a kapcsolatot.

Milyen jogok illetik meg önt?

Önnek joga van hozzáférnie az önről tárolt személyes adatokhoz, azok másolatának megszerzéséhez, kérni adatainak törlését vagy helyesbítését, vagy adatai másik adatkezelőhöz történő átvitelét.

Kérdéseivel forduljon hozzánk az címen. Megkeresésére egy hónapon belül válaszolnunk kell, azonban ha megkeresése túl összetett vagy túl sok egyéb megkeresés érkezik hozzánk, tájékoztatni fogjuk önt arról, hogy ez a határidő további két hónappal meghosszabbítható.

Hozzáférés személyes adataihoz

Önnek joga van hozzáférni személyes adataihoz, kérésre tájékoztatást kapni az adatkezelés alapját képező okokról, továbbá joga van személyes adatainak törlését vagy helyesbítését kérni, illetve, hogy véleménye figyelembe vétele nélkül ne tartozzon a kizárólag automatizált adatkezelésen alapuló döntések hatálya alá. Kérdéseivel forduljon hozzánk az címen. Önnek továbbá joga van tiltakozni az adatkezelés ellen, visszavonhatja hozzájárulását és panaszt kezdeményezhet a nemzeti felügyeleti hatóságnál, amennyiben úgy véli, hogy ez az adatkezelés jogszerűtlen, és kártérítést követelhet a jogszerűtlen adatkezelés következtében keletkezett károkért.

Panasz benyújtásának joga

Az általános adatvédelmi rendelet előírja, hogy az adatkezelő tájékoztassa az érintetteket a nemzeti és uniós jog értelmében a személyes adatokkal való visszaélés esetére fennálló jogérvényesítési mechanizmusokról. Az adatkezelőnek tájékoztatnia kell az érintetteket arról a jogukról, hogy a felügyeleti hatóságnál, és szükség esetén a nemzeti bíróságnál panaszt nyújthatnak be személyes adataikkal való

visszaélés esetén.[540] Az Európa Tanács szabályozása szintén elismeri az adatalany jogát a joggyakorlás módjairól való tájékoztatáshoz, beleértve a 9. cikk (1) bekezdés f) pontja szerinti jogorvoslathoz való jogot.

A tájékoztatási kötelezettség alóli kivételek

Az általános adatvédelmi rendelet kivételt biztosít a tájékoztatási kötelezettség alól. Az általános adatvédelmi rendelet 13. cikkének (4) bekezdése, valamint 14. cikkének (5) bekezdése értelmében az érintettek tájékoztatására vonatkozó kötelezettséget nem kell alkalmazni, amennyiben az érintett már rendelkezik az összes releváns információval.[541] Ezenkívül, amennyiben a személyes adatokat nem az érintettől szerezték be, a tájékoztatási kötelezettség nem alkalmazandó, ha az információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne, különösen a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból végzett adatkezelés esetében.[542]

Továbbá a tagállamoknak van mérlegelési mozgásterük az általános adatvédelmi rendelet keretében, hogy korlátozzák az egyének rendelet értelmében fennálló kötelezettségeit és jogait, amennyiben az egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül, például a nemzetbiztonság és közbiztonság védelme, igazságügyi nyomozások és eljárások védelme vagy a gazdasági és pénzügyi érdekek védelme, valamint az adatvédelmi érdekeknél kényszerítőbb erejű magánérdekek védelme érdekében.[543]

Minden kivételnek vagy korlátozásnak egy demokratikus társadalomban szükségesnek, valamint a kitűzött jogszerű céllal arányosnak kell lennie. Nagyon kivételes esetekben, például orvosi javallatra, az érintett védelme önmagában megköveteli az átláthatóság korlátozását; ez különösen az érintettek betekintési jogának korlátozására vonatkozik.[544] Minimális szintű védelemként azonban a nemzeti jognak tiszteletben kell tartania az uniós jogban védelmet élvező alapvető jogok és szabadságok lényegét.[545] Ehhez szükséges, hogy a nemzeti jog tartalmazzon olyan konkrét

540 Általános adatvédelmi rendelet, 13. cikk (2) bekezdés d) pont és 14. cikk (2) bekezdés e) pont; Korszerűsített 108. Egyezmény, 8. cikk (1) bekezdés f) pont.

541 Általános adatvédelmi rendelet, 13. cikk (4) bekezdés és 14. cikk (5) bekezdés a) pont.

542 *Uo.*, 14. cikk (5) bekezdés b)–e) pont.

543 *Uo.*, 23. cikk (1) bekezdés.

544 *Uo.*, 15. cikk.

545 *Uo.*, 23. cikk (1) bekezdés.

rendelkezéseket, amelyek tisztázzák az adatkezelés célját, a személyes adatok érintett kategóriáit, garanciákat és egyéb eljárási követelményeket.[546]

A közérdekű archiválás céljából, tudományos és történelmi kutatási vagy statisztikai célból gyűjtött adatok esetében az uniós vagy tagállami jog biztosíthat eltéréseket a tájékoztatási kötelezettség tekintetében, ha az valószínűsíthetően lehetetlenné tenné, vagy súlyosan hátráltatná az adott célok elérését.[547]

Hasonló korlátozásokat tartalmaz az Európa Tanács szabályozása, ahol a Korszerűsített 108. Egyezmény 9. cikke szerinti érintetti jogokat korlátozni lehet a Korszerűsített 108. Egyezmény 11. cikke alapján, szigorú feltételek teljesülése esetén. Továbbá a Korszerűsített 108. Egyezmény 8. cikk (2) bekezdése szerint az adatkezelés átláthatóságának kötelezettsége nem áll fenn akkor, amikor az adatalany már rendelkezik a vonatkozó információkkal.

Hozzáférés a személy saját adataihoz

Az **Európa Tanács joga szerint** az egyén saját személyes adataihoz való hozzáférésének jogát kifejezetten elismeri a Korszerűsített 108. Egyezmény 8. cikke. Ez minden egyén számára biztosítja a jogot, hogy kérésre tájékoztatást kapjon a rá vonatkozó személyes adatok kezeléséről, amelyet érthető módon kell közölni. Az egyén saját személyes adataihoz való hozzáférésének jogát nem csak a Korszerűsített 108. Egyezmény rendelkezései ismerik el, hanem az EJEB ítélkezési gyakorlata is. Az EJEB ismételten megállapította, hogy az egyének rendelkeznek a saját személyes adataikra vonatkozó tájékoztatáshoz való joggal, és hogy ez a jog a magánélet tiszteletben tartásának szükségességéből ered.[548] Az állami vagy magán szervezetek által tárolt személyes adatokhoz való hozzáférés joga azonban bizonyos körülmények között korlátozható.[549]

Az **uniós jog szerint** az egyén saját személyes adataihoz való hozzáférésének jogát kifejezetten elismeri az általános adatvédelmi rendelet 15. cikke, és azt az EU Alapjogi Chartája 8. cikkének (2) bekezdése a személyes adatok védelméhez való

546 *Uo.*, 23. cikk (2) bekezdés.

547 *Uo.*, 89. cikk (2) és (3) bekezdés.

548 EJEB, *Gaskin kontra Egyesült Királyság*, 10454/83. sz. ügy, 1989. július 7.; EJEB, *Odièvre kontra Franciaország* [Nagykamara], 42326/98. sz. ügy, 2003. február 13.; EJEB, *K.H. és társai kontra Szlovákia*, 32881/04. sz. ügy, 2009. április 28.; EJEB, *Godelli kontra Olaszország*, 33783/09. sz. ügy, 2012. szeptember 25.

549 EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987. március 26.

alapjog részeként határozza meg.[550] Az európai adatvédelmi jogban kiemelt szerepet kap az egyén saját személyes adataihoz való hozzáférésének joga.[551]

Az általános adatvédelmi rendelet minden egyén számára biztosítja a jogot, hogy hozzáférjen saját személyes adataihoz és az adatkezeléssel kapcsolatos egyes információkhoz, amelyeket az adatkezelők kötelesek megadni.[552] Az érintett jogosult különösen arra, hogy (az adatkezelőtől) visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e, és tájékoztatást kapjon legalább a következőkre vonatkozóan:

- az adatkezelés céljai;
- érintett adatkategóriák;
- adatok címzettjei, illetve a címzettek kategóriái, akik felé az adatokat továbbítják;
- a személyes adatok tárolásának tervezett időtartama, vagy ha ez nem lehetséges, ezen időtartam meghatározásának szempontjai;
- az érintett azon joga, hogy kérelmezheti a rá vonatkozó személyes adatok helyesbítését, törlését vagy kezelésének korlátozását;
- a felügyeleti hatósághoz címzett panasz benyújtásának joga;
- ha az adatkezelés tárgyát képező adatokat nem az érintettől gyűjtötték, a forrásukra vonatkozó minden elérhető információ;
- automatizált döntések esetében az adatok automatizált adatkezelés során alkalmazott logika.

550 Lásd még: EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel és Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014. július 17.; EUB, *ClientEarth, Pesticide Action Network Europe (PAN Europe) kontra Európai Élelmiszerbiztonsági Hatóság (EFSA), Európai Bizottság*, C-615/13. P. sz. ügy, 2015. július 16.

551 EUB, *YS kontra Minister voor Immigratie, Integratie en Asiel és Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014. július 17.

552 Általános adatvédelmi rendelet, 15. cikk (1) bekezdés.

Az adatkezelő köteles az adatkezelés tárgyát képező személyes adatok másolatát az érintett rendelkezésére bocsátani. Az érintettel közölt minden információt érthető formában kell megadni, ami azt jelenti, hogy az adatkezelőnek biztosítania kell, hogy az érintett megértse az adott tájékoztatást. Például, a személyes adatokba való betekintésre irányuló kérelemre válaszul rendszerint nem elegendő szakmai rövidítéseket, kódolt kifejezéseket vagy mozaikszavakat használni, hacsak nem fejtik ki e kifejezések jelentését. Automatizált döntéshozatalkor, ideértve a profilalkotást is, az automatizált döntéshozatal általános logikáját meg kell magyarázni, beleértve azokat a konkrét kritériumokat is, amelyeket az érintett értékelése során mérlegeltek. Hasonló követelmények az **Európa Tanács jogában** is léteznek.[553]

Példa: A személyes adataihoz való hozzáférés segít az érintettnek eldönteni, hogy adatai pontosak-e vagy sem. Éppen ezért lényeges, hogy az érintettet érthető módon tájékoztassák ne csak a tényleges adatkezelés tárgyát képező személyes adatairól, hanem azokról a kategóriákról, amelyek alatt ezeket a személyes adatokat kezelik, például név, IP-cím, geolokalizációs koordináták, hitelkártyaszám, stb.

Az adatkezelőnek – hozzáférés iránti kérelemre válaszul – tájékoztatást kell adnia a kezelés alatt álló adatok forrásával kapcsolatban, amennyiben az adatokat nem az érintettől szerezte be. E rendelkezés a tisztességes eljárás, az átláthatóság és az elszámoltathatóság elvével összefüggésben értendő. Az adatkezelő nem semmisítheti meg az adatok forrására vonatkozó információt azért, hogy mentesüljön annak kiadása alól – kivéve, ha a törlésre a hozzáférés iránti kérelem beérkezése ellenére sor kerülne –, és továbbra is eleget kell tennie az elszámoltathatóságra vonatkozó általános kötelezettséggel.

Az EUB ítélkezési gyakorlatában megállapítottak szerint a személyes adatokhoz való hozzáférés joga indokolatlanul nem korlátozható határidők megállapításával. Az érintettek számára észszerű lehetőséget kell biztosítani arra, hogy információt gyűjtsenek a múltban elvégzett adatkezelési műveletekről.

553 Lásd a Korszerűsített 108. Egyezmény 8. cikke (1) bekezdésének c) pontját.

Példa: A *Rijkeboer* ügyben[554] az EUB-ot annak megállapítására kérték, hogy valamely személynek a rá vonatkozó személyes adatok címzettjeire vagy a címzettek kategóriájára vonatkozó információkhoz, illetve az adatok tartalmához való hozzáférés joga korlátozható-e az adathozzáférés iránti kérelem benyújtását megelőző egyéves időtartamra.

Annak meghatározásához, hogy az uniós szabályozás lehetővé tesz-e, vagy sem ilyen időbeli korlátozást, az EUB úgy döntött, hogy a 12. cikket az irányelv célkitűzéseire figyelemmel értelmezi. Az EUB először is megállapította, hogy a hozzáféréshez való jog szükséges annak lehetővé tételéhez, hogy az érintett gyakorolja azon jogát, hogy kérelmére az adatkezelő helyesbítse, törölje vagy zárolja az adatait, vagy kérelmére az adatkezelő értesítse az adatokról tudomást szerző harmadik feleket e helyesbítésről, törlésről vagy zárolásról. Tényleges hozzáférési jog szükséges továbbá azért, hogy az érintettek számára lehetővé tegye az adatkezelés elleni tiltakozáshoz való joguk gyakorlását vagy panasz benyújtásának jogát, illetve azon jogukat, hogy kártérítést követeljenek.[555]

Az érintetteket megillető jogok hatékony érvényesülése érdekében az EUB megállapította, hogy „e jognak szükségszerűen a múltra is vonatkoznia kell. Ellenkező esetben ugyanis az érintett személy nem gyakorolhatná eredményesen a jogszerűtlennek vagy helytelennek vélt adatok helyesbítéséhez, törléséhez vagy zárolásához fűződő, valamint jogorvoslati és kártérítéshez való jogát."

6.1.2 A helyesbítéshez való jog

Az **uniós jogban** és az **Európa Tanács jogában** is az érintetteknek joguk van személyes adataik helyesbítéséhez. A személyes adatok pontossága elengedhetetlen az érintettek magas szintű adatvédelmének biztosításához.[556]

554 EUB, *College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer*, C-553/07. sz. ügy, 2009. május 7.

555 Általános adatvédelmi rendelet, 15. cikk (1) bekezdés c) és f) pont, 16. cikk, 17. cikk (2) bekezdés és 21. cikk, továbbá VIII. fejezet.

556 *Uo.*, 16. cikk és (65) preambulumbekezdés; Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés e) pont.

Példa: A *Ciubotaru kontra Moldova* ügyben[557] a felperes állítólag azért nem tudta moldovánról románra változtatni az etnikai származására vonatkozó bejegyzést a hivatalos nyilvántartásban, mert kérelmét nem támasztotta alá bizonyítékkal. Az EJEB megítélése szerint elfogadható, ha az állam az egyén etnikai származásának nyilvántartásba vételekor objektív bizonyítékot kér. Amennyiben az állítás pusztán szubjektív, bizonyítékkal alá nem támasztott alapokon nyugszik, a hatóságok visszautasíthatják azt. A felperes állítása azonban nem csupán saját etnikai hovatartozásának szubjektív megítélésén alapult; objektíven ellenőrizhető kapcsolódási pontokat tudott kimutatni – például a nyelv, a név, az együttérzés és egyebek tekintetében – a román etnikumhoz. A hazai jog szerint azonban a felperesnek bizonyítania kellett, hogy szülei a román etnikumhoz tartoztak. Figyelembe véve Moldova történelmi realitását, egy ilyen követelmény leküzdhetetlen akadályt jelentett azzal kapcsolatban, hogy a felperes a szovjet hatóságok által a szüleire vonatkozóan bejegyzett etnikai identitástól eltérő etnikai származást vetessen nyilvántartásba. Az állam azzal, hogy megakadályozta, hogy a felperes állítását objektíven ellenőrizhető bizonyítékok fényében vizsgálják, nem tett eleget azon pozitív kötelezettségének, hogy biztosítsa a felperes magánélethez való jogának tényleges tiszteletben tartását. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Egyes esetekben elegendő, ha az érintett egyszerűen csak kéri például neve betűzésének helyesbítését, megváltozott címének vagy telefonszámának kijavítását. Az **uniós jog** és az **Európa Tanács joga** alapján a pontatlan személyes adatokat indokolatlan vagy túlzott késedelem nélkül helyesbíteni kell.[558] Ha azonban az ilyen kéréshez jogilag lényeges kérdés kapcsolódik – például az érintett jogi személyisége, vagy a jogi dokumentumok kézbesítése szempontjából helyes tartózkodási helye –, előfordulhat, hogy a helyesbítés iránti kérelem nem elegendő, és az adatkezelő követelheti az állítólagos valótlanság bizonyítását. E követelés nem róhat túl nagy bizonyítási terhet az érintettre, és ezáltal nem akadályozhatja meg az érintettet abban, hogy adatait helyesbíttesse. Az EJEB számos olyan esetben megállapította az EJEE 8. cikkének megsértését, amikor a felperes nem tudta vitatni a titkos nyilvántartásokban tárolt információk helyességét.[559]

557 EJEB, *Ciubotaru kontra Moldova*, 27138/04. sz. ügy, 2010. április 27., 51. és 59. pont.

558 Általános adatvédelmi rendelet, 16. cikk; Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés.

559 EJEB, *Rotaru kontra Románia* [Nagykamara], 28341/95. sz. ügy, 2000. május 4.

Példa: A *Cemalettin Canli kontra Törökország* ügyben[560] az EJEB megállapította az EJEE 8. cikkének megsértését büntetőeljárásban történt hibás rendőrségi jelentés miatt.

A felperest kétszer vonták büntetőeljárás alá illegális szervezetben való állítólagos tagság miatt, de nem ítélték el. Amikor a felperest újra letartóztatták és más bűncselekmény miatt elítélték, a rendőrség *„tájékoztató további bűncselekményekről"* címmel jelentést nyújtott be a büntetőbíróságra, amelyben a felperesről azt állították, hogy két illegális szervezet tagja. A felperesnek a jelentés és a rendőrségi nyilvántartás módosítására irányuló kérését elutasították. Az EJEB megállapította, hogy a rendőrségi jelentésben szereplő információk az EJEE 8. cikkének hatálya alá tartoznak, mivel a nyilvános információk is a „magánélet" körébe tartozhatnak, ha szisztematikusan gyűjtötték és a hatóságok által vezetett aktákban tárolják azokat. Ezenfelül, a rendőrségi jelentés valótlan volt, az elkészítése és a büntetőbírósághoz való benyújtása pedig nem felelt meg a hazai jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették a 8. cikket.

Az adatok helyességének megállapítására indított polgári peres eljárásban vagy hatósági eljárásban az érintett kérheti, hogy adatállományában bejegyzést vagy megjegyzést helyezzenek el, miszerint az adatok helyességét vitatják, és az erre vonatkozó hivatalos döntés folyamatban van.[561] Ez idő alatt az adatkezelő nem tüntetheti fel az adatokat helyesként, és nem hallgathatja el, hogy azok módosítás alatt vannak, különösen nem harmadik felekkel szemben.

6.1.3 A törléshez való jog („az elfeledtetéshez való jog")

Az adatvédelmi elvek, nevezetesen az adattakarékosság elvének (a személyes adatok kezelését az adatkezelési cél teljesítéséhez szükségesre kell korlátozni) hatékony alkalmazása szempontjából különösen fontos biztosítani az érintettek számára

560 EJEB, *Cemalettin Canli kontra Törökország*, 22427/04. sz. ügy, 2008. november 18., 33. és 42–43. pont; EJEB, *Dalea kontra Franciaország*, 964/07. sz. ügy, 2010. február 2.

561 Általános adatvédelmi rendelet, 18. cikk és (67) preambulumbekezdés.

a rájuk vonatkozó személyes adatok törléséhez való jogot. A törléshez való jog ezért megtalálható az Európa tanácsi és uniós jogi eszközökben egyaránt.[562]

Példa: A *Segerstedt-Wiberg és társai kontra Svédország* ügyben[563] a felperesek tagjai voltak bizonyos liberális és kommunista politikai pártoknak. A felperesek gyanították, hogy adataikat felvették a rendőrségi nyilvántartásba, és kérték azok törlését. Az EJEB meggyőződött arról, hogy a kérdéses adatok tárolására volt jogalap, és az adatok tárolása jogszerű célt szolgált. Egyes felperesek esetében azonban az EJEB úgy találta, hogy az adatok tartós megőrzése aránytalan beavatkozást jelent e személyek magánéletébe. Egy felperes esetében például a hatóságok megőrizték azt az információt, hogy 1969-ben tüntetések során H. Schmid állítólag erőszakosan ellenállt a rendőri ellenőrzésnek. Az EJEB megállapította, hogy ez az információ – figyelembe véve különösen azt, hogy milyen régen keletkezett – semmiféle releváns nemzetbiztonsági érdeket nem szolgálhat. A Bíróság azt állapította meg, hogy az öt felperes közül négy esetében megsértették az EJEE 8. cikkét, mivel – figyelemmel a felperesek állítólagos cselekedete óta eltelt hosszú időre – hiányzott adataik folytatólagos tárolásának relevanciája.

Példa: A *Brunet kontra Franciaország* ügyben[564] a felperesek feljelentést tettek személyes adataiknak elítéltekre, vádlottakra és áldozatokra vonatozó adatokat tartalmazó rendőrségi adatbázisban való tárolása miatt. Annak ellenére, hogy a felperes elleni büntetőeljárást megszüntették, adatai szerepeltek az adatbázisban. Az EJEB megállapította, hogy megsértették az EJEE 8. cikkét. E következtetés levonásához a bíróság mérlegelte, hogy gyakorlatilag nem volt a felperesnek lehetősége töröltetni adatait az adatbázisból. Az EJEB továbbá megvizsgálta az adatbázisban szereplő információk jellegét, és azt állapította meg, hogy azok a felperes magánéletét illetően betolakodó jellegűek voltak, mivel személyazonosságával és személyiségével kapcsolatos adatokat tartalmaztak. Ráadásul megállapította, hogy a személyes adatok adatbázisban való megőrzésének ideje, ami 20 év volt, túlzottan hosszú volt, különös figyelemmel arra, hogy soha egyetlen bíróság sem ítélte el a felperest.

562 *Uo.*, 17. cikk.

563 EJEB, *Segerstedt-Wiberg és társai kontra Svédország*, 62332/00. sz. ügy, 2006. június 6., 89. és 90. pont. Lásd még például: EJEB, *M.K. kontra Franciaország*, 19522/09. sz. ügy, 2013. április 18.

564 EJEB, *Brunet kontra Franciaország*, 21010/10. sz. ügy, 2014. szeptember 18.

A Korszerűsített 108. Egyezmény kifejezetten elismeri, hogy minden egyénnek joga van töröltetni a pontatlan, hibás vagy jogszerűtlenül kezelt adatokat.[565]

Az uniós jog alapján az általános adatvédelmi rendelet 17. cikke érvényre juttatja az érintettek adataik törlésére irányuló kéréseit. A személyes adatok indokolatlan késedelem nélküli törléséhez való jog a következő esetekben áll fenn:

- a személyes adatokra már nincs szükség abból a célból, amelyből azokat gyűjtötték vagy más módon kezelték;
- az érintett visszavonja az adatkezelés alapját képező hozzájárulását, és az adatkezelésnek nincs más jogalapja;
- az érintett tiltakozik az adatkezelése ellen, és nincs elsőbbséget élvező jogszerű ok az adatkezelésre;
- a személyes adatokat jogellenesen kezelték;
- a személyes adatokat az adatkezelőre alkalmazandó uniós vagy tagállami jogban előírt jogszabályi kötelezettség teljesítéséhez törölni kell;
- a személyes adatok gyűjtésére az általános adatvédelmi rendelet 8. cikkében említett, információs társadalommal összefüggő szolgáltatások gyermekeknek történő kínálásával kapcsolatosan került sor.[566]

Az azzal kapcsolatos bizonyítási teher, hogy az adatkezelés jogszerű, az adatkezelőket terheli, mivel az adatkezelők felelnek az adatkezelés jogszerűségéért.[567] Az elszámoltathatóság elve szerint az adatkezelőnek bármikor tudnia kell bizonyítani, hogy az általa végzett adatkezelésnek megbízható jogalapja van, ellenkező esetben be kell szüntetni az adatkezelést.[568] Az általános adatvédelmi rendelet kivételeket határoz meg az elfeledtetéshez való jog alól, beleértve azon eseteket, amikor a személyes adatok kezelése a következők miatt szükséges:

565 Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés e) pont.

566 Általános adatvédelmi rendelet, 17. cikk (1) bekezdés.

567 *Uo.*

568 *Uo.*, 5. cikk (2) bekezdés.

- a véleménynyilvánítás szabadságához és a tájékozódáshoz való jog gyakorlása céljából;

- a személyes adatok kezelését előíró, az adatkezelőre alkalmazandó uniós vagy tagállami jog szerinti kötelezettség teljesítése, illetve közérdekből vagy az adatkezelőre ruházott közhatalmi jogosítvány gyakorlása keretében végzett feladat végrehajtása céljából;

- a népegészségügy területét érintő közérdek alapján;

- közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból;

- jogi igények előterjesztéséhez, érvényesítéséhez, illetve védelméhez.[569]

Az EUB megerősítette a törléshez való jog jelentőségét a magas szintű adatvédelem biztosítása szempontjából.

Példa: A *Google Spain* ügyben[570] az EUB azt vizsgálta meg, hogy a Google köteles-e törölni a felperes pénzügyi nehézségeire vonatkozó elavult információkat a keresés találati listájából. A Google többek között azt vitatta, hogy felelős lenne. Azzal érvelt, hogy ő mindössze az információkat tároló kiadó – ami ebben az esetben a felperes fizetésképtelenségi ügyéről beszámoló újság volt – weboldalára mutató hiperhivatkozást jelenít meg.[571] A Google szerint az elavult információk weboldalról való törlésére irányuló kérést a weboldal tárolója, nem pedig a Google felé kell intézni, amely egyszerűen egy az eredeti oldalra mutató linket biztosít. Az EUB arra a következtetésre jutott, hogy a Google, amikor a webes információk és

569 *Uo.*, 17. cikk (3) bekezdés.

570 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 55–58. pont.

571 A Google azt is vitatta, hogy vonatkoznának rá az uniós adatvédelmi szabályok, mivel a Google Inc. az USA-ban bejegyzett cég, és a szóban forgó személyes adatok kezelésére szintén az USA-ban került sor. Az uniós adatvédelmi törvény alkalmazhatatlansága melletti második érv ahhoz az állításhoz kapcsolódott, miszerint a keresőmotorok nem tekinthetők „adatkezelőnek" a találataik között megjelenített adatok tekintetében, mivel nem ismerik az adatokat és ellenőrzést sem gyakorolnak felettük. Az EUB elutasította mindkét érvet, és kitartott amellett, hogy ebben az esetben alkalmazandó a 95/46/EK irányelv, és folytatta az általa garantált jogok, különösen a személyes adatok törléséhez való jog terjedelmének vizsgálatát.

weboldalak között keres, és amikor a találati lista összeállításához indexálja a tartalmat, adatkezelővé válik, amelyre az uniós jog szerinti felelősségek és kötelezettségek vonatkoznak.

Az EUB tisztázta, hogy az internetes keresőmotorok és a személyes adatokat szolgáltató találati listák lehetővé teszik, hogy létrehozzák az érintett részletes profilját.[572] A keresőmotorok az ilyen találati listában szereplő adatokat mindenütt jelenlevővé teszik. Figyelemmel a lehetséges esetek súlyosságára, ezt a beavatkozást önmagában a keresőmotor működtetőjének ezen adatkezeléshez fűződő gazdasági érdeke nem igazolhatja. Tisztességes egyensúlyt kell teremteni különösen az internethasználóknak az információkhoz való hozzáféréshez fűződő jogos érdekei és az érintettnek az EU Alapjogi Chartájának 7. és 8. cikkében biztosított alapjogai között. Figyelemmel a fokozottan digitalizált társadalomra, az a követelmény, hogy a személyes adatok pontosak legyenek és csak a szükségesre korlátozódjanak (pl. nyilvános információnál) alapvető követelmény az egyének számára történő magas szintű adatvédelem biztosítása érdekében. A „(a keresőmotor működtetőjének) – adatkezelőként – felelősségi körén, hatáskörén és lehetőségein belül biztosítania kell, hogy az általa végzett adatkezelés megfelel" az uniós jognak, annak érdekében, hogy a biztosított garanciák valamennyi joghatásukat kifejthessék.[573] Ez azt jelenti, hogy a személyes adatok töröltetéséhez való jog, ha az adatkezelés már elavult vagy többé már nem szükséges, kiterjed azokra az adatkezelőkre is, aki lemásolják az információkat.[574]

Annak vizsgálata során, hogy a Google köteles-e törölni a felperesre vonatkozó hivatkozásokat, az EUB úgy vélte, hogy bizonyos feltételek mellett az egyénnek jogában áll kérni személyes adatai törlését. E jogra akkor lehet hivatkozni, ha az egyénre vonatkozó információk pontatlanok, nem megfelelők, irrelevánsak vagy az adatkezelés céljához mérten

572 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 36., 38., 80–81. és 97. pont.

573 *Uo.*, 81–83. pont.

574 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13., 88. pont. Lásd még: 29. cikk szerinti munkacsoport (2014), *Az EUB „Google Spain and Inc kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González" C-131/12. sz. ügyben hozott ítéletének végrehajtására vonatkozó iránymutatás*, WP 225, Brüsszel, 2014. november 26.; a Miniszteri Bizottság tagállamokhoz intézett CM/Rec(2012)3. sz. ajánlása az emberei jogok védelméhez a keresőmotorok tekintetében, 2012. április 4.

túlzottak. Az EUB elismerte, hogy ez a jog nem abszolút. Egyéb jogokkal, különösen a nyilvánosság bizonyos információhoz való hozzáféréséhez fűződő érdekével összevetve szükséges mérlegelni. Minden törlés iránti kérelmet eseti alapon kell megvizsgálni, hogy megfelelő egyensúlyt lehessen teremteni egyrészről az érintett személyes adatok védelméhez és magánélethez való alapjogai, másrészről pedig valamennyi internethasználó – köztük a kiadók – jogos érdekei között. Az EUB iránymutatást adott azon tényekre vonatkozóan, amelyeket a mérlegelés során figyelembe kell venni. A kérdéses információ természete különösen fontos tényező. Ha az információ az egyén magánéletéhez kapcsolódik, és nem fűződik közérdek az információ rendelkezésre állásához, az adatvédelem és a magánélet megelőzi a nyilvánosság tájékoztatáshoz való jogát. Ezzel szemben azonban, ha az érintett közszereplőnek tűnik, vagy az információ azon jellege indokolja, hogy az ahhoz való hozzáférést a nyilvánosság nyomós érdeke indokolja, az érintett adatvédelemhez és magánélethez való alapjogába való beavatkozás jogosnak minősül.

Az ítéletet követően a 29. cikk szerinti munkacsoport iránymutatást fogadott el az EUB ítéletének végrehajtására.[575] Az iránymutatás tartalmaz egy listát azon közös kritériumokról, amelyeket a felügyeleti hatóságoknak az egyének adattörlés iránti kérelmeihez kapcsolódó panaszainak kezelése során kell alkalmazniuk, és elmagyarázza, hogy mivel jár a törléshez való jog, továbbá iránymutatást ad a jogok közötti megfelelő egyensúly kialakításához. Az iránymutatás ismételten rámutatott arra, hogy a vizsgálatot eseti alapon kell elvégezni. Mivel az elfeledtetéshez való jog nem abszolút, egy ilyen kérés kimenete függhet az adott eset körülményeitől. Ezt szemlélteti az EUB ítélkezési gyakorlata is a Google után.

Példa: A *Camera di Commercio di Lecce kontra Manni* ügyben[576] az EUB-nek azt kellett megvizsgálnia, hogy az egyén jogában áll-e személyes adatainak nyilvános cégjegyzékből való törlését kérni, miután cége megszűnt. Salvatore Manni kérelmezte a leccei kereskedelmi kamaránál adatainak nyilvántartásból való törlését, miután felfedezte, hogy ha a potenciális ügyfelek megnézik a nyilvántartást, azt látják, hogy egykor

575 29. cikk szerinti munkacsoport (2014), *Az EUB „Google Spain and Inc kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González" C-131/12. sz. ügyben hozott ítéletének végrehajtására vonatkozó iránymutatás*, WP 225, Brüsszel, 2014. november 26.

576 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017. március 9.

egy olyan vállalatnak az ügyvezetője volt, amely több mint egy évtizeddel korábban csődbe ment. A felperes úgy vélte, hogy ez az információ elriasztja a potenciális ügyfeleket.

S. Manni személyes adatainak védelméhez való jogának és a nyilvánosság információhoz való hozzáféréshez fűződő érdekeinek mérlegelése során az EUB először a nyilvános cégjegyzék célját vizsgálta meg. Rámutatott arra, hogy a közhitelű cégnyilvántartások nyilvánosságra hozatalát törvény, és különösen egy a vállalati információk harmadik felek általi hozzáférésének megkönnyítésére irányuló uniós irányelv írja elő. Ezért hozzáférést kell biztosítani harmadik felek számára valamely vállalat alapvető dokumentumaihoz és a vállalatra vonatkozó egyéb információkhoz „különösen a társaság nevében történő kötelezettségvállalásra feljogosított személyek adatait illetően". A közzététel célja – tekintettel a tagállamok közötti intenzív kereskedelemre – volt a jogbiztonság garantálása is, annak biztosításával, hogy harmadik felek hozzáférhessenek a vállalatok valamennyi lényeges információjához az egész Unióban.

Az EUB továbbá megjegyezte, hogy még az idő múlásával, és a vállalat megszűnésével is gyakran fennmaradnak a vállalathoz kapcsolódó jogok és kötelezettségek. A feloszlásra vonatkozó viták hosszasak lehetnek, és a vállalattal, vezetőivel, valamint felszámolóival kapcsolatos kérdések még évekkel a vállalat megszűnése után is felmerülhetnek. Az EUB azt állapította meg, hogy figyelemmel a lehetséges helyzetek nagy számára, és az egyes tagállamokban előírt eltérő elévülési időkre, „a jelen helyzetben lehetetlennek tűnik a társaságok megszűnésétől számított olyan egységes időszak meghatározása, amelynek az elteltével az említett adatoknak a nyilvántartásba történő bejegyzése és az azokat érintő adatszolgáltatás többé nem szükséges". A közzététel törvényes célja és amiatt, hogy nehéz megállapítani azon időszak hosszát, amely végén a személyes adatok anélkül törölhetők a nyilvántartásból, hogy az sértené harmadik felek érdekeit, az EUB megállapította, hogy az uniós adatvédelmi szabályok nem garantálják az egyének személyes adatok törléséhez való jogát S. Manni helyzetében.

Azokban az esetekben, amikor az adatkezelő hozta nyilvánosságra a személyes adatokat és azokat törölnie kell, az adatkezelő köteles minden „észszerű" lépést megtenni, hogy értesítse az azonos adatokat kezelő többi adatkezelőt arról, hogy

az érintett az adatok törlését kérte. Az adatkezelő tevékenységének figyelembe kell vennie a rendelkezésre álló technológiákat és a végrehajtás költségeit.[577]

6.1.4 Az adatkezelés korlátozásához való jog

Az általános adatvédelmi rendelet 18. cikke felhatalmazza az érintetteket arra, hogy átmenetileg korlátozzák az adatkezelőt személyes adataik kezelése tekintetében. Az érintettek az alábbi esetekben kérhetik, hogy az adatkezelő korlátozza az adatkezelést:

- ha vitatják a személyes adatok pontosságát;
- az adatkezelés jogellenes, és az érintett kéri, hogy az adatok törlése helyett korlátozzák azok felhasználását;
- az adatokat jogi igények előterjesztéséhez, érvényesítéséhez vagy védelméhez kell megtartani;
- függőben van egy arra vonatkozó határozat, hogy az adatkezelő jogos indokai elsőbbséget élveznek-e az érintett jogos indokaival szemben.[578]

A személyes adatok kezelésének korlátozására alkalmazott módszerek közé tartozhat többek között a kiválasztott személyes adatoknak egy másik adatkezelő rendszerbe történő ideiglenes áthelyezése vagy a felhasználók számára való hozzáférhetőségük megszüntetése, vagy egy honlapról az ott közzétett adatok ideiglenes eltávolítása.[579] Az adatkezelőnek tájékoztatnia kell az érintettet, mielőtt az adatkezelés korlátozását feloldja.[580]

Értesítési kötelezettség a személyes adatok helyesbítése vagy törlése, illetve az adatkezelés korlátozása tekintetében

Az adatkezelő köteles tájékoztatni minden olyan címzettet a személyes adatok valamennyi helyesbítéséről vagy törléséről, akivel, illetve amellyel a személyes adatot közölték, kivéve, ha ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést

577 Általános adatvédelmi rendelet, 17. cikk (2) bekezdés és (66) preambulumbekezdés.

578 *Uo.*, 18. cikk (1) bekezdés.

579 *Uo.*, (67) preambulumbekezdés.

580 *Uo.*, 18. cikk (3) bekezdés.

igényel.[581] Ha az érintett tájékoztatást kér e címzettekről, az adatkezelő köteles megadni ezt a tájékoztatást.[582]

6.1.5 Az adathordozhatósághoz való jog

Az általános adatvédelmi rendelet értelmében az érintettet megilleti az adathordozhatósághoz való jog azokban az esetekben, amikor valamely adatkezelő rendelkezésére bocsátott személyes adatokat automatizált módon, hozzájárulás alapján kezelik, vagy amikor a személyes adatok kezelése egy szerződés teljesítéséhez szükséges és automatizált módon történik. Ez azt jelenti, hogy az adathordozhatósághoz való jog nem vonatkozik azon helyzetekre, amikor az adatkezelés jogalapja a hozzájárulástól vagy szerződéstől eltérő egyéb jogalap.[583]

Amennyiben vonatkozik az adathordozhatósághoz való jog, az érintettek jogosultak arra, hogy személyes adataikat az adatkezelők egymás között közvetlenül továbbítsák, ha ez technikailag megvalósítható.[584] Ennek megkönnyítése érdekében az adatkezelőnek az adathordozhatóságot lehetővé tevő interoperábilis formátumokat kell kifejlesztenie.[585] Az általános adatvédelmi rendelet előírja, hogy az adatoknak tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban kell lenniük.[586] Az interoperabilitás tág értelemben úgy határozható meg, mint az információs rendszerek azon képessége, hogy egymással adatokat cseréljenek és információt osszanak meg.[587] Noha a használt formátumok célja az interoperabilitás elérése, az általános adatvédelmi rendelet nem tesz ajánlást a konkrét formátumra vonatkozóan: a formátumok ágazatonként eltérőek lehetnek.[588]

A 29. cikk szerinti munkacsoport iránymutatása alapján az adathordozhatósághoz való jog „támogatja a felhasználó választását, rendelkezését és tudatos magatartását”, és célja, hogy az érintettek számára biztosítsa saját személyes adataik feletti

581 *Uo.*, 19. cikk.

582 *Uo.*

583 *Uo.*, (68) preambulumbekezdés és 20. cikk (1) bekezdés.

584 *Uo.*, 20. cikk (2) bekezdés.

585 *Uo.*, (68) preambulumbekezdés és 20. cikk (1) bekezdés.

586 *Uo.*, (68) preambulumbekezdés.

587 Európai Bizottság, Közlemény a határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerekről, COM(2016) 205 final, 2016. április 2.

588 29. cikk szerinti munkacsoport (2016), *Iránymutatás az adatok hordozhatóságáról*, WP 242, 2016. december 13., felülvizsgálva 2017. április 5-én, 13. o.

ellenőrzést.[589] Az iránymutatás tisztázza az adathordozhatóság fő elemeit, amelyek a következők:

- az érintett joga arra, hogy a rá vonatkozó, az adatkezelő által kezelt személyes adatokat tagolt, széles körben használt, géppel olvasható és interoperábilis formátumban megkapja;
- jog arra, hogy – ha ez technikailag megvalósítható – a személyes adatokat az adatkezelők egymás között – akadályoztatás nélkül – közvetlenül továbbítsák;
- ellenőrzés rendszere – ha az adatkezelő válaszol az adathordozhatósági kérelemre, az érintett utasításai szerint kell eljárnia, ami azt jelenti, hogy nem felelős a címzett adatvédelmi törvénynek való megfelelőségéért, figyelemmel arra, hogy az érintett dönti el, hogy kinek továbbítsa az adatokat;
- az adathordozhatósághoz való jog gyakorlása – csakúgy, mint az általános adatvédelmi rendeletben biztosított egyéb jogok esetében – nem sérthet bármely más jogot.

6.1.6 A tiltakozáshoz való jog

Az érintett jogosult arra, hogy a saját helyzetével kapcsolatos okokból tiltakozzon személyes adatainak kezelése ellen, illetve tiltakozzon adatainak közvetlen üzletszerzési célú kezelése ellen. A tiltakozáshoz való jog automatizált eszközökkel is gyakorolható.

Tiltakozáshoz való jog az érintett konkrét helyzete alapján

Az érintettet megilleti annak általános joga, hogy tiltakozzon adatainak kezelése ellen.[590] Az általános adatvédelmi rendelet 21. cikkének (1) bekezdése felhatalmazza az érintettet, hogy a saját helyzetével kapcsolatos okokból tiltakozzon személyes adatainak kezelése ellen, ha az adatkezelés jogalapja az adatkezelő közérdekű feladatának végrehajtása, vagy ha az adatkezelés az adatkezelő jogos érdekén

589 *Uo.*

590 Lásd még: EJEB, *M.S. kontra Svédország*, 20837/92. sz. ügy, 1997. augusztus 27. (orvosi adatokat közöltek hozzájárulás vagy a tiltakozáshoz való jog biztosítása nélkül); EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987. március 26.; EJEB, *Mosley kontra Egyesült Királyság*, 48009/08. sz. ügy, 2011. május 10.

alapul.[591] A tiltakozáshoz való jog a profilalkotási tevékenységekre is vonatkozik. Egy hasonló jogot a Korszerűsített 108. Egyezmény is elismer.[592]

Az érintettet konkrét helyzete alapján megillető tiltakozási jog célja, hogy megfelelő egyensúlyt teremtsen az érintett adatvédelemhez való joga és másoknak az érintett adatai kezeléséhez fűződő jogos érdekei között. Az EUB tisztázta, hogy az érintett jogai „főszabályként" megelőzik az adatkezelő gazdasági érdekeit „a kérdéses információ jellegétől, illetve attól is függően, hogy az információ mennyire érzékeny az érintett személy magánélete szempontjából, illetve hogy a nyilvánosságnak milyen érdeke fűződik ezen információ megszerzéséhez".[593] Az általános adatvédelmi rendelet értelmében a bizonyítási teher az adatkezelőket terheli, akiknek az adatkezelés folytatását indokoló kényszerítő okokat kell felmutatniuk.[594] Ehhez hasonlóan a Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés tisztázza, hogy az adatkezelés jogszerű okát (amely elsőbbséget élvezhet az érintett tiltakozáshoz való jogával szemben) eseti alapon kell igazolni.[595]

Példa: A *Manni* ügyben[596] az EUB megállapította, hogy a személyes adatok cégnyilvántartásban való közzététel törvényes célja és különösen a harmadik személyek érdekei védelmének és jogbiztonság biztosításának szükségessége miatt elvben S. Manni nem jogosult személyes adatainak cégnyilvántartásból való törlését kérni. Elismerte azonban az adatkezelés elleni tiltakozás jogának meglétét leszögezve, hogy „nem zárható ki, [...] hogy felmerülhetnek olyan különös helyzetek, amelyekben az érintett személy sajátos helyzetével kapcsolatos lényeges, jogos érdekek kivételesen igazolják, hogy a rá vonatkozó, a nyilvántartásba bejegyzett személyes adatokhoz való hozzáférést [...] kellően hosszú időszak elteltével az adatokba való betekintéshez fűződő különös érdeküket igazoló harmadik személyekre korlátozzák".

591 Általános adatvédelmi rendelet, (69) preambulumbekezdés, 6. cikk (1) bekezdés e) és f) pont.

592 Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés d) pont; a profilalkotásra vonatkozó ajánlás, 5. cikk (3) bekezdés.

593 EUB, *Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González* [nagytanács], C-131/12. sz. ügy, 2014. május 13.

594 Lásd még a Korszerűsített 108. Egyezmény 9. cikke (1) bekezdésének d) pontját, amely kimondja, hogy az érintett tiltakozhat adatainak kezelése ellen „kivéve, ha az adatkezelő bizonyítja, hogy az adatkezelést olyan jogos okok indokolják, amelyek elsőbbséget élveznek az érintett érdekeivel, jogaival és szabadságaival szemben".

595 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 78. pont.

596 EUB, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni*, C-398/15. sz. ügy, 2017. március 9., 47. és 60. pont.

Az EUB úgy vélte, hogy a nemzeti bíróságok feladata megvizsgálni az egyes eseteket, figyelemmel az egyén valamennyi lényeges körülményére és arra, hogy léteznek-e olyan jogos és kényszerítő okok, amelyek kivételesen igazolhatják harmadik feleknek a cégnyilvántartásokban szereplő személyes adatokhoz való hozzáférésének korlátozását. Tisztázta ugyanakkor, hogy Manni esetében kizárólag azon körülmény, miszerint potenciális ügyfélkörét állítólag befolyásolta személyes adatainak cégnyilvántartásban való közzététele, nem minősül ilyen jogos és kényszerítő oknak. Manni potenciális ügyfeleinek jogos érdeke fűződik a régi vállalkozásának csődjére vonatkozó információkat megismerni.

Az eredményes tiltakozás hatása az, hogy az adatkezelő a jövőben nem kezelheti a kérdéses adatokat. Az érintett adatain a tiltakozás előtt végzett feldolgozási műveletek azonban továbbra is jogszerűek.

Tiltakozáshoz való jog a közvetlen üzletszerzési célú adatkezelés ellen

Az általános adatvédelmi rendelet 21. cikkének (2) bekezdése konkrét tiltakozási jogot biztosít a személyes adatok közvetlen üzletszerzés céljából történő kezelése ellen, amit az elektronikus hírközlési adatvédelmi irányelv 13. cikke részletesebben tisztáz. Egy ilyen jogot a Korszerűsített 108. Egyezmény, valamint az Európa Tanács közvetlen üzletszerzésre vonatkozó ajánlása is biztosít.[597] A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés tisztázza, hogy a személyes adatok közvetlen üzletszerzési célú kezelése elleni tiltakozásnak a szóban forgó személyes adatok feltétlen törlését vagy eltávolítását kell eredményeznie.[598]

Az érintett jogosult arra, hogy bármikor és térítésmentesen tiltakozzon személyes adatainak közvetlen üzletszerzés érdekében történő kezelése ellen. Az érintetteket erről a jogukról egyértelműen és minden más információtól elkülönítve kell tájékoztatni.

597 Európa Tanács, Miniszteri Bizottság (1985), (85)20. sz. ajánlás a tagállamok részére a közvetlen üzletszerzési célokra felhasznált személyes adatok védelméről, 1985. október 25., 4. cikk, (1) bekezdés.

598 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 79. pont.

Tiltakozáshoz való jog az automatizált eszközökkel kapcsolatban

Amennyiben a személyes adatok felhasználása és kezelése információs társadalommal összefüggő szolgáltatások céljából történik, az érintett gyakorolhatja személyes adatainak automatizált eszközökkel való kezelése elleni tiltakozáshoz való jogát.

Az információs társadalommal összefüggő szolgáltatások általában térítés ellenében, távolról, elektronikus úton és a szolgáltatást igénybe vevő egyéni kérelmére nyújtott szolgáltatások.[599]

Az információs társadalommal összefüggő szolgáltatásokat nyújtó adatkezelőknek megfelelő műszaki előírásokat és eljárásokat kell biztosítaniuk az automatizált eszközökkel kapcsolatos tiltakozáshoz való jog hatékony gyakorlása érdekében.[600] Ez lehet például a sütik letiltása a weboldalakon, vagy az internetes böngészés nyomon követésének leállítása.

Tiltakozáshoz való jog tudományos vagy történelmi kutatási vagy statisztikai célú adatkezelés ellen

Az uniós jog értelmében a személyes adatok tudományos kutatási célú kezelését tág körűen kell értelmezni, oly módon, hogy az magában foglalja többek között a technológiafejlesztési és demonstrációs tevékenységeket, az alapkutatást, az alkalmazott kutatást, és a magánfinanszírozású kutatást.[601] A történelmi kutatás magában foglalja a genealógiai célú kutatást is, szem előtt tartva, hogy a rendelet elhunyt személyre nem alkalmazandó.[602] A statisztikai célú adatkezelésnek minősül a személyes adatok statisztikai felmérések vagy statisztikai eredmények kiszámításának céljából történő gyűjtése és kezelése.[603] A kutatási célból végzett adatkezelés esetén is az érintett konkrét helyzete képezi az adatkezelés elleni tiltakozás jogalapját.[604] Az egyetlen kivételt az jelenti, ha az adatkezelésre közérdekű okból végzett feladat végrehajtása érdekében van szükség. A törléshez való jog azonban

599 A 98/48/EK irányelvvel módosított, a műszaki szabványok és szabályok terén történő információszolgáltatási eljárás megállapításáról szóló 98/34/EK irányelv, 1. cikk (2) bekezdés.

600 Általános adatvédelmi rendelet, 21. cikk (5) bekezdés.

601 *Uo.*, (159) preambulumbekezdés.

602 *Uo.*, (160) preambulumbekezdés.

603 *Uo.*, (162) preambulumbekezdés.

604 *Uo.*, 21. cikk (6) bekezdés.

nem érvényes akkor, ha az adatkezelés tudományos vagy történelmi kutatási célból vagy statisztikai célból szükséges (közérdekű okból vagy anélkül).[605]

Az általános adatvédelmi rendelet a 89. cikkben garanciák és eltérések biztosításával egyensúlyt teremt a tudományos, statisztikai vagy történelmi kutatási célból történő adatkezelés követelménye és az érintettek jogai között. Így tehát az uniós vagy tagállami jog biztosíthat eltéréseket a tiltakozáshoz való jog tekintetében, amennyiben e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják a kutatási célok elérését, és az adott célok megvalósításához szükség van ilyen eltérésre.

Az **Európa Tanács jogában** a Korszerűsített 108. Egyezmény 9. cikkének (2) bekezdése megállapítja, hogy az érintettek jogaira – beleértve a tiltakozáshoz való jogot is – jogszabályban korlátozásokat lehet megállapítani a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történő adatkezelés vonatkozásában, amennyiben az érintettek jogai és alapvető szabadságai megsértésének kockázata nem áll felismerhetően fenn.

A Magyarázó Jelentés (41. bekezdés) ugyanakkor elismeri, hogy az érintettek számára biztosítani kell annak lehetőségét, hogy hozzájárulásukat csak a kutatás egyes területei vonatkozásában, vagy a kutatási projektek egyes részeire adják meg, amennyiben a tervezett adatkezelési cél ezt lehetővé teszi, és hogy tiltakozzanak az adatkezelés ellen, ha azt észlelik, hogy az – jogos ok nélkül – túlzottan beavatkozik a jogaikba és szabadságaikba.

Más szavakkal, az ilyen adatkezelés eleve összeegyeztethetőnek minősülne, feltéve, hogy léteznek egyéb garanciákés, hogy az adatkezelési műveletek elvben kizárják a megszerzett adatoknak az adott egyént érintő döntések vagy intézkedések céljából történő felhasználását.

6.1.7 Automatizált döntéshozatal, ideértve a profilalkotást is

Az automatizált döntések olyan döntések, amelyeket kizárólag automatizált módon, emberi beavatkozás nélkül kezelt személyes adatok felhasználásával hoznak. **Az uniós jog értelmében** az érintett jogosult arra, hogy ne terjedjen ki rá olyan

605 *Uo.*, 17. cikk (3) bekezdés d) pont.

automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti. Ha az ilyen döntés valószínűleg jelentős mértékben érintené az egyének életét, mivel az például hitelképességgel, online toborzással, munkahelyi teljesítménnyel, a magatartás vagy megbízhatóság elemzésével kapcsolatos, a nem kívánatos következmények elkerülése érdekében különleges védelemre van szükség. Az automatizált döntéshozatal magában foglalja a profilalkotást is, amely a „természetes személyekre vonatkozó személyes jellemzők bármilyen automatizált személyes adatok kezelése keretében történő kiértékelése, különösen az érintett munkahelyi teljesítményére, anyagi helyzetére, egészségi állapotára, személyes preferenciáira vagy érdeklődési körökre, megbízhatóságra vagy viselkedésre, tartózkodási helyére vagy helyváltoztatásai elemzésére és előrejelzésére”.[606]

Példa: Egy jövőbeli ügyfél hitelképességének gyors felméréséhez a hitelreferencia ügynökségek (CRA) meghatározott adatokat gyűjtenek arra vonatkozóan, hogy az ügyfél miként vezette hitel- és szolgáltatási-/közműszámláit, valamint az ügyfél előző lakcímeire vonatkozó adatokat, valamint nyilvános forrásokból származó információkat, mint amilyen például a választói névjegyzék, nyilvános nyilvántartások (beleértve a bírósági ítéleteket is), továbbá a csődeljárásra, illetve fizetésképtelenségre vonatkozó adatokat. Ezeket a személyes adatokat ezután beviszik egy minősítő algoritmussal működő rendszerbe, amely kiszámítja a potenciális ügyfél hitelképességét jelző összesített értéket.

A 29. cikk szerinti munkacsoport szerint az érintettnek azon joga, hogy ne terjedjen ki rá olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással jár vagy őt hasonlóan jelentős mértékben érinti, egy általános tilalomnak felel meg, és az érintettnek nem szükséges proaktívan tiltakozni egy ilyen döntés ellen.[607]

Mindazonáltal az általános adatvédelmi rendelet alapján a joghatással járó vagy az egyént jelentős mértékben érintő automatizált döntéshozatal elfogadható, ha az szükséges egy szerződés megkötéséhez vagy az adatkezelő és az érintett között létrejött szerződés teljesítéséhez, vagy ha az érintett kifejezetten hozzájárult

606 *Uo.*, (71) preambulumbekezdés, 4. cikk 4. pont és 22. cikk.

607 29. cikk szerinti munkacsoport, *Iránymutatás a 2016/679 rendelet alkalmazásában történő automatizált egyedi döntéshozatalhoz és a profilalkotáshoz*, WP 251, 2017. október 3., 15. o.

ahhoz. Az automatizált döntéshozatal továbbá elfogadható, ha azt törvény engedélyezi, és ha az érintett jogai, szabadságai és jogos érdekei megfelelő védelemben részesülnek.[608]

Az általános adatvédelmi rendelet az adatkezelőnek a személyes adatok gyűjtésekor adandó tájékoztatásra vonatkozó kötelezettségei között rendelkezik arról, hogy az érintetteket tájékoztatni kell az automatizált döntéshozatal tényéről, ideértve a profilalkotást is.[609] Az adatkezelő által kezelt személyes adatokhoz való hozzáférés jogát ez nem befolyásolja.[610] A tájékoztatásnak nemcsak a profilalkotás tényére kell kitérnie, hanem érthető információkat kell biztosítani az alkalmazott logikára és arra vonatkozóan, hogy az ilyen adatkezelés az érintettre nézve milyen várható következményekkel jár.[611] A kérelmekre automatizált döntéshozatalt alkalmazó egészségbiztosító társaságnak például általános tájékoztatást kell adnia az érintetteknek az algoritmus működésére, továbbá arra vonatkozóan, hogy az algoritmus mely tényezőit használja a biztosítási díj kiszámításához. Hasonlóan, a „hozzáférési jog" gyakorlása során az érintettek tájékoztatást kérhetnek az adatkezelőtől az automatizált döntéshozatal tényére és az alkalmazott logikára vonatkozóan.[612]

Az érintetteknek adott tájékoztatás célja, hogy biztosítsa az átláthatóságot, és lehetővé tegye az érintettek számára a tájékoztatáson alapuló hozzájárulás megadását, ha erről van szó, vagy, hogy emberi beavatkozást kérjenek. Az adatkezelő köteles megfelelő intézkedéseket tenni az érintett jogainak, szabadságainak és jogos érdekeinek védelmére. Ez magában foglalja az érintettnek legalább azt a jogát, hogy az adatkezelő részéről emberi beavatkozást kérjen, álláspontját kifejezhesse, és a személyes adatainak automatizált kezelésén alapuló döntéssel szemben kifogást nyújtson be.[613]

A 29. cikk szerinti munkacsoport további iránymutatást dolgozott ki az automatizált döntéshozatal általános adatvédelmi rendelet szerinti alkalmazására vonatkozóan.[614]

608 Általános adatvédelmi rendelet, 22. cikk (2) bekezdés.

609 *Uo.*, 12. cikk.

610 *Uo.*, 15. cikk.

611 *Uo.*, 13. cikk (2) bekezdés f) pont.

612 *Uo.*, 15. cikk (1) bekezdés h) pont.

613 *Uo.*, 22. cikk (3) bekezdés.

614 29. cikk szerinti munkacsoport, *Iránymutatás a 2016/679 rendelet alkalmazásában történő automatizált egyedi döntéshozatalhoz és a profilalkotáshoz*, WP 251, 2017. október 3.

Az Európa Tanács joga szerint az egyén jogosult mentesülni az olyan döntések hatálya alól, amelyek jelentős mértékben érintik őt, és amely véleménye figyelembe vétele nélkül kizárólag automatizált adatkezelésen alapul.[615] Az a követelmény, hogy figyelembe vegyék az érintett véleményét, amikor a döntéseket kizárólag automatizált adatkezelés alapján hozzák, azt jelenti, hogy jogosultak legyenek megtámadni az ilyen döntéseket, és képesnek kell lenniük vitatni az adatkezelő által használt adatok pontosságát, valamint a rájuk alkalmazott profil relevanciáját.[616] Az egyén azonban nem gyakorolhatja ezt a jogát, ha az automatizált döntéshozatalt az adatkezelőre vonatkozó olyan jogszabály teszi lehetővé, amely megfelelő intézkedéseket is meghatároz az érintett jogainak, szabadságainak és jogos érdekeinek védelme érdekében. Ezenkívül az érintett jogosult kérésre tájékoztatást kapni az elvégzett adatkezelés alapjául szolgáló indokról.[617] A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés példákat hoz a pontozásos hitelbírálatra. Az egyénnek jogában áll tudni nem csak magát a pozitív vagy negatív pontozásos döntést, hanem személyes adatai kezelését alátámasztó és az adott döntést eredményező *logikát* is. „Ezen elemek megértése elősegíti a többi alapvető biztosítékok, például a tiltakozáshoz való jog és a felügyeleti hatósághoz címzett panasz benyújtása jogának hatékony gyakorlását".[618]

A profilalkotásra vonatkozó ajánlás, noha jogilag nem kötelező, meghatározza a személyes adatok gyűjtésének és kezelésének feltételeit a profilalkotással összefüggésben.[619] Rendelkezéseket tartalmaz arra vonatkozóan, hogy biztosítani szükséges, hogy a profilalkotással összefüggésben végzett adatkezelés tisztességes, jogszerű, arányos legyen, valamint meghatározott és törvényes célból történjen. Tartalmaz továbbá rendelkezéseket az adatkezelők által az érintettek számára nyújtandó tájékoztatásra vonatkozóan. Az adatminőség elve – amely megköveteli, hogy az adatkezelők tegyenek intézkedéseket a profilalkotással járó adatpontatlansági tényezők kijavítására, a kockázatok, illetve hibák korlátozására, és időszakosan értékeljék az adatok és az alkalmazott algoritmusok minőségét – szintén megjelenik az ajánlásban.

615 Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés a) pont.

616 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 75. pont.

617 Korszerűsített 108. Egyezmény, 9. cikk (1) bekezdés c) pont.

618 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 77. pont.

619 Európa Tanács, Miniszteri Bizottság, CM/Rec(2010)13. sz. ajánlás a tagállamok részére az egyéneknek a profilalkotás összefüggésében a személyes adatok automatikus feldolgozásával kapcsolatos védelméről, 5. cikk (5) bekezdés.

6.2 Jogorvoslat, felelősség, szankciók és kártérítés

Főbb pontok

- A Korszerűsített 108. Egyezmény szerint a részes felek nemzeti jogának megfelelő jogorvoslatokat és szankciókat kell megállapítania az adatvédelemhez való jog megsértése esetére.
- Az EU-ban az általános adatvédelmi rendelet rendelkezik az érintettek jogorvoslati lehetőségeiről jogaik megsértése esetén, ahogy a rendelet előírásait be nem tartó adatkezelőkkel és adatfeldolgozókkal szembeni szankciókról is. Rendelkezik továbbá a kártérítéshez való jogról és a felelősségről.
  - Az érintett jogosult panaszt benyújtani a felügyeleti hatóságnál a rendelet feltételezett megsértése miatt, valamint az érintettet megilleti a hatékony bírósági jogorvoslathoz és kártérítéshez való jog.
  - A hatékony jogorvoslathoz való jog gyakorlása során az egyént képviselheti az adatvédelem terén tevékenységet folytató nonprofit szervezet.
  - Az adatkezelő vagy adatfeldolgozó felelősséggel tartozik minden olyan vagyoni vagy nem vagyoni kárért, amelyet a rendeletet sértő adatkezelés okozott.
  - A felügyeleti hatóságok legfeljebb 20 000 000 euró összegű közigazgatási bírságot, illetve vállalkozások esetében az előző pénzügyi év teljes éves világpiaci forgalmának legfeljebb 4%-át kitevő összeget szabhatnak ki attól függően, hogy melyik érték magasabb.
- Az érintettek – végső megoldásként, bizonyos körülmények között – az adatvédelmi jogsértéseket az EJEB elé vihetik.
- Minden természetes vagy jogi személy jogosult az Európai Adatvédelmi Testület határozatának érvénytelenítésére irányuló eljárást kezdeményezni az EUB előtt a Szerződésekben meghatározott feltételek mellett.

A személyes adatok Európán belüli védelmének biztosításához nem elegendő jogi eszközöket elfogadni. Ahhoz, hogy az európai adatvédelmi szabályok hatékonyak legyenek, fontos olyan mechanizmusokat kidolgozni, amelyek lehetővé teszik az egyének számára, hogy fellépjenek a jogaik megsértése ellen, és kártérítést követeljenek az elszenvedett kárért. Az is fontos, hogy a felügyeleti hatóságok rendelkezzenek hatáskörrel hatékony, visszatartó erejű és a szóban forgó szabályszegéssel arányos szankciókat kiszabni.

Az adatvédelmi törvény által biztosított jogokat az a személy gyakorolhatja, akinek a jogai veszélyben forognak, tehát maga az érintett. Jogai gyakorlásában azonban – a nemzeti jog követelményeinek megfelelő – más személyek is képviselhetik az érintettet. Számos nemzeti jogszabály értelmében a gyermekeket és a szellemi fogyatékkal élőket gyámjuknak kell képviselnie.[620] Az uniós adatvédelmi jog alapján egy egyesület – amelynek törvényes célja az adatvédelmi jogok előmozdítása – képviselheti az érintetteket a felügyeleti hatóság vagy a bíróság előtt.[621]

6.2.1 A felügyeleti hatósághoz címzett panasz benyújtásának joga

Mind az **Európa Tanács**, mind pedig az **EU joga** alapján az egyének jogosultak kérelmeket és panaszokat benyújtani az illetékes felügyeleti hatóságnak, ha úgy vélik, hogy személyes adataik kezelése nem a törvény előírásainak megfelelően történt.

A Korszerűsített 108. Egyezmény elismeri az érintettek azon jogát, hogy igénybe vegyék a felügyeleti hatóság segítségét az egyezményben biztosított jogaik gyakorlása során, állampolgárságuktól vagy lakóhelyüktől függetlenül.[622] A segítségnyújtás iránti kérelem csak kivételes körülmények között utasítható vissza, és nem számolható fel díj, illetve költség az érintettek számára a segítségnyújtással kapcsolatban.[623]

Hasonló rendelkezések megtalálhatók az EU jogrendszerében is. Az általános adatvédelmi rendelet előírja, hogy a felügyeleti hatóságok fogadjanak el a panaszok benyújtását megkönnyítő intézkedéseket, például hozzanak létre elektronikus úton is kitölthető panasz benyújtására szolgáló formanyomtatványt.[624] Az érintett panaszt nyújthat be a felügyeleti hatóságnál a tartózkodási helye, a munkahelye vagy a feltételezett jogsértés helye szerinti tagállamban.[625] A panaszokat ki kell vizs-

620 FRA (2015), *Kézikönyv a gyermekjogokra vonatkozó európai jogról*, Luxembourg, Kiadóhivatal; FRA (2013), *A mentális problémákkal küzdő és a korlátozott értelmi képességű személyek alapjogai*, Luxembourg, Kiadóhivatal.

621 Általános adatvédelmi rendelet, 80. cikk.

622 Korszerűsített 108. Egyezmény, 18. cikk.

623 *Uo.*, 16–17. cikk.

624 Általános adatvédelmi rendelet, 57. cikk (2) bekezdés.

625 *Uo.*, 77. cikk (1) bekezdés.

gálni, és a felügyeleti hatóság köteles tájékoztatni az érintettet a panaszával foglalkozó eljárás eredményéről.[626]

Az uniós intézmények vagy szervek feltételezett szabálysértése az európai adatvédelmi biztos figyelmébe ajánlható.[627] Amennyiben az európai adatvédelmi biztos hat hónapon belül nem válaszol, a panaszt elutasítottnak kell tekinteni. Az európai adatvédelmi biztos határozata ellen fellebbezés az EUB-hez nyújtható be a 45/2001 rendelet keretében, amely kötelezettséget ír elő az uniós intézmények és szervek számára az adatvédelmi szabályok betartására.

Biztosítani kell annak lehetőségét, hogy valamely nemzeti felügyeleti hatóság határozatait bíróság előtt meg lehessen támadni. Ez azon érintettekre, valamint az adatkezelőkre és adatfeldolgozókra egyaránt vonatkozik, akik a felügyeleti hatóság előtt lefolytatott eljárásban félként vettek részt.

Példa: 2017 szeptemberében a spanyol adatvédelmi hatóság megbírságolta a Facebookot több adatvédelmi rendelkezés megsértése miatt. A felügyeleti hatóság elmarasztalta a közösségi hálózatot a személyes adatok – beleértve a személyes adatok különleges kategóriáit is – reklámcélból és az érintettek hozzájárulásának beszerzése nélkül történő gyűjtéséért, tárolásáért és kezeléséért. A határozat alapját a felügyeleti hatóság saját kezdeményezésére indított vizsgálata képezte.

6.2.2 Hatékony bírósági jogorvoslathoz való jog

A felügyeleti hatóságnak címzett panasz benyújtása mellett biztosítani kell az egyénnek számára a jogot a hatékony bírósági jogorvoslathoz és ahhoz, hogy ügyüket bíróság el vihessék. A jogorvoslathoz való jog az európai jogi tradícióba mélyen beágyazott jog, és az EU alapjogi Chartájának 47. cikke, valamint az EJEE 13. cikke egyaránt alapjogként ismeri el.[628]

626 *Uo.*, 77. cikk (2) bekezdés.

627 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

628 Lásd például: EJEB, *Karabeyoğlu kontra Törökország*, 30083/10. sz. ügy, 2016. június 7.; EJEB, *Mustafa Sezgin Tanrıkulu kontra Törökország*, 27473/06. sz. ügy, 2017. július 18.

Az **uniós jog alapján** az általános adatvédelmi rendelet rendelkezéseiből – amely megállapítja a hatékony bírósági jogorvoslathoz való jogot a felügyeleti hatóságokkal, adatkezelőkkel és adatfeldolgozókkal szemben – és az EUB ítélkezési gyakorlatából egyaránt egyértelmű, hogy mennyire fontos biztosítani az érintettek számára a hatékony jogorvoslathoz való jogot jogaik megsértése esetén.

Példa: A *Schrems* ügyben[629] az EUB érvénytelennek nyilvánította a biztonságos kikötőre vonatkozó megfelelőségi határozatot. Ez a határozat lehetővé tette a személyes adatok nemzetközi továbbítását az EU-ból olyan egyesült államokbeli szervezeteknek, amelyek a biztonságos kikötő megállapodás keretében önmaguk tanúsították a megfelelést. Az EUB azt állapította meg, hogy a biztonságos kikötő megállapodásnak számos hiányossága van, amelyek veszélyeztetik az uniós polgárok magánélet védelméhez, személyes adatok védelméhez és hatékony jogorvoslathoz való alapjogait.

A magánélethez és adatvédelemhez való jog megsértését illetően az EUB kiemelte, hogy az egyesült államokbeli szabályozás lehetővé tette egyes hatóságok számára, hogy hozzáférjenek a tagállamokból az Egyesült Államokba továbbított személyes adatokhoz, és azokat az adattovábbítás eredeti céljával össze nem egyeztethető módon, valamint a nemzetbiztonság védelméhez feltétlenül szükséges és azzal arányos mértéket meghaladóan kezeljék. A hatékony jogorvoslathoz való joggal kapcsolatban megállapította, hogy az érintett személyeknek nem volt olyan közigazgatási, illetve bírósági jogorvoslati lehetőségük, amely lehetővé tette volna, hogy hozzáférjenek a rájuk vonatkozó adatokhoz, és azokat adott esetben helyesbíttessék, illetve töröltessék. Az EUB azt a következtetést vonta le, hogy az olyan szabályozás, amely nem biztosít a jogalany számára semmilyen jogorvoslati lehetőséget abból a célból, hogy a rá vonatkozó személyes adatokhoz hozzáférést kapjon, vagy azokat helyesbíttesse, illetve töröltesse, „nem tartja tiszteletben a hatékony bírói jogvédelemhez való jog lényegét, amelyet a Charta 47. cikke mond ki". Kiemelte, hogy a jogszabályi megfelelőséget garantáló bírósági jogorvoslati lehetőség megléte a jogállamiság szerves részét képezi.

629 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

A felügyeleti hatóság jogilag kötelező érvényű határozatát megtámadni kívánó egyének, adatkezelők vagy adatfeldolgozók bírósági eljárást kezdeményezhetnek.[630] A „döntés" fogalmát tágan kell értelmezni, és ez kiterjed a felügyeleti hatóságok vizsgálati, szankcionálási és engedélyezési hatáskörére, valamint a panaszt elutasító határozatokra. A felügyeleti hatóságok nem kötelező érvényű intézkedései azonban, például a vélemények vagy tanácsok nem képezhetik bírósági eljárás tárgyát.[631] A bírósági eljárást az érintett felügyeleti hatóság székhelye szerinti tagállam bírósága előtt kell megindítani.[632]

Azokban az esetekben, amikor az adatkezelő vagy adatfeldolgozó megsérti az érintett jogait, az érintettek jogosultak keresetet benyújtani a bíróságon.[633] Az adatkezelő vagy adatfeldolgozó ellen indított eljárásoknál különösen fontos biztosítani az érintett számára annak lehetőségét, hogy megválassza, hol indítson eljárást. Ez az adatkezelő vagy az adatfeldolgozó tevékenységi helye szerinti tagállam bírósága előtt vagy az érintett szokásos tartózkodási helye szerinti tagállam bírósága előtt is megteheti.[634] A második lehetőség nagymértékben megkönnyíti az egyének jogainak gyakorlását, mivel lehetővé teszi számukra, hogy abban az országban indítsanak eljárást, ahol laknak és egy számukra ismerős joghatóságban. Az adatkezelőkkel és adatfeldolgozókkal szemben indított eljárások helyének ezek tevékenységi helye szerinti tagállamra korlátozása visszatarthatja az adatkezelőket attól, hogy bírósági eljárást indítsanak, mivel ez utazási és egyéb költségekkel járna, továbbá az eljárás idegen nyelven és idegen joghatóságban zajlana. Ez alól egyedüli kivételt az az eset képez, amikor az adatkezelő vagy adatfeldolgozó valamely tagállamnak a közhatalmi jogkörében eljáró közhatalmi szerve, és az adatkezelésre hatáskörük gyakorlása keretében kerül sor. Ebben az esetben az eljárás tekintetében kizárólag az érintett közhatalmi szerv szerinti állam bíróságai az illetékesek.[635]

Noha legtöbb esetben az adatvédelmi szabályokat érintő ügyekben a tagállamok bíróságai döntenek, néhány eset az EUB elé vihető. Az első lehetőségnél az érintett, adatkezelő, adatfeldolgozó vagy felügyeleti hatóság az Európai Adatvédelmi Testület egy határozata ellen megsemmisítés iránti kérelmet nyújthat be. Az eljárás azonban az EUMSZ 263 cikkben rögzített feltételek hatálya alá tartozik, ami azt

630 Általános adatvédelmi rendelet, 78. cikk.

631 *Uo.*, (143) preambulumbekezdés.

632 *Uo.*, 78. cikk (3) bekezdés.

633 *Uo.*, 79. cikk.

634 *Uo.*, 79. cikk (2) bekezdés.

635 *Uo.*

jelenti, hogy ahhoz, hogy a keresetet elfogadhatónak nyilvánítsák, az egyéneknek és szervezeteknek bizonyítaniuk kell, hogy a Testület határozata közvetlenül és személyükben érinti őket.

A második eset a személyes adatokat jogszerűtlenül kezelő uniós intézményeket és testületeket érinti. Azokban az esetekben, amikor uniós intézmények vagy szervek sértik meg az adatvédelmi törvényt, az érintettek közvetlenül az Európai Unió Törvényszékénél (a Törvényszék az EUB részét képezi) nyújthatnak be keresetet. A Törvényszék első fokon az uniós jog uniós intézmények általi megsértésével foglalkozik. Így tehát az európai adatvédelmi biztos – mint uniós intézmény – ellen a Törvényszéken is benyújtható kereset.[636]

Példa: A *Bavarian Lager* ügyben[637] a társaság kérelemmel fordult az Európai Bizottsághoz, hogy biztosítson számára hozzáférést egy bizottsági ülés teljes jegyzőkönyvéhez, amely állítólag a vállalatra vonatkozó jogi kérdésekkel foglalkozott. Az Bizottság a vállalat hozzáférési kérelmét elsőbbséget élvező adatvédelmi érdekekre hivatkozva elutasította.[638] A Bavarian Lager az uniós intézmények adatvédelmi rendeletének 32. cikke értelmében a határozat ellen eljárást indított az elsőfokú bíróságon (a Törvényszék elődjénél). Az Elsőfokú Bíróság (a T-194/04. sz. *Bavarian Lager Co. Ltd. kontra az Európai Közösségek Bizottsága* ügyben hozott) határozatával megsemmisítette a Bizottságnak a hozzáférési kérelmet elutasító határozatát. Az Európai Bizottság a határozat ellen fellebbezett az EUB-nél.

Az EUB az elsőfokú bíróság ítéletét félretéve (a nagytanácsban) hozott ítéletet, és helyben hagyta az Európai Bizottságnak azon határozatát, amelyben elutasította az ülés teljes jegyzőkönyvéhez való hozzáférésre irányuló kérelmet az ülésen jelenlévők személyes adatainak védelme érdekében. Az EUB úgy vélte, hogy a Bizottság helyesen járt el, amikor elutasította az információk közzétételét, figyelemmel arra, hogy a résztvevők nem adták hozzájárulásukat személyes adataik közléséhez. Ezenkívül a Bavarian Lager nem bizonyította, hogy szükséges hozzáférnie a szóban forgó információkhoz.

636 45/2001/EK rendelet, 32. cikk (3) bekezdés.

637 EUB, *Európai Bizottság kontra The Bavarian Lager Co. Ltd.* [nagytanács], C-28/08. P. sz. ügy, 2010.

638 Az érvelés elemzéséért lásd: EDPS (2011), *Nyilvános hozzáférés személyes adatokat tartalmazó dokumentumokhoz a Bavarian Lager ügyben hozott ítélet után*, Brüsszel, EDPS.

Végezetül az érintettek, a felügyeleti hatóságok, az adatkezelők vagy adatfeldolgozók a belföldi eljárások során kérhetik a nemzeti bíróságot, hogy forduljon pontosításért a Bírósághoz az uniós Szerződések értelmezésével, valamint az uniós intézmények, szervek, hivatalok vagy ügynökségek aktusainak értelmezésével és érvényességével kapcsolatban. Az ilyen pontosítások előzetes döntéshozatal néven ismertek. Az előzetes döntéshozatal nem nyújt közvetlen jogorvoslatot a panaszosnak, lehetővé teszi viszont a nemzeti bíróságok számára, hogy az uniós jog helyes értelmezését alkalmazzák. Az előzetes döntéshozatali mechanizmuson keresztül jutottak el azok a nagy horderejű ügyek – például a *Digital Rights Ireland* és a *Kärntner Landesregierung és társai*[639]*, valamint a Schrems*[640] *–, amelyek nagymértékben befolyásolták az uniós adatvédelmi jog kialakulását.*

Példa: A *Digital Rights Ireland* és *Kärntner Landesregierung és társai*[641] egy egyesített ügy volt, amelyet az ír legfelsőbb bíróság és az osztrák alkotmánybíróság nyújtottak be a 2006/24/EK (adatmegőrzési irányelv) uniós adatvédelmi irányelvnek való megfelelősége vonatkozásában. Az osztrák alkotmánybíróság kérdéseket nyújtott be az EUB-nek a 2006/24/EK irányelv 3. és 9. cikkének érvényességével kapcsolatban, figyelemmel az EU Alapjogi Chartájának 7., 9. és 11. cikkére. Ezek arra vonatkoztak, hogy az adatmegőrzési irányelvet átültető osztrák szövetségi távközlési törvény egyes rendelkezései összeegyeztethetőek-e a korábbi adatvédelmi irányelvvel és az uniós intézmények adatvédelmi rendeletével.

A *Kärntner Landesregierung és társai* ügyben M. Seitlinger – az alkotmánybírósági eljárás egyik felperese – elmondta, hogy ő munkavégzési célból és a magánélete során egyaránt használja a telefont, az internetet és az emailt. Következésképpen az általa küldött és kapott információk a távközlési közszolgáltatási hálózatokon keresztül áramlottak. A 2003. évi osztrák távközlési törvény értelmében M. Seitlinger távközlési szolgáltatóját jogszabály kötelezte arra, hogy a hálózat M. Seitlinger általi használatáról adatokat gyűjtsön és tároljon. M. Seitlinger úgy értékelte,

639 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

640 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

641 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

hogy személyes adatainak szóban forgó gyűjtése és tárolása semmiképpen sem volt szükséges azon technikai célok érdekében, hogy az információkat a hálózaton keresztül elküldje vagy fogadja. Ezen adatok számlázási célokra való gyűjtésére és tartós tárolására sem volt szükség. M. Seitlinger kijelentette, hogy nem járult hozzá, hogy ilyen módon felhasználják személyes adatait, amelyek gyűjtésének és tárolásának egyetlen oka a 2003-as osztrák távközlési törvény.

M. Seitlinger ezért keresetet indított az osztrák Alkotmánybíróságon, amelyben azt állította, hogy a távközlési szolgáltatójával szemben előírt törvényi kötelezettségek sértik az EU Alapjogi Chartájának 8. cikke szerinti alapvető jogait. Figyelemmel arra, hogy az osztrák szabályozás végrehajtotta az uniós jogot (az akkori adatmegőrzési irányelvet), az osztrák alkotmánybíróság az ügyet az EUB elé vitte, hogy döntsön arról, hogy az irányelv és az EU Alapjogi Chartájában biztosított magánélethez és adatvédelemhez való jogok összeegyeztethetők-e.

Az EUB nagytanácsa döntést hozott az ügyben, amelynek eredményeképp hatályon kívül helyezte az uniós adatmegőrzési törvényt. Az EUB megállapította, hogy az irányelv különösen súlyos beavatkozást jelentett a magánélethez és adatvédelemhez való alapjogokba anélkül, hogy a beavatkozást a feltétlenül szükséges mértékre korlátozta volna. Az irányelv törvényes célt szolgált, mivel lehetővé tette a nemzeti hatóságok számára, hogy a súlyos bűncselekmények kivizsgálása és büntetőeljárás alá vonása érdekében további lehetőségekkel rendelkezzenek, e tekintetben tehát a bűnügyi nyomozás hasznos eszközeit alkotják. Az EUB azonban megállapította, hogy az alapvető jogokat csak akkor lehet korlátozni, ha az feltétlenül szükséges, és ehhez egyértelmű és pontos szabályoknak kell társulniuk a hatályát illetően, és az egyéneknek kellő biztosítékokkal kell rendelkezniük.

Az EUB véleménye szerint az irányelv nem állta meg a helyét a szükségességi vizsgán. Először is, nem hozott létre a beavatkozás mértékét korlátozó egyértelmű és pontos szabályokat. Ahelyett, hogy kapcsolat meglétét írta volna elő a megőrzött adatok és egy súlyos bűncselekmény között, az irányelv valamennyi felhasználó valamennyi elektronikus kommunikációs eszközön keresztül bonyolított összes metaadatára vonatkozott. Így gyakorlatilag beavatkozott a teljes uniós lakosság magánélethez és az adatvédelemhez való jogába, ami aránytalannak minősíthető. Nem

> tartalmazott a személyes adatokhoz hozzáférő személyek körének korlátozására vonatkozó feltételeket, és az ilyen hozzáférésre nem vonatkoztak eljárási feltételek sem, például egy közigazgatási hatóság vagy bíróság hozzáférés előtti jóváhagyásának előírása. Végezetül, az irányelv nem határozott meg egyértelmű biztosítékokat a megőrzött adatok védelmére. Ezért nem biztosította az adatok hatékony védelmét a visszaélések kockázatával és az adatok jogosulatlan hozzáférésével és felhasználásával szemben.[642]

Elvben a Bíróságnak meg kell válaszolnia az elé vitt kérdéseket, és azon az alapon nem tagadhatja meg az előzetes döntéshozatalt, hogy válasza az eredeti ügy szempontjából nem releváns és nem is a kellő időben születik. Akkor azonban megtagadhatja, ha a kérdés nem tartozik a hatáskörébe.[643] Az EUB csupán az előzetes döntéshozatalra elé terjesztett kérelem alapelemeire vonatkozóan hoz határozatot, míg az eredeti ügyben továbbra is a nemzeti bíróság illetékes.[644]

Az **Európa Tanács joga szerint** a részes felek kötelesek megfelelő bírósági és nem bírósági jogorvoslati lehetőségeket kidolgozni a Korszerűsített 108. Egyezmény rendelkezéseinek megsértésére.[645] Az adatvédelmi jogok feltételezett megsértése, amit az EJEE egyik részes fele követett el, és ami az EJEE 8. cikkét is sérti, ezenfelül az EJEB elé is vihető, ha az összes hazai jogorvoslati lehetőséget már kimerítették. Ahhoz, hogy az EJEE 8. cikkének megsértését az EJEB elé vigyék, más elfogadhatósági kritériumoknak is meg kell felelni (az EJEE 34–35. cikkei).[646]

Bár az EJEB-hez intézett kereseti kérelmek közvetlenül a részes felek ellen is benyújthatók, közvetve magánfelek cselekedeteivel vagy mulasztásaival is foglalkozhatnak, amennyiben egy részes fél nem tett eleget az EJEE értelmében fennálló pozitív kötelezettségeinek, és nemzeti jogában nem nyújtott elegendő védelmet az adatvédelmi jogok megsértése ellen.

642 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8., 69. pont.

643 EUB, *Pasquale Foglia kontra Mariella Novello*, 244/80. sz. ügy, 1981. december 16.; EUB, *Büntetőeljárás Gasparini és társai ellen*, C-467/04. sz. ügy., 2006. szeptember 28.

644 EUB, *International Transport Workers' Federation, Finnish Seamen's Union kontra Viking Line ABP, OÜ Viking Line Eesti* [nagytanács], C-438/05. sz. ügy, 2007. december 11., 85. pont.

645 Korszerűsített 108. Egyezmény, 12. cikk.

646 EJEE, 34–37. cikk.

Példa: A *K.U. kontra Finnország* ügyben[647] a felperes egy gyermek volt, aki azért tett panaszt, mert egy internetes társkereső oldalon szexuális tartalmú hirdetést tettek közzé a nevében. A szolgáltató a finn jog által előírt titoktartási kötelezettségek miatt nem fedte fel azon személy személyazonosságát, aki közzétette az információkat. A felperes azt állította, hogy a finn jog nem nyújt elegendő védelmet a felperesről az interneten terhelő adatokat elhelyező magánszemély ilyen jellegű cselekményeivel szemben. Az EJEB megállapította, hogy az államok nemcsak kötelesek tartózkodni az egyének magánéletébe való önkényes beavatkozástól, hanem pozitív kötelezettségek is terhelhetik őket, amelyek „a magánélet tiszteletben tartásának biztosítására irányuló intézkedések elfogadását" jelentik „akár az egyének egymás közötti kapcsolatainak szférájában is". A felperes esetében a gyakorlati és hatékony védelem megkövetelte volna, hogy tegyenek tényleges lépéseket az elkövető azonosítására és vád alá helyezésére. Az állam azonban nem biztosított ilyen védelmet, ezért a Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: A *Köpke kontra Németország* ügyben[648] a felperest a munkahelyén elkövetett lopással gyanúsították meg, és rejtett videokamerás megfigyelés alá helyezték. Az EJEB megállapította, hogy „semmi nem mutat arra, hogy a belföldi hatóságok mérlegelési mozgásterükön belül nem teremtettek megfelelő egyensúlyt egyfelől a felperes magánéletének tiszteletben tartásához való, 8. cikk szerinti joga, másfelől munkáltatójának a tulajdon védelméhez fűződő érdeke és a gondos igazságszolgáltatáshoz fűződő közérdek között". A keresetet ezért elfogadhatatlannak nyilvánították.

Ha az EJEB megállapítja, hogy egy részes fél megsértette az EJEE által védelemben részesített bármelyik jogot, a részes fél köteles az EJEB ítéletét végrehajtani (EJEE 46. cikk). A végrehajtási intézkedéseknek először is véget kell vetniük a jogsértésnek, és – amennyire lehetséges – orvosolniuk kell a jogsértés felperest érintő negatív következményeit. Az ítéletek végrehajtásához a Bíróság által megállapítotthoz hasonló jogsértések megelőzésére irányuló általános intézkedések is szükségesek, amelyek lehetnek jogszabály-módosítások, az ítélkezési gyakorlatban bekövetkező változások vagy egyéb intézkedések.

647 EJEB, *K.U. kontra Finnország*, 2872/02. sz. ügy, 2008. december 2.

648 EJEB, *Köpke kontra Németország*, 420/07. sz. ügy, 2010. október 5.

Ha az EJEB az EJEE megsértését állapítja meg, az EJEE 41. cikke értelmében az EJEB igazságos elégtételt ítélhet meg a felperesnek a részes fél költségére.

Nonprofit jellegű szerv, szervezet vagy egyesület megbízásához való jog

Az általános adatvédelmi rendelet lehetővé teszi a felügyeleti hatósághoz panaszt benyújtó vagy bíróság előtt keresetet indító egyén számára, hogy képviseletével nonprofit jellegű szervet, szervezetet vagy egyesületet bízzon meg.[649] Követelmény e nonprofit szervezetekkel szemben, hogy alapszabályában rögzített céljaik a közérdeket szolgálják, és az adatvédelem területén tevékenykedjenek. Az ilyen szervezet benyújthatja a panaszt vagy gyakorolhatja a bírósági jogorvoslathoz való jogot az érintett(ek) nevében. A rendelet lehetőséget biztosít a tagállamok számára eldönteni – a nemzeti jogukkal összhangban –, hogy valamely testület nyújthat-e be panaszt az érintettek nevében az érintettektől kapott megbízás nélkül.

Ez a képviseleti jog lehetővé teszi az egyének számára, hogy kihasználják a nonprofit szerveztek szakértelmét, illetve szervezési, valamint pénzügyi lehetőségeit, ami nagymértékben megkönnyíti az egyének jogainak gyakorlását. Az általános adatvédelmi rendelet megengedi e szervezetek számára, hogy több érintett nevében kollektív keresetet nyújtsanak be. Ez az igazságszolgáltatási rendszer működését és hatékonyságát is támogatja, ugyanis a hasonló kereseteket csoportosítják és együttesen vizsgálják.

6.2.3 Felelősség és a kártérítéshez való jog

A hatékony jogorvoslathoz való jognak lehetővé kell tennie az egyének számára, hogy kártérítést követeljenek személyes adataiknak az alkalmazandó jogszabályokkal ellentétes kezelése eredményeképp elszenvedett károkért. Az adatkezelők és adatfeldolgozók jogellenes adatkezelés miatti felelősségét kifejezetten elismeri az általános adatvédelmi rendelet.[650] A rendelet jogot biztosít az egyének számára, hogy az adatkezelőtől vagy adatfeldolgozótól kártérítést kapjanak mind a vagyoni mind pedig a nem vagyoni károk vonatkozásában, miközben a preambulumbekezdésében kimondja, hogy „a kár fogalmát a Bíróság ítélkezési gyakorlatának fényében tágan kell értelmezni, mégpedig oly módon, hogy az teljes mértékben tükrözze

649 Általános adatvédelmi rendelet, 80. cikk.

650 *Uo.*, 82. cikk.

e rendelet célkitűzéseit".[651] Az adatkezelők felelősséggel tartoznak, és kártérítési kötelezettség terheli őket, ha nem tesznek eleget a rendelet szerinti kötelezettségeiknek. Az adatfeldolgozó csak abban az esetben tartozik felelősséggel az adatkezelés által okozott károkért, ha nem tartotta be a rendeletben meghatározott, kifejezetten az adatfeldolgozókat terhelő kötelezettségeket, vagy ha az adatkezelő jogszerű utasításait figyelmen kívül hagyta vagy azokkal ellentétesen járt el. Ha valamely adatkezelő vagy adatfeldolgozó teljes kártérítést fizetett, az általános adatvédelmi rendelet rendelkezik arról, hogy – az ugyanazon adatkezelésben érintett többi adatkezelőtől vagy adatfeldolgozótól – visszaigényelje a kártérítésnek azt a részét, amely megfelel a károkozásért viselt felelősségük mértékének.[652] Ugyanakkor a felelősség alóli mentesülés rendkívül szigorú, és bizonyítania kell, hogy a kárt előidéző eseményért őt semmilyen módon nem terheli felelősség.

A kártérítésnek „teljesnek és ténylegesnek" kell lennie az elszenvedett károkozás vonatkozásában. Ha egy adatkezelésben több adatkezelő, illetve adatfeldolgozó okozott kárt, akkor minden egyes adatkezelő vagy adatfeldolgozó egyetemleges felelősséggel tartozik a teljes kárért. Ennek a szabálynak a célja biztosítani a tényleges kártérítést az érintettek számára, továbbá egy összehangolt megközelítést az adatkezelési tevékenységekben részt vevő adatkezelők és adatfeldolgozók tekintetében.

Példa: Az érintettek nem kötelesek a károkozásért felelős valamennyi szervezettel szemben eljárást indítani vagy kártérítést követelni, mivel az drága és hosszadalmas eljárást eredményezne. Elegendő a közös adatkezelők egyikével szemben eljárást indítani, amelyet majd a teljes károkozásért felelősségre vonnak. Ilyen esetekben a kártérítést megfizető adatkezelő vagy adatfeldolgozó később jogosult az adatkezelésben érintett és a jogsértésért felelős többi szervezettől visszaigényelni a kártérítésnek azt a részét, amely megfelel a károkozásért viselt felelősségük mértékének. A különböző közös adatkezelők és adatfeldolgozók közötti eljárásokra azt követően kerül sor, hogy az érintett megkapta a kártérítést, és ezeknek az érintett nem jogosultja.

Az Európa Tanács jogi keretrendszerében a Korszerűsített 108. Egyezmény 12. cikke előírja a részes felek számára, hogy megfelelő jogorvoslati lehetőségeket

651 *Uo.*, (146) preambulumbekezdés.

652 *Uo.*, 82. cikk (2) és (5) bekezdés.

dolgozzanak ki az egyezmény előírásait végrehajtó nemzeti jogszabályok megsértéséért. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés kimondja, hogy a jogorvoslatnak tartalmaznia kell valamely határozat vagy gyakorlat bíróság előtti megtámadásának lehetőségét, ugyanakkor lehetővé kell tenni nem bírósági jogorvoslati lehetőségeket is.[653] E jogorvoslatokhoz való hozzáférés módozatainak és különböző szabályainak, továbbá a követendő eljárások megállapítását az egyezmény az egyes részes felek döntésére bízza. A részes feleknek és a nemzeti bíróságoknak mérlegelniük kell a kártérítésre vonatkozó rendelkezéseket az adatkezelés által okozott vagyoni és nem vagyoni károk esetére, valamint a kollektív kereset indításának lehetőségét.[654]

6.2.4 Szankciók

Az **Európa Tanács jogában** a Korszerűsített 108. Egyezmény 12. cikke úgy rendelkezik, hogy mindegyik részes fél vállalja, hogy megfelelő szankciókat és jogorvoslatokat állapít meg a 108. Egyezményben foglalt adatvédelmi alapelveket érvényesítő hazai jog rendelkezéseinek megsértése esetén. Az egyezmény nem állapít meg vagy szab ki konkrét szankciókat. Ezzel szemben egyértelműen kimondja, hogy minden egyes részes fél maga dönthet a bírósági vagy nem bírósági szankciókról, amelyek lehetnek büntetőjogi, közigazgatási vagy polgári jogi szankciók. A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés úgy rendelkezik, hogy a szankcióknak ténylegesnek, arányosnak és visszatartó erejűnek kell lenniük.[655] A részes feleknek a hazai jogrendjükben elérhető szankciók jellegének és súlyosságának meghatározásakor tiszteletben kell tartaniuk ezt az elvet.

Az **uniós jogban** az általános adatvédelmi rendelet felhatalmazza a tagállamok felügyeleti hatóságait, hogy közigazgatási bírságot szabjanak ki a rendelet megsértése miatt. A bírságok szintjéről, és a nemzeti hatóságok által a bírság kiszabására vonatkozó döntés meghozatalakor figyelembe veendő körülményekről, továbbá a bírság maximális összegéről szintén a 83. cikk rendelkezik. A szankciók rendszere ezzel az egész Unióban harmonizált.

Az általános adatvédelmi rendelet sávos megközelítést alkalmaz a bírságokra. A felügyeleti hatóságok legfeljebb 20 000 000 euró összegű közigazgatási bírságot, illetve vállalkozások esetében azok teljes éves világpiaci forgalmának legfeljebb

653 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 100. pont.

654 *Uo.*

655 *Uo.*

4%-át kitevő összeget szabhatnak ki attól függően, hogy melyik érték magasabb. Ilyen mértékű bírsággal sújtható az adatkezelés elveinek, illetve a hozzájárulás feltételeinek megsértése, az érintettek jogainak valamint a rendelet személyes adatok harmadik országbeli címzett részére történő továbbítására vonatkozó rendelkezéseinek a megsértése. Egyéb jogsértések esetén a felügyeleti hatóságok legfeljebb 10 000 000 euró vagy egy vállalkozás esetén teljes éves világpiaci forgalmának legfeljebb 2%-át kitevő összeget szabhatnak ki attól függően, hogy melyik érték magasabb.

A kiszabandó bírság típusának és mértékének megállapításakor a felügyeleti hatóságoknak egy sor tényezőt kell figyelembe venniük.[656] Például, megfelelően mérlegelni kell a jogsértés jellegét, súlyosságát és időtartamát, az érintett adatkategóriákat, és azt, hogy a jogsértést szándékosan vagy gondatlanságból követték-e el. Azt is figyelembe kell venni, ha az adatkezelő vagy adatfeldolgozó intézkedéseket tett az érintettek által elszenvedett károk enyhítése érdekében. Hasonlóan fontos tényező a felügyeleti hatóság döntésének meghozatala során a felügyeleti hatósággal való együttműködés szintje a jogsértést követően, valamint az, hogy a felügyeleti hatóság miként értesült a jogsértésről (például az adatkezelésért felelős szervezet jelentette, vagy az az érintett, akinek a jogait megsértették).[657]

Azon túl, hogy a felügyeleti hatóságok közigazgatási bírságokat szabhatnak ki, átfogó korrekciós hatáskörrel is rendelkeznek. A felügyeleti hatóság úgynevezett „korrekciós" hatáskörét az általános adatvédelmi rendelet 58. cikke rögzíti. Ezek között megtalálható az adatkezelők és adatfeldolgozók utasítása, figyelmeztetése és elmarasztalása, az adatkezelési tevékenységek átmeneti vagy akár végleges megtiltása.

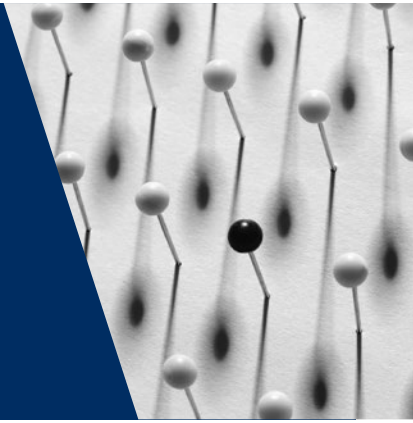
Ami az uniós jog uniós intézmények vagy szervek általi megsértésének szankcióit illeti, szankciókat – az uniós intézmények adatvédelmi rendeletének speciális feladata miatt – fegyelmi intézkedés formájában irányozhatnak elő. A rendelet 49. cikke szerint „ha az Európai Közösségek tisztviselője vagy más alkalmazottja az e rendeletben foglalt kötelezettségeit szándékosan vagy gondatlanságból megszegi, ellene [...] fegyelmi eljárás indul".

656 Általános adatvédelmi rendelet, 83. cikk (2) bekezdés.

657 29. cikk szerinti munkacsoport (2017), *Iránymutatás a 2016/679 rendelet szerinti közigazgatási bírság alkalmazásáról és megállapításáról*, WP 253, 2017. október 3.

7

Személyes adatok nemzetközi továbbítása és áramlása



EU	Tárgyalt kérdések	Európa Tanács
Személyes adatok továbbítása		
Általános adatvédelmi rendelet, 44. cikk	Fogalom	Korszerűsített 108. Egyezmény, 14. cikk (1) és (2) bekezdés
Személyes adatok szabad áramlása		
Általános adatvédelmi rendelet, 1. cikk (3) bekezdés és (170) preambulumbekezdés	Az uniós tagállamok között	
	A 108. Egyezmény részes felei között	Korszerűsített 108. Egyezmény, 14. cikk (1) bekezdés
Harmadik országok vagy nemzetközi szervezetek számára történő adattovábbítás		
Általános adatvédelmi rendelet, 45. cikk EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015	Megfelelőségi határozat/megfelelő védelmi szinttel rendelkező harmadik országok vagy nemzetközi szervezetek	Korszerűsített 108. Egyezmény, 14. cikk (2) bekezdés
Általános adatvédelmi rendelet, 46. cikk (1) bekezdés és 46. cikk (2)	Megfelelő biztosítékok, ideértve az érvényesíthető jogokat és jogorvoslati lehetőségeket az érintettek számára, általános szerződési feltételek, kötelező erejű vállalati szabályok, magatartási kódexek és tanúsítási mechanizmusok révén	Korszerűsített 108. Egyezmény, 14. cikk (2), (3), (5) és (6) bekezdés

EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet, 46. cikk (3) bekezdés Általános adatvédelmi rendelet, 46. cikk (5) bekezdés	**Az illetékes felügyeleti hatóság engedélyétől függően: kikötések és rendelkezések beillesztése a közhatalmi szervek között létrejött közigazgatási megállapodásokba** **A 95/46 irányelv alapján meglévő felhatalmazások**	
Reglamento general de protección de datos, artículo 46, apartado 5	**Autorizaciones existentes con arreglo a la Directiva 95/46**	
Általános adatvédelmi rendelet, 47. cikk	**Kötelező erejű vállalati szabályok**	
Általános adatvédelmi rendelet, 49. cikk	**Kivételes esetekben biztosított eltérések**	Korszerűsített 108. Egyezmény, 14. cikk (4) bekezdés
Példák: EU–USA PNR-megállapodás EU–USA SWIFT-megállapodás	**Nemzetközi megállapodások**	Korszerűsített 108. Egyezmény, 14. cikk (3) bekezdés a) pont

Az uniós jogban az általános adatvédelmi rendelet rendelkezik az adatok szabad áramlásáról az Európai Unión belül. Tartalmaz ugyanakkor konkrét előírásokat is a személyes adatok Unión kívüli harmadik országokba, illetve nemzetközi szervezeteknek való továbbítására vonatkozóan. A rendelet elismeri az ilyen adattovábbítások fontosságát különösen a nemzetközi kereskedelemmel és együttműködéssel összefüggésben, azonban azt is elismeri, hogy ez a személyes adatokra nézve fokozottabb kockázattal jár. A rendelet ezért arra törekszik, hogy az EU-n belüli védelemmel azonos szintű védelmet biztosítson a harmadik országba továbbított személyes adatok számára.[658] Az Európa Tanács joga szintén elismeri, hogy fontos végrehajtani a határokon átnyúló adatáramokra vonatkozó szabályokat, a részes felek közötti szabad áramlás és a nem részes felek közötti adattovábbításokra megállapított egyedi követelmények alapján.

658 Általános adatvédelmi rendelet, (101) és (116) preambulumbekezdés.

7.1 A személyes adatok továbbításának jellege

Főbb pontok

- Az EU és az Európa Tanács joga is tartalmaz szabályokat a személyes adatok harmadik országbeli címzettek, vagy nemzetközi szervezetek részére történő továbbítására.
- Annak biztosítása érdekében, hogy az érintettek jogai védelemben részesüljenek az adatok Unión kívüli továbbítása során lehetővé teszi, hogy az uniós szabályozás által megkövetelt szintű védelem kísérje végig az EU-ból származó személyes adatokat.

Az **Európa Tanács joga** a határokon átnyúló adatáramlást a személyes adatok külföldi joghatóság alá tartozó címzettek részére történő továbbításaként jellemzi.[659] A határokon átnyúló adattovábbítás olyan címzett számára, aki nem tartozik valamely részes fél joghatósága alá kizárólag akkor megengedett, ha biztosított a megfelelő szintű védelem.[660]

Az **uniós jog** „olyan személyes adatok továbbítását [szabályozza], amelyeket harmadik országba vagy nemzetközi szervezet részére történő továbbításukat követően adatkezelésnek vetnek alá vagy szándékoznak alávetni [...].[661] Az ilyen adattovábbítás csak akkor megengedett, ha az megfelel az általános adatvédelmi rendelet V. fejezetében megállapított szabályoknak.

A személyes adatok határokon átnyúló áramlása megengedett olyan címzett számára, aki az Európa tanácsi jog vagy az uniós jog értelmében valamely részes fél vagy tagállam joghatósága alá tartozik. Bizonyos feltételek teljesítése mellett mindkét jogrendszer megengedi az adatok olyan országba történő továbbítását, amely nem részes fél vagy tagállam.

659 A Korszerűsített 108. Egyezményhez fűzött Magyarázó Jelentés, 102. pont.

660 Korszerűsített 108. Egyezmény, 14. cikk (2) bekezdés.

661 Általános adatvédelmi rendelet, 44. cikk.

7.2 A személyes adatok szabad mozgása/áramlása a tagállamok vagy részes felek között

Főbb pontok

- Nem korlátozható a személyes adatok Unión belüli áramlása, valamint a személyes adatoknak a Korszerűsített 108. Egyezmény részes felei közötti továbbítása. Mivel azonban a Korszerűsített 108. Egyezmény nem minden részes fele tagja az EU-nak, az adatok valamely uniós tagállamból történő továbbítása egy harmadik országba, annak ellenére, hogy az a Korszerűsített 108. Egyezmény részes fele, nem lehetséges, ha az nem teljesíti az általános adatvédelmi rendeletben meghatározott feltételeket.

Az **Európa Tanács joga szerint** biztosítani kell a személyes adatok szabad áramlását a Korszerűsített 108. Egyezmény részes felei között. Az adattovábbítás azonban megtiltható, ha fennáll „a valós és komoly kockázata annak, hogy a másik részes félnek történő továbbítás az egyezmény rendelkezéseinek kijátszásához vezethet", vagy ha bármely felet a személyes adatok „védelméről szóló, valamely regionális nemzetközi szervezethez tartozó államok által közösen alkalmazott harmonizált szabályok erre kötelezik".[662]

Az uniós jogban tilos a személyes adatok uniós tagállamok közötti szabad áramlásának korlátozása vagy tiltása a természetes személyeknek a személyes adatok kezelése tekintetében történő védelmével összefüggő okokból.[663] Az Európai Gazdasági Térségről (EGT) [664] szóló megállapodás, amely Izlandot, Liechtensteint és Norvégiát is a belső piachoz csatolta, kibővítette a szabad adatáramlás területét.

662 Korszerűsített 108. Egyezmény, 14. cikk (1) bekezdés.

663 Általános adatvédelmi rendelet, 1. cikk (3) bekezdés.

664 A Tanács és a Bizottság 1993. december 13-i határozata az Európai Közösségek, azok tagállamai, valamint az Osztrák Köztársaság, a Finn Köztársaság, az Izlandi Köztársaság, a Liechtensteini Hercegség, a Norvég Királyság, a Svéd Királyság és a Svájci Államszövetség között az Európai Gazdasági Térségről létrejött megállapodás megkötéséről, HL L 1., 1994.1.3.

Példa: Ha egy több uniós tagállamban, köztük Szlovéniában és Franciaországban is letelepedett nemzetközi vállalatcsoport egyik leányvállalata Szlovéniából Franciaországba továbbít személyes adatokat, az ilyen adatáramlást szlovén nemzeti jogszabály nem korlátozhatja, és nem tilthatja a személyes adatok kezelése védelmével összefüggő okokból.

Ha azonban ugyanez a szlovén leányvállalat ugyanazokat a személyes adatokat az anyavállalatnak akarja továbbítani Malajziába, a szlovén adatexportőrnek figyelembe kell venni az általános adatvédelmi rendelet V. fejezetében foglalt szabályokat. Ezeknek a rendelkezéseknek a célja, hogy biztosítsák azon érintettek személyes adatainak védelmét, akik nem tartoznak az Unió joghatósága alá.

Az uniós jog értelmében a személyes adatok EGT tagállamaiba való áramlása a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából a 2016/680 irányelv[665] hatálya alá tartozik. Ez biztosítja, hogy a személyes adatok illetékes hatóságok általi cseréje az Unión belül adatvédelmi okokból ne legyen korlátozható vagy tiltható. Az Európa Tanács jogában valamennyi személyes adat kezelése (ideértve azok határokon átnyúló továbbítását a 108. Egyezmény részes feleinek) a célok és intézkedési területekre vonatkozó kivételek nélkül a 108. Egyezmény hatálya alá tartozik, bár a részes felek meghatározhatnak mentességeket. Az EGT valamennyi tagja egyben a 108. Egyezményben is részes fél.

665 Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4.

7.3 Harmadik országok/nem részes felek vagy nemzetközi szervezetek számára történő adattovábbítás

Főbb pontok

- Az **Európa Tanács** és az **Unió** joga egyaránt megengedi a személyes adatok továbbítását harmadik országok vagy nemzetközi szervezet részére, feltéve, hogy teljesülnek bizonyos feltételek a személyes adatok védelme érdekében.
  - Az **Európa Tanács jogában** megfelelő szintű védelem érhető el az állam vagy nemzetközi szervezet jogszabályán keresztül, vagy megfelelő előírások alkalmazásával.
  - Az **uniós jogban** adattovábbításra akkor kerülhet sor, ha a harmadik ország megfelelő szintű védelmet biztosít, vagy ha az adatkezelő vagy adatfeldolgozó gondoskodik a megfelelő biztosítékokról, beleértve az érintettek számára érvényesíthető jogokat és jogorvoslati lehetőségeket, például általános adatvédelmi kikötések vagy kötelező erejű vállalati szabályok alkalmazásával.
- Az **Európa Tanács és az EU joga egyaránt** biztosít eltérést, amely lehetővé teszi a személyes adatok továbbítását egyedi körülmények között még akkor is, ha nincs se megfelelő szintű védelem, se nem alkalmaznak megfelelő biztosítékokat.

Noha mind az Európa Tanács, mind az EU joga lehetővé teszi az adatok harmadik országokba vagy nemzetközi szervezet részére történő továbbítását, különböző feltételeket állapítanak meg. Mindegyik feltételrendszer figyelembe veszi az illető szerv eltérő felépítését és céljait.

Az **uniós jogban** elvben két módja létezik a személyes adatok harmadik országokba vagy nemzetközi szervezet részére történő továbbítására. A személyes adatok továbbítása a következők alapján történhet: az Európai Bizottság megfelelőségi határozata;[666] vagy megfelelőségi határozat hiányában, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat biztosít, beleértve az érintettek számára érvényesíthető jogokat és jogorvoslati lehetőségeket.[667] Megfelelőségi határozat vagy garanciák hiányában számos eltérés áll rendelkezésre.

666 Általános adatvédelmi rendelet, 45. cikk.

667 *Uo.*, 46. cikk.

Az **Európa Tanács** jogában ugyanakkor a szabad adattovábbítás az egyezménynek nem részes felei részére csak a következők alapján megengedett:

- az illető állam vagy a nemzetközi szervezet jogszabályai, beleértve az alkalmazandó nemzetközi egyezményeket vagy a megfelelő garanciákat biztosító megállapodásokat;

- az adattovábbításban vagy további adatkezelésben érintett személyek által elfogadott és végrehajtott jogilag kötelező érvényű és érvényesíthető eszközök által biztosított eseti vagy jóváhagyott általános garanciák.[668]

Az uniós joghoz hasonlóan megfelelő szintű adatvédelem hiányában számos eltérés áll rendelkezésre.

7.3.1 Adattovábbítás megfelelőségi határozat alapján

Az **uniós jogban** a személyes adatok megfelelő szintű adatvédelmet biztosító harmadik országokba irányuló szabad áramlásáról az általános adatvédelmi rendelet 45. cikke rendelkezik. Az EUB pontosította, hogy a „megfelelő szintű védelem" kifejezés megköveteli, hogy a harmadik ország az alapjogok és szabadságok olyan szintű védelmét biztosítsa, amely „lényegében egyenértékű"[669] az uniós jogban biztosított garanciákkal. Ugyanakkor azok az eszközök, amelyeket a harmadik ország az ilyen védelmi szint biztosításához igénybe vesz, különbözhetnek azoktól az eszközöktől, amelyeket az Unióban alkalmaznak; a megfelelőségre vonatkozó előírás nem követeli meg az uniós szabályok pontról pontra történő leképezését.[670]

Az Európai Bizottság a külföldi országok adatvédelmi szintjét azok nemzeti jogszabályainak és alkalmazandó nemzetközi kötelezettségeinek megvizsgálásával állapítja meg. Szintén figyelembe kell venni egy ország részvételét többoldalú vagy regionális rendszerekben, különösen a személyes adatok védelmét illetően. Ha az Európai Bizottság azt állapítja meg, hogy a harmadik ország vagy nemzetközi

668 Korszerűsített 108. Egyezmény, 14. cikk (3) bekezdés a) és b) pont.

669 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6., 96. pont.

670 *Uo.*, 74. pont. Lásd még: Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak „A személyes adatok cseréje és védelme a globalizált világban", COM(2017) 7 final, 2017. január 10., 6. o.

szervezet megfelelő szintű védelmet biztosít, kötelező érvényű megfelelőségi határozatot bocsáthat ki.[671] Mindazonáltal az EUB kimondta, hogy a nemzetközi felügyeleti hatóságok annak ellenére rendelkeznek hatáskörrel arra vonatkozóan, hogy megvizsgálják valamely személy őt érintő személyes adatok kezelésével kapcsolatos kérelmét, akinek a személyes adatait olyan harmadik országba továbbították, amelyet a Bizottság megfelelő szintű védelmet biztosítónak minősített, amennyiben ez a személy arra hivatkozik, hogy az ezen országban hatályos jog és gyakorlatok nem biztosítanak megfelelő védelmi szintet.[672]

Az Európai Bizottság megvizsgálhatja egy harmadik országon belüli terület megfelelőségét, vagy vizsgálatát korlátozhatja egy adott ágazatra, ahogy azt Kanada magán kereskedelmi szabályozása esetében tette, például.[673] Az EU és harmadik országok közötti megállapodásokon alapuló továbbítások tekintetében is számos megfelelőségre vonatkozó megállapítás létezik. Ezek a határozatok egyetlen adattípus továbbítására vonatkoznak, például az utasnyilvántartási adatok (PNR) légitársaságok által a külföldi határellenőrző hatóságok részére történő továbbítására, amikor a légitársaság az EU-ból bizonyos tengerentúli célállomásokra repül (lásd a 7.3.4 szakaszt).

A megfelelőségi határozatok folyamatos ellenőrzés hatálya alá tartoznak. Az Európai Bizottság rendszeresen felülvizsgálja az ilyen határozatokat, hogy nyomon kövesse azok állapotát esetlegesen befolyásoló fejleményeket. Ezért ha az Európai Bizottság azt állapítja meg, hogy az adott harmadik ország vagy nemzetközi szervezet már nem tesz eleget a megfelelőségi határozatot alátámasztó feltételeknek, módosíthatja, felfüggesztheti vagy hatályon kívül helyezheti a határozatot. A Bizottság tárgyalásokat is kezdeményezhet az érintett harmadik országgal vagy nemzetközi szervezettel a határozata mögött meghúzódó probléma orvoslása érdekében. Költségvetés-tervezet

Az Európai Bizottság által a 95/46/EK irányelv alapján elfogadott megfelelőségi határozatok addig maradnak érvényben, amíg azokat az általános adatvédelmi

671 A megfelelőségre vonatkozó megállapítást elnyert országok folyamatosan frissülő listáját lásd az Európai Bizottság Jogérvényesülési Főigazgatósága honlapján.

672 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6., 63. és 65–66. pont.

673 Európai Bizottság (2002), 2002/2/EK határozat (2001. december 20.) a 95/46/EK európai parlamenti és tanácsi irányelv értelmében a személyes adatoknak a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény által biztosított megfelelő védelméről, HL L 2., 2002.1.4.

rendelet 45. cikkével összhangban elfogadott bizottsági határozat nem módosítja, váltja fel vagy helyezi hatályon kívül.

A mai napig az Európai Bizottság Andorrát, Argentínát, Kanadát (a személyes információk védelméről és az elektronikus dokumentumokról szóló kanadai törvény (PIPADA) alá tartozó kereskedelmi szervezeteket), Feröer szigeteket, Guernsey-szigetet, Jersey-szigetet, Izraelt, a Man-szigetet, Új-Zélandod, Svájcot és Uruguayt ismerte el megfelelő védelmet nyújtó országként. Figyelemmel az adatok Amerikába történő továbbítására, az Európai Bizottság 2000-ben elfogadott egy megfelelőségi határozatot, amely lehetővé teszi az adattovábbítást azon vállalatok számára, amelyek nyilatkoztak arról, hogy az EU-ból továbbított személyes adatokat védik, és megfelelnek az ún. „biztonságos kikötő" adatvédelmi elveknek.[674] Az EUB ezt a határozatot 2015-ben érvénytelenítette, és egy új megfelelőségi határozatot fogadott el 2016 júliusában, amely a vállalatok csatlakozását 2016. augusztus 1-jétől tette lehetővé.

Példa: A *Schrems* ügyben[675] Maximilian Schrems, egy osztrák állampolgár éveken keresztül Facebook-felhasználó volt. Az M. Schrems által a Facebooknak megadott egyes vagy összes adatot a Facebook ír leányvállalatától az USA-ban lévő szerverekre továbbították, ahol azokat kezelték. M. Schrems panaszt nyújtott be az ír adatvédelmi hatóságnál azzal, hogy véleménye szerint figyelemmel Edward Snowden, egy visszaélést bejelentő amerikai személy az USA hírszerző szolgálatainak a tevékenységeire vonatkozóan kiszivárogtatott információkra tekintettel az USA joga és gyakorlata nem biztosít elégséges védelmet az abba az országba továbbított személyes adatok tekintetében. Az ír hatóság elutasította a panaszt azzal, hogy 2000. július 26-i határozatában az Európai Bizottság úgy vélte, hogy a „biztonságos kikötő" megállapodás keretében az USA megfelelő szintű védelmet biztosít a továbbított személyes adatok vonatkozásában. Az ügyet az ír legfelsőbb bíróság elé terjesztették, amely azt előzetes döntéshozatalra az EUB elé utalta.

674 A Bizottság 2000/520/EK határozata (2000. július 26.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján, az Egyesült Államok Kereskedelmi Minisztériuma által kiadott biztonságos kikötő adatvédelmi elvek által biztosított védelem megfelelőségéről és az ezzel kapcsolatos gyakran felvetődő kérdésekről, HL L 2015., 2000.8.25. A határozatot az EUB érvénytelennek nyilvánította a *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügyben.

675 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

Az EUB ítélete szerint a Bizottságnak a biztonságos kikötő keretrendszer megfelelőségére vonatkozó határozata érvénytelen. Az EUB először megállapította, hogy a határozat megengedte a biztonságos kikötő adatvédelmi elvek alkalmazásának korlátozását a nemzetbiztonság, a közérdek vagy a bűnüldözés követelményeinek teljesítése, illetve belföldi jogszabályok alapján. A határozat ezért lehetővé tette azon személyek alapvető jogaiba való beavatkozást, akiknek a személyes adatait az USA-ba továbbították vagy továbbíthatták.[676] Megállapította továbbá, hogy a határozat nem tartalmazott megállapításokat olyan állami szabályok meglétére az USA-ban, amelyek korlátozták volna ezt a beavatkozást, sem az ilyen beavatkozással szembeni hatékony jogi védelem meglétére.[677] Az EUB kiemelte, hogy az alapvető jogok és szabadságok Unióban biztosított védelmi szintje megköveteli, hogy az olyan szabályozásnak, amely beavatkozást jelent a 7. és 8. cikkben biztosított alapvető jogokba, egyértelmű és pontos szabályokat kell tartalmaznia a szóban forgó intézkedés hatálya és alkalmazása vonatkozásában, és minimális követelményeket kell előírnia a személyes adatok védelmét illetően.[678] Figyelemmel arra, hogy a Bizottság határozata nem állapította meg, hogy az USA belföldi joga, vagy vállalt nemzetközi kötelezettségei alapján ténylegesen megfelelő védelmi szintet biztosít, az EUB arra a következtetésre jutott, hogy nem teljesítette az adatvédelmi irányelv adattovábbításra vonatkozó megfelelő rendelkezéseiben foglalt követelményeket, és ezért a megállapodást érvénytelennek nyilvánította.[679]

Az USA védelmi szintje tehát nem volt „lényegében megegyező" az EU által garantált alapvető jogokkal és szabadságokkal.[680] Az EUB azt állította, hogy megsértették az EU Alapjogi Chartájának különböző cikkeit. Először is, megsértette a 7. cikk lényegét, mivel az USA szabályozása „lehetővé teszi a hatóságok számára, hogy általános jelleggel hozzáférjenek az elektronikus kommunikációk tartalmához". Másodszor, megsértette a 47. cikk lényegét is, mivel a szabályozása nem biztosított az egyének számára jogorvoslati lehetőséget a személyes adatokhoz való hozzáférés tekintetében, illetve nem biztosította a személyes adatok helyesbítésének vagy törlésének

676 *Uo.*, 84. pont.

677 *Uo.*, 88–89. pont.

678 *Uo.*, 91–92. pont.

679 *Uo.*, 96–97. pont.

680 *Uo.*, 71–74. és 96. pont.

lehetőségét. Végezetül pedig, figyelemmel arra, hogy a biztonságos kikötő megállapodás megsértette a fenti cikkeket, a személyes adatok kezelése nem volt jogszerű, ami a 8. cikk megsértését is eredményezte.

Miután az EUB a biztonságos kikötő megállapodást érvénytelennek nyilvánította, a Bizottság és az USA megállapodott egy új keretrendszerben, az EU–USA adatvédelmi pajzsban. 2016. július 12-én a Bizottság elfogadott egy határozatot, amely kimondja, hogy az USA az adatvédelmi pajzs keretében megfelelő szintű védelmet biztosít az Unióból az USA-beli szervezetek részére továbbított személyes adatok tekintetében.[681]

A biztonságos kikötő megállapodáshoz hasonlóan az EU–USA adatvédelmi pajzs keretrendszerének célja a kereskedelmi célból az EU-ból az USA-ba továbbított személyes adatok védelme.[682] Az amerikai vállalatok önkéntesen tanúsíthatják az adatvédelmi pajzs listájának való megfelelésüket azzal, hogy kötelezettséget vállalnak a keret adatvédelmi előírásainak betartására. Az illetékes USA hatóságok ellenőrzik és igazolják a tanúsított vállalatok előírásoknak való megfelelőségét.

Az adatvédelmi pajzs különösen a következőkről rendelkezik:

- az EU-ból személyes adatokat fogadó vállalatokat terhelő adatvédelmi kötelezettség;

- védelem és jogorvoslati lehetőség az egyének számára különösen egy ombudsmani mechanizmus létrehozásával, amely az amerikai hírszerző szolgálatoktól független, és azon egyénektől érkező panaszokkal foglalkozik, akik úgy vélik, hogy személyes adataikat jogszerűtlenül használták fel az amerikai hatóságok a nemzetbiztonság területén;

681 A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről, HL L 207., 2016.8.1. A 29. cikk szerinti munkacsoport üdvözölte azokat a jobbításokat, amelyeket az adatvédelmi pajzs mechanizmusa hozott a biztonságos kikötő határozathoz képest, és helyeselte, hogy a Bizottság és az amerikai hatóságok figyelembe vették az adatvédelmi pajzs dokumentációjának végleges változatában az EU–USA magánélet-védelmi pajzs tervezet megfelelőségi határozatáról szóló véleményében megfogalmazott aggályokat. Mindazonáltal számos komoly aggályt emelt ki. Bővebb információért lásd: 29. cikk szerinti munkacsoport, *01/2016. sz. vélemény az EU–US magánélet-védelmi pajzs tervezet megfelelőségi határozatáról*, elfogadás időpontja: 2016. április 13., 16/EN WP 238.

682 További információkért lásd az EU–USA adatvédelmi pajzs tájékoztatóját.

- éves közös felülvizsgálat a keretrendszer végrehajtásának ellenőrzésére;[683] az első felülvizsgálatra 2017 szeptemberében került sor.[684]

Az adatvédelmi pajzsra vonatkozó határozatot az amerikai kormány írásos kötelezettségvállalásai és biztosítékai kísérik. Ezek állapítják meg az amerikai kormány személyes adatokhoz való bűnüldözési és nemzetbiztonsági célú hozzáférésére vonatkozó korlátozásokat és biztosítékokat.

7.3.2 Megfelelő garanciák alá tartozó adattovábbítás

Az **unió jog** és az **Európa Tanács joga** egyaránt említi az adatokat exportáló adatkezelő és a harmadik országban lévő címzett vagy nemzetközi szervezet közötti szerződési feltételeket, mint a címzettnél a megfelelő adatvédelmi szint biztosításának egyik lehetséges eszközét.

Az **uniós jog** értelmében a személyes adatok továbbítása harmadik országba vagy nemzetközi szervezetnek akkor megengedett, ha az adatkezelő vagy adatfeldolgozó megfelelő garanciákat nyújtott, és csak azzal a feltétellel, hogy az érintettek számára érvényesíthető jogok és hatékony jogorvoslati lehetőségek állnak rendelkezésre.[685] Az elfogadható „megfelelő garanciák" listáját az uniós adatvédelmi törvény tartalmazza. Megfelelő garanciák a következők révén biztosíthatók:

- közhatalmi vagy egyéb, közfeladatot ellátó szervek közötti, jogilag kötelező erejű, kikényszeríthető jogi eszköz;
- kötelező erejű vállalati szabályok;
- a felügyeleti hatóság vagy a Bizottság által elfogadott általános adatvédelmi feltételek;
- magatartási kódexek;
- tanúsítási mechanizmusok.[686]

683 Bővebb információért lásd az Európai Bizottság weboldalán az EU–USA adatvédelmi pajzsról szóló részt.

684 Európai Bizottság, A Bizottság jelentése az Európai Parlamentnek és a Tanácsnak az EU–USA adatvédelmi pajzs működésének első éves felülvizsgálatáról COM(2017) 611 final, 2017. október 18.

685 Általános adatvédelmi rendelet, 46. cikk.

686 *Uo.*, 46. cikk (1) bekezdés c), d) pont, (2) bekezdés a), b), e), f) pont, és 47. cikk.

Az adatkezelő vagy az adatfeldolgozó, illetve az adatok harmadik országbeli címzettje közötti testre szabott szerződéses kikötések jelenthetik a megfelelő garanciák nyújtásának másik módját. Ilyen szerződéses kikötéseket azonban engedélyeztetni kell az illetékes felügyeleti hatósággal, mielőtt azokra a személyes adatok továbbítása eszközeként lehetne támaszkodni. Hasonlóan a közhatalmi hatóságok is használhatnak a közigazgatási megállapodásba beillesztendő adatvédelmi rendelkezéseket, feltéve, hogy ezeket a felügyeleti hatóság engedélyezte.[687]

Az **Európa Tanács jogában** egy olyan államba vagy nemzetközi szervezethez irányuló adatáramlás, amely nem részese a Korszerűsített 108. Egyezménynek akkor megengedett, ha biztosított a megfelelő szintű védelem. Ez a következőkkel érhető el:

- az állam vagy nemzetközi szervezet joga; vagy
- jogilag kötelező érvényű dokumentumba beépített eseti vagy általános garanciák.[688]

Szerződéses kikötések alá tartozó adattovábbítás

Az **Európa Tanács joga** és az **uniós jog** egyaránt elismeri az adatokat exportáló adatkezelő és a harmadik országban lévő címzett közötti szerződési feltételeket,mint a címzettnél a megfelelő adatvédelmi szint biztosításának egyik lehetséges eszközét.[689]

Uniós szinten az Európai Bizottság a 29. cikk szerinti munkacsoport segítségével általános adatvédelmi feltételeket dolgozott ki, amelyeket egy bizottsági határozat hivatalosan is a megfelelő adatvédelem bizonyítékának minősített.[690] Mivel a Bizottság határozatai teljes egészében kötelező erejűek a tagállamokban, az adattovábbítás felügyeletével megbízott nemzeti hatóságoknak eljárásaik során el kell ismerniük ezen általános szerződési feltételeket.[691] Ha tehát az adatokat exportáló adatkezelő és a harmadik országbeli címzett megállapodnak és aláírják a szóban forgó feltételeket, ennek elegendő bizonyítékul kell szolgálnia a felügyeleti hatóság

687 *Uo.*, 46. cikk (3) bekezdés.

688 Korszerűsített 108. Egyezmény, 14. cikk (3) bekezdés b) pont.

689 Általános adatvédelmi rendelet, 46. cikk (3) bekezdés; Korszerűsített 108. Egyezmény, 14. cikk (3) bekezdés b) pont.

690 Általános adatvédelmi rendelet, 46. cikk (2) bekezdés b) pont és 46. cikk (5) bekezdés.

691 *Uo.*, 46. cikk (2) bekezdés c) pont; az Európai Unió működéséről szóló szerződés, 288. cikk.

felé a megfelelő biztosítékok meglétére. A *Schrems* ügyben mindazonáltal az EUB azt állapította meg, hogy az Európai Bizottság nem korlátozhatja a nemzeti felügyeleti hatóságok azon hatáskörét, hogy felügyelje a személyes adatok olyan harmadik országba irányuló továbbítását, amely egy bizottsági megfelelőségi határozat alá tartozik.[692] Így tehát a nemzeti hatóságok nem akadályozhatók abban, hogy gyakorolják meglévő hatáskörüket, ideértve a személyes adatok továbbításának felfüggesztésére vagy megtiltására vonatkozó hatáskörüket olyan esetekben, amikor az adattovábbítás sérti az uniós vagy nemzeti adatvédelmi szabályozást, így például, ha az adatátvevő nem tartja tiszteletben az általános szerződési feltételeket.[693]

Az általános adatvédelmi szerződési feltételek megléte az uniós jogi keretrendszerben nem akadályozza meg, hogy az adatkezelők más, eseti, egyedi szerződéses feltételeket határozzanak meg, azzal, hogy ezeket a feltételeket a felügyeleti hatóságoknak jóvá kell hagyniuk.[694] Ezeknek azonban az általános adatvédelmi feltételek által biztosítottal azonos szintű védelmet kell biztosítaniuk. Az eseti feltételek jóváhagyása során a felügyeleti hatóságok kötelesek alkalmazni az egységességi mechanizmust a szabályozói megközelítés Unió egész területén történő egységes alkalmazásának biztosítására.[695] Ezt azt jelenti, hogy az illetékes hatóságnak a feltételekre vonatkozó határozattervezetét közölnie kell az Európai Adatvédelmi Testülettel. Az Európai Adatvédelmi Testület erre vonatkozóan véleményt bocsát ki, és a felügyeleti hatóságnak ezt a véleményt a legmesszebbmenőkig figyelembe kell vennie a határozat véglegesítése során. Amennyiben nem tervezi követni az Európai Adatvédelmi Testület véleményét, elindul az Európai Adatvédelmi Testületen belüli vitarendezési eljárás, és a Testület kötelező érvényű határozatot fogad el.[696]

Az általános szerződési feltételek legfontosabb elemei a következők:

692 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6., 96–98. és 102–105. pont.

693 Az EUB *Schrems* ügyben kialakított álláspontjának figyelembe vétele érdekében a Bizottság módosította az általános szerződési feltételekre vonatkozó határozatát. A Bizottság (EU) 2016/2297 végrehajtási határozata (2016. december 16.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országokba és harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló 2001/497/EK és 2010/87/EU határozatok módosításáról, HL L 344., 2016.12.17.

694 Általános adatvédelmi rendelet, 46. cikk (3) bekezdés a) pont.

695 *Uo.*, 63. cikk és 64. cikk (1) bekezdés e) pont.

696 *Uo.*, 64. cikk és 65. cikk.

- egy harmadik fél kedvezményezettre vonatkozó feltétel, amely lehetővé teszi, hogy az érintettek akkor is gyakorolhassák a szerződéses jogokat, ha maguk nem felek a szerződésben;

- az adatok címzettje vagy az adatátvevő jogvita esetén aláveti magát az adatokat exportáló adatkezelő nemzeti felügyeleti hatósága és/vagy nemzeti bíróságai hatáskörének.

Jelenleg az adatkezelőtől adatkezelőig terjedő adattovábbításokra vonatkozó általános feltételeknek két csomagja létezik, ezek közül választhat az adatokat exportáló adatkezelő.[697] Az adatkezelőtől az adatfeldolgozóig terjedő adattovábbításokra vonatkozóan az általános feltételeknek csak egy csomagja létezik.[698] Ezek az általános szerződési feltételek azonban jelenleg bírósági eljárás tárgyát képezik.

Példa: Miután az EUB érvénytelennek nyilvánította a biztonságos kikötő határozatot,[699] a személyes adatokat nem lehetett a szóban forgó megfelelőségi határozat alapján továbbítani az USA-ba. Miközben halottak voltak a tárgyalások az amerikai hatóságokkal, és függőben volt egy új megfelelőségi határozat elfogadása (amelyre végül 2016. július 12-én került sor),[700] az adattovábbításokra csak másik jogalap alapján kerülhetett sor, például általános szerződési feltételek vagy kötelező vállalati szabályok alapján. Számos vállalat, köztük a Facebook Ireland is (amely ellen a biztonságos kikötő határozat érvénytelenítését eredményező ügy zajlott), általános szerződési feltételekre váltottak, hogy folytathassák az adatok továbbítását az Unióból az USA-ba.

697 Az I. csoportot a Bizottságnak a 95/46/EK irányelv alapján a személyes adatok harmadik országokba irányuló továbbítására vonatkozó általános szerződési feltételekről szóló 2001/497/EK határozatának (2001. június 15.) melléklete tartalmazza, HL L 181., 2001.7.4. A II. csoportot a Bizottságnak a 2001/497/EK határozat módosításáról a személyes adatoknak harmadik országokba irányuló továbbadására vonatkozó alternatív általános szerződési feltételek bevezetéséről szóló 2004/915/EK határozata (2004. december 27.) tartalmazza, HL L 385., 2004.12.29.

698 A 95/46/EK európai parlamenti és tanácsi irányelv alapján a személyes adatok harmadik országbeli adatfeldolgozók részére történő továbbítására vonatkozó általános szerződési feltételekről szóló, 2010. február 5-i 2010/87/EK európai bizottsági határozat, HL L 39., 2010.2.12. E kézikönyv szerkesztésének idején az általános szerződési feltételek alkalmazása az USA-ba irányuló személyes adattovábbítások alapjaként az ír legfelsőbb bíróság előtti eljárás tárgát képezte.

699 EUB, *Maximillian Schrems kontra Data Protection Commissioner* [nagytanács], C-362/14. sz. ügy, 2015. október 6.

700 A Bizottság (EU) 2016/1250 végrehajtási határozata (2016. július 12.) a 95/46/EK európai parlamenti és tanácsi irányelv alapján az EU–USA adatvédelmi pajzs által biztosított védelem megfelelőségéről, HL L 207., 2016.8.1.

M. Schrems panaszt nyújtott be az ír felügyeleti hatósághoz, amelyben kérte, hogy függessze fel az adatok általános szerződési feltételek alapján történő továbbítását az USA-ba. Lényegében azt állította, hogy amikor személyes adatait a Facebook ír leányvállalata továbbítja a Facebook Inc.-hez, és az Egyesült Államokban lévő szerverekre, nincs garancia azok védelmére. A Facebook Inc.-t kötik az amerikai törvények, amelyek kötelezhetik, hogy adja át a személyes adatokat az amerikai bűnüldözési hatóságoknak, és az európai egyének számára nincs jogorvoslati lehetőség, hogy megtámadják ezt a gyakorlatot.[701] Ezért az EUB arra a következtetésre jutott, hogy a biztonságos kikötő határozat érvénytelen, és mivel a bíróság ítélete a szóban forgó határozat vizsgálatára korlátozódott, a felperes úgy gondolta, hogy a felvetett kérdés akkor is helytálló, amikor az adattovábbításra szerződéses feltételek alapján kerül sor. A kézikönyv megírása idején az ügyet az ír legfelsőbb bíróság vizsgálta. A felperes az ügyet nyilvánvalóan az EUB elé szándékozik vinni, ahol meg akarja támadni az Európai Bizottságnak az általános szerződési feltételekre vonatkozó határozatát. Az 5. fejezetben ismertetettek szerint kizárólag ez EUB rendelkezik hatáskörrel arra, hogy érvénytelenné nyilvánítsson egy uniós eszközt.

Kötelező erejű vállalati szabályok alá tartozó adattovábbítás

Az **uniós jog** lehetővé teszi továbbá a személyes adatok kötelező erejű vállalati szabályok alapján történő továbbítását olyan nemzetközi adattovábbítás esetén, amelyre azonos vállalatcsoporton belül vagy olyan vállalkozások között kerül sor, amelyek közös gazdasági tevékenységet folytatnak.[702] Mielőtt a személyes adatok továbbításának eszközeként kötelező erejű vállalati szabályokra lehetne támaszkodni, az illetékes felügyeleti hatóságnak az egységességi mechanizmusnak megfelelően jóvá kell azokat hagynia.

Ahhoz, hogy a kötelező erejű vállalati szabályokat jóváhagyják, azoknak jogilag kötelező érvényűnek kell lenniük, valamennyi lényeges adatvédelmi elvre ki kell terjedniük, és a csoport valamennyi tagjára vonatkozniuk kell, illetve valamennyi tagnak érvényesíteni kell azokat. Kifejezetten érvényesíthető jogokkal kell felruházniuk az érintetteket, tartalmazniuk kell valamennyi lényeges adatvédelmi elvet, és meg meg kell felelniük bizonyos formális követelményeknek, például tartalmazniuk

701 Bővebb információért lásd: Maximilian Schrems 2015. december 1-jén az ír adatvédelmi biztoshoz benyújtott, a Facebook Ireland Ltd elleni felülvizsgált panasza.

702 Általános adatvédelmi rendelet, 47. cikk.

kell a vállalkozás szervezeti felépítését, az adattovábbítások ismertetését és, hogy miként alkalmazzák az adatvédelmi elveket. Ebbe beletartozik az is, hogy az érintetteket tájékoztatják ezekről. A kötelező erejű vállalati szabályoknak többek között részletezniük kell az érintettek személyes jogait és a felelősségre vonatkozó rendelkezéseket a szabályok megsértése esetén.[703] A kötelező erejű vállalati szabályok jóváhagyásakor a felügyeleti hatóságok együttműködése tekintetében életbe lép az egységességi mechanizmus (lásd az 5. fejezetet).

Az egységességi mechanizmus keretében a fő felügyeleti hatóság felülvizsgálja a javasolt kötelező erejű vállalati szabályokat, egy határozattervezetet fogad el, és tájékoztatja arról az Európai Adatvédelmi Testületet. A Testület egy véleményt bocsát ki az ügyről, és a fő felügyeleti hatóság hivatalosan jóváhagyhatja a kötelező erejű vállalati szabályokat, miközben a „lehető legnagyobb mértékben" figyelembe veszi a Testület véleményét. Ez a vélemény jogilag nem kötelező, azonban ha a felügyeleti hatóság figyelmen kívül szándékozik hagyni azt, elindul egy vitarendezési mechanizmus, és a Testületet fel kell hívni egy jogilag kötelező erejű határozat elfogadására – tagjainak kétharmados többségével.[704]

Az **Európa Tanács jogában** a jogilag kötelező erejű dokumentumokban beágyazott eseti vagy általános garanciák[705] szintén tartalmaznak kötelező erejű vállalati szabályokat.

7.3.3 Kivételes esetekben biztosított eltérések

Az **uniós jogban** a személyes adatok harmadik országba történő továbbítása még megfelelőségi határozat vagy garanciák, például általános szerződési feltételek vagy kötelező erejű vállalati szabályok hiányában is indokolt lehet a következő körülmények valamelyikének fennállása esetén:

- az érintett kifejezett hozzájárulását adta az adattovábbításhoz;
- az érintett és az adatkezelő szerződést köt – vagy tervez kötni –, és az adatok külföldre történő továbbítása a szerződés teljesítéséhez szükséges;

703 Részletesebb leírásért lásd az általános adatvédelmi rendelet 47. cikkét.

704 *Uo.*, 57. cikk (1) bekezdés s) pont, 58. cikk (1) bekezdés j) pont, 64. cikk (1) bekezdés f) pont, 65. cikk (1) és (2) bekezdés.

705 Korszerűsített 108. Egyezmény, 14. cikk (3) bekezdés b) pont.

- szerződés megkötése az adatkezelő és egy harmadik fél között az érintett érdekében;
- fontos közérdek miatt;
- jogi követelések létrejötte, érvényesítése vagy védelme miatt;
- az érintett létfontosságú érdekeinek védelme miatt;
- az adatok nyilvános nyilvántartásból történő továbbítása miatt (ez a nyilvánosság azon érdekét szolgálja, hogy hozzáférhessenek a nyilvános nyilvántartásokban tárolt adatokhoz).[706]

Ha egyik fenti feltétel sem teljesül, és az adattovábbítás nem alapulhat a megfelelőségi határozaton vagy megfelelő garanciákon, adattovábbítás csak akkor történhet, ha az adattovábbítás nem ismétlődő, csak korlátozott számú érintettre vonatkozik, az adatkezelő olyan kényszerítő erejű jogos érdekében szükséges, amely érdekhez képest nem élveznek elsőbbséget az érintett jogai.[707] Ezekben az esetekben az adatkezelőnek meg kell vizsgálnia az adattovábbítás körülményeit, és garanciákat kell biztosítania. Az adatkezelőnek tájékoztatnia kell a felügyeleti hatóságot és az érintett személyeket az adattovábbításról és az azt indokoló jogos érdekről.

Az a tény, hogy az eltérésekhez csak végső esetben lehet folyamodni jogszerű adattovábbítás esetén[708] (csak megfelelőségi határozat hiányában és akkor alkalmazhatók, ha nincsenek egyéb garanciák) hangsúlyozza kivételes jellegüket, és ezt az általános adatvédelmi rendelet preambulumbekezdései[709] részletesebben kiemelik. Mint ilyen, az eltérések hozzájárulás alapján lehetőséget jelentenek az adatok továbbítására „bizonyos körülmények esetén", és ha az adattovábbítás „alkalomszerű, és valamely szerződéssel vagy jogi igénnyel kapcsolatban válik szükségessé"[710].

Ráadásul a 29. cikk szerinti munkacsoport iránymutatása szerint meghatározott kivételes esetekben biztosított eltérésekre csak kivételes, eseti esetekben szabad

706 Általános adatvédelmi rendelet, 49. cikk.

707 *Uo.*

708 *Uo.*, 49. cikk (1) bekezdés.

709 Lásd: általános adatvédelmi rendelet, 49. cikk (1) bekezdés a)–b) pont és (113) preambulumbekezdés.

710 *Uo.*, 49. cikk (1) bekezdés.

hagyatkozni, és nem szabad azokat tömeges vagy ismétlődő adattovábbításokra használni.[711] Az európai adatvédelmi biztos kiemelte a 45/2001 rendelet keretében végzett adattovábbítások jogalapjaként használt eltérések kivételes jellegét, és megjegyezte, hogy ez a megoldás csak „korlátozott esetekben" és „alkalmi továbbításoknál" alkalmazható.[712]

Példa: Egy egyesült államokbeli székhellyel rendelkező globális értékesítési rendszert (GDS) szolgáltató vállalat online foglalási rendszert kínál több légitársaság, hotel és hajókörutat kínáló társaság számára világszerte, ezzel több tíz millió személy adatát kezeli az EU-ban. Ahhoz, hogy az adatokat először továbbítsa az USA-ban lévő szervereire, a GDS vállalat az adattovábbítás jogalapjaként egy eltérésre támaszkodik, mégpedig arra, hogy az szerződéskötéshez szükséges. Így tehát nem hoz fel egyéb garanciát az Európából származó és az USA-ba továbbított, majd világszerte hoteleknek ismételten szétosztott személyes adatok tekintetében (ami azt jelenti, hogy a későbbi adattovábbítások tekintetében sincs semmilyen garancia). A GDS vállalat nem felel meg az általános adatvédelmi rendeletnek a jogszerű nemzetközi adattovábbításra vonatkozó követelményeinek, mivel tömeges adattovábbításokra jogalapként egy eltérést alkalmaz.

Hacsak nincs egy megfelelőségi határozat érvényben, az EU és tagállamai jogosultak fontos közérdekre hivatkozva korlátozni a személyes adatok bizonyos kategóriáinak harmadik országba történő továbbítását, még akkor is, ha az adattovábbítás egyéb feltételei teljesülnek. Ezeket a korlátozásokat kivételnek kell tekinteni, és a tagállamok kötelesek tájékoztatni a Bizottságot a vonatkozó rendelkezésekről.[713]

Az **Európa Tanács joga** a következő esetekben lehetővé teszi az adatoknak a megfelelő adatvédelemmel nem rendelkező területekre történő továbbítását:

- az érintett hozzájárulását adta;
- az érintett létfontosságú érdekei teszik szükségessé a továbbítást;

711 29. cikk szerinti munkacsoport, *Munkadokumentum a 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről*, 1995. október 24., WP 114, Brüsszel, 2005. november 25.

712 Európai adatvédelmi biztos, *Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies*, Brüsszel, 2014. július 14., 15. o.

713 Lásd: általános adatvédelmi rendelet, 49. cikk (5) bekezdés.

- jogos, magasabb érdekek miatt, különösen fontos közérdekből, vagy jogszabály rendelkezik róla;

- egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül.[714]

7.3.4 Adattovábbítás nemzetközi megállapodások alapján

Az EU köthet harmadik országokkal a személyes adatok meghatározott célból történő továbbítását szabályozó nemzetközi megállapodásokat. Ezeknek a megállapodásoknak megfelelő garanciákat kell tartalmazniuk a szóban forgó egyének személyes adatainak biztosítása érdekében. Az általános adatvédelmi rendelet nem érinti e nemzetközi megállapodásokat.[715]

A tagállamok köthetnek nemzetközi megállapodásokat olyan harmadik országokkal vagy nemzetközi szervezetekkel is, amelyek megfelelő szintű védelmet biztosítanak az egyének alapjogai és szabadságai tekintetében, amennyiben e megállapodások nem érintik az általános adatvédelmi rendelet alkalmazását.

Egy hasonló szabályról rendelkezik a Korszerűsített 108. Egyezmény 12. cikke (3) bekezdésének a) pontja.

A személyes adatok továbbítását érintő nemzetközi megállapodásokra jó példa az utasnyilvántartási adatállományokra (PNR) vonatkozó megállapodások.

Utasnyilvántartási adatállományok

PNR adatokat légitársaságok gyűjtenek a járatfoglalási eljárás során és többek között ezen adatok közé a légi utasok neve, címe, hitelkártya-adatai és ülésszáma tartozik. A légi fuvarozók saját kereskedelmi céljaikból is gyűjtik ezeket az adatokat. Az EU bizonyos harmadik országokkal (Ausztrália, Kanada és az USA) megállapodást kötött a PNR adatok továbbítására súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében. Az Unió 2016-ban

714 Korszerűsített 108. Egyezmény, 14. cikk (4) bekezdés.

715 Általános adatvédelmi rendelet, (102) preambulumbekezdés.

elfogadta az EU-PNR irányelvként is ismert (EU) 2016/861 irányelvet[716]. Ez az irányelv biztosítja a jogi keretrendszert az uniós tagállamok számára a PNR adatok továbbításához más harmadik ország illetékes hatóságainak, hasonlóképpen a súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében. A PNR adatok továbbítása harmadik ország hatóságainak eseti alapon történik, és egyéni elbírálás tárgyát képezi, hogy az adattovábbítás szükséges-e az irányelvben meghatározott célból, és azzal a feltétellel, hogy az alapjogokat tiszteletben kell tartani.

Az EU és harmadik országok közötti PNR megállapodásoknak az EU Alapjogi Chartájában biztosított magánélethez és az adatvédelemhez való alapjogokkal való összeegyezethetőségét vitatták. Amikor 2014-ben a – Kanadával folytatott tárgyalásokat követően – az EU aláírt egy megállapodást a PNR adatok továbbításáról és kezeléséről, az Európai Parlament úgy döntött, hogy az ügyet az EUB elé viszi, hogy a bíróság megvizsgálja a megállapodás jogszerűségét az uniós jog, különösen a Charta 7. és 8. cikke tekintetében

Példa: Az EU és Kanada közötti PNR-megállapodás jogszerűségére vonatkozó véleményében[717] a Bizottság megállapította, hogy a tervezett megállapodás a jelenlegi formájában nem összeegyeztethető a Chartában elismert alapjogokkal, és ezért a megállapodás nem köthető meg. Mivel személyes adatok kezelését érintette, beavatkozásnak minősült a Charta 8. cikke értelmében védelmet élvező személyes adatok védelméhez való jogba. Ugyanakkor a Charta 7. cikkében rögzített magánélet tiszteletben tartásához való jog korlátozását is jelentette, figyelemmel arra, hogy a PNR-adatok olyan módon összesíthetők és elemezhetők, amely információt szolgáltat az utazási szokásokról, a különböző egyének közötti kapcsolatokról, pénzügyi helyzetükről, étkezési szokásaikról és egészségügyi állapotukról, ily módon pedig ellentétes a magánélet védelmével.

A tervezett megállapodás által előidézett beavatkozás az alapjogokba közérdekű cél elérését szolgálta, mégpedig a közbiztonságot és a terrorizmus és súlyos transznacionális bűnözés elleni küzdelmet. Az EUB azonban

716 Az Európai Parlament és a Tanács (EU) 2016/681 irányelve (2016. április 27.) az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról, HL L 119., 2016.5.4.

717 EUB, *A Bíróság 1/15. sz. véleménye* [nagytanács], 2017. július 26.

emlékeztetett arra, hogy ahhoz, hogy indokolt legyen, a beavatkozásnak szigorúan a követett cél eléréséhez szükséges mértékűre kell korlátozódnia. A rendelkezések elemzését követően az EUB arra a következtetésre jutott, hogy a tervezett megállapodás nem felelt meg a „feltétlenül szükséges" kritériumnak. E következtetés levonásához az EUB többek között a következő tényezőket mérlegelte:

- Azt, hogy a tervezett megállapodás különleges adatok továbbításával járt. A tervezett megállapodás alapján gyűjtött PNR tartalmazhatott különleges adatokat, mint például az utas faji eredetére vagy etnikai hovatartozására, vallásos meggyőződésére vagy egészségügyi állapotára vonatkozó adatok. A különleges adatok továbbítása és kezelése a kanadai hatóságok által kockázatot jelenthetett a megkülönböztetésmentesség elvére, és így a közbiztonságnak a terrorizmus és a súlyos nemzetközi bűncselekmények elleni védelmétől eltérő indokokon alapuló egyértelmű és különösen szilárd igazolást követelt. A tervezett megállapodás nem tudott ilyen indoklást szolgáltatni.[718]

- Az összes utas PNR-adatának folyamatos tárolása öt éven keresztül, még az után is, hogy az utasok elhagyták Kanadát, szintén a feltétlenül szükséges mértéket meghaladónak minősült. Az EUB úgy vélte, hogy a kanadai hatóságok számára meg lehetne engedni, hogy még azt követően is megtartsák azon utasok adatait, akik tekintetében objektív bizonyítékok arra engednek következtetni, hogy fenyegetést jelentenek a közbiztonságra, miután azok elhagyták Kanadát. Ezzel szemben az *összes* olyan utas személyes adatának tárolása, akik tekintetében még csak közvetett bizonyíték sincs arra vonatkozóan, hogy kockázatot jelentenének a közbiztonságra, nem indokot.[719]

A 108. Egyezmény konzultatív bizottsága véleményt adott ki a PNR megállapodások Európa Tanács joga szerinti adatvédelmi vonatkozásairól.[720]

718 *Uo.*, 165. pont.

719 *Uo.*, 204–207. pont.

720 Európa Tanács, *Vélemény az utasnyilvántartási adatállományok feldolgozásának adatvédelmi vonzatairól*, T-PD(2016)18rev, 2016. augusztus 19.

Üzenetadatok

Az európai bankokból kiinduló legtöbb pénzátutalást a belga székhelyű Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) dolgozza fel, amely egyik számítógépközpontjának „tükörképét" az USA-ban működteti; a SWIFT azzal a kéréssel szembesült, hogy terrorizmussal kapcsolatos nyomozás céljából közöljön adatokat az USA Pénzügyminisztériumával.[721]

Uniós szemszögből nézve nem állt rendelkezése kellő jogalap ezeknek a – többségében uniós polgárokra vonatkozó – adatoknak a kiadására az USA-nak egyszerűen azon a jogcímen, hogy a SWIFT egyik adatszolgáltató-feldolgozó központja ott található.

„SWIFT megállapodás" néven 2010-ben külön megállapodás jött létre az EU és az USA között, amelynek célja az volt, hogy megteremtse a szükséges jogalapot, és biztosítsa a megfelelő adatvédelmi előírásokat.[722]

E megállapodás alapján – a terrorizmus vagy a terrorizmus finanszírozásának megakadályozása, kivizsgálása, felderítése, illetve büntetőeljárás alá vonása céljából – a SWIFT által tárolt pénzügyi adatokat továbbra is adnak át az USA Pénzügyminisztériumának. Az USA Pénzügyminisztériuma pénzügyi adatokat kérhet a SWIFT-től, amennyiben a kérés:

- a lehető legpontosabban megjelöli a pénzügyi adatokat;
- egyértelműen megindokolja az adat szükségességét;

721 Lásd ezzel összefüggésben: 29. cikk szerinti munkacsoport (2011), *14/2011. sz. vélemény a pénzmosás és a terrorizmus finanszírozásának megelőzésével kapcsolatos adatvédelmi kérdésekről*, WP 186, Brüsszel, 2011. június 13.; 29. cikk szerinti munkacsoport (2006), *10/2006. sz. vélemény a személyes adatoknak a Nemzetközi Bankközi Pénzügyi Telekommunikációs Társaság (SWIFT) általi kezeléséről*, WP 128, Brüsszel, 2006. november 22.; Belga bizottság a magánélet védelmére (Commission de la protection de la vie privée) (2008), *„Control and recommendation procedure initiated with respect to the company SWIFT scrl"* (A SWIFT scrl tekintetében indított ellenőrzési és ajánlásmegfogalmazási eljárás), határozat, 2008. december 9.

722 A Tanács 2010. július 13-i 2010/412/EU határozata az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról szóló megállapodás megkötéséről, HL L 195., 2010.7.27. A megállapodás szövegét csatolták e határozathoz, HL L 195., 2010.7.27.

- megfogalmazása a lehető legpontosabb annak érdekében, hogy a kért adatok mennyisége a lehető legkisebb legyen;

- nem az egységes eurofizetési térséget (SEPA) érintő adat megszerzésére irányul.[723]

Az Europolnak az USA Pénzügyminisztériuma által benyújtott minden kérésből kapnia kell egy példányt, és ellenőriznie kell, hogy betartják-e a SWIFT-megállapodás elveit.[724] Ha megerősíti, hogy igen, a SWIFT-nek közvetlenül az USA Pénzügyminisztériuma részére kell átadnia a pénzügyi adatokat. A minisztériumnak a pénzügyi adatokat biztonságos fizikai környezetben kell tárolnia, ahol kizárólag a terrorizmust vagy annak finanszírozását vizsgáló elemzők férhetnek hozzájuk, és a pénzügyi adatok nem kapcsolhatók össze más adatbázisokkal. Általában a SWIFT-től kapott adatokat legkésőbb öt évvel a kézhezvételt követően törölni kell. A konkrét nyomozáshoz vagy büntetőeljáráshoz lényeges pénzügyi adatok csak az adott nyomozáshoz vagy büntetőeljáráshoz szükséges ideig megőrizhetők.

Az USA Pénzügyminisztériuma a SWIFT által kapott adatokból származó információkat egyesült államokbeli vagy az USA-n kívüli, bűnüldözéssel, közbiztonsággal vagy terrorizmus elleni küzdelemmel foglalkozó hatóságoknak továbbíthatja – csakis a terrorizmus vagy a terrorizmus finanszírozásának megakadályozása, kivizsgálása, felderítése, illetve büntetőeljárás alá vonása céljából. Ha a pénzügyi adatok harmadik fél részére történő továbbítása uniós tagállam állampolgárát vagy lakosát érinti, az információ harmadik ország hatóságának való bármely továbbadása az érintett tagállam illetékes hatóságainak előzetes hozzájárulásával történhet. Kivétel megállapítható, ha az adat továbbadása a közbiztonságot közvetlenül és súlyosan fenyegető veszély elhárításához elengedhetetlenül szükséges.

A SWIFT-megállapodás elveinek betartását független ellenőrök – köztük az Európai Bizottság által kinevezett személy – ellenőrzik. Lehetőségük van valós időben és visszamenőlegesen ellenőrizni a szolgáltatott adatok tekintetében végzett kereséseket, kiegészítő adatokat bekérni annak igazolására, hogy összefüggésbe hozhatók-e ezek a keresések a terrorizmussal, és a hatóság zárolhatja a keresések némelyikét vagy akár az összes olyan keresést, amelyek úgy tűnnek, hogy sértik a megállapodásban rögzített garanciákat.

723 *Uo.*, 4. cikk (2) bekezdés.

724 Az Europol Közös Ellenőrző Hatósága ellenőrizte az Europol tevékenységét ezen a területen.

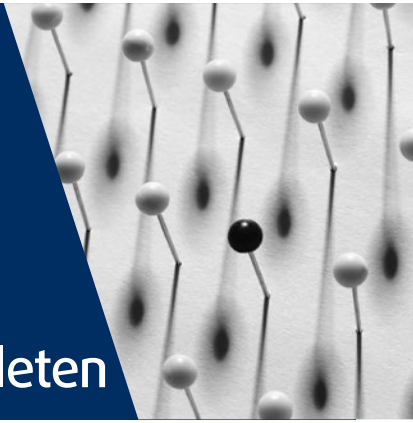
Az érintetteknek joguk van ahhoz, hogy az illetékes uniós felügyeleti hatóságtól megerősítést kapjanak arról, hogy személyes adataik védelméhez fűződő jogaikat tiszteletben tartották. Az érintettek a SWIFT-megállapodás alapján az USA Pénzügyminisztériuma által gyűjtött és tárolt adataik helyesbítését, törlését vagy zárolását is kérhetik. Az érintettek hozzáférési joga azonban bizonyos jogszabályi korlátozások alá eshet. Ha a hozzáférést megtagadják, az érintettet írásban tájékoztatni kell az elutasításról, valamint az USA-ban igénybe vehető közigazgatási és bírósági jogorvoslati lehetőségekről.

A SWIFT megállapodás öt évig érvényes, érvényességének első időszaka 2015 augusztusában járt le. Automatikusan mindig további egy (1) évvel meghosszabbodik, kivéve, ha valamelyik fél a másikat írásban, legalább hat (6) hónappal korábban azon szándékáról értesíti, hogy a megállapodás hatályát meghosszabbítani nem kívánja. Az automatikus meghosszabbítást 2015, 2016 és 2017 augusztusában alkalmazták, és ezek a SWIFT megállapodás legalább 2018 augusztusáig tartó érvényességét biztosítják.[725]

725 Megállapodás az Európai Unió és az Amerikai Egyesült Államok között az Európai Unióból származó pénzügyi üzenetadatoknak a terrorizmus finanszírozásának felderítését célzó program céljából történő feldolgozásáról és az Amerikai Egyesült Államok részére való átadásáról, 23. cikk (2) bekezdés.

8

Adatvédelem a rendőrségi és büntető igazságszolgáltatási területen



EU	Tárgyalt kérdések	Európa Tanács
A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv	Általánosságban	Korszerűsített 108. Egyezmény
	Rendőrség	Rendőrségi ajánlás Gyakorlati útmutató a személyes adatok bűnüldöző szektorban történő felhasználásához
	Felügyelet	EJEB, *B.B. kontra Franciaország*, 5335/06. sz. ügy, 2009 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008 EJEB, *Allan kontra Egyesült Királyság*, 48539/99. sz. ügy, 2002 EJEB, *Malone kontra Egyesült Királyság*, 8691/79. sz. ügy, 1984 EJEB, *Klass és társai kontra Németország*, 5029/71. sz. ügy, 1978 EJEB, *Szabó és Vissy kontra Magyarország*, 37138/14. sz. ügy, 2016 EJEB, *Vetter kontra Franciaország*, 59842/00. sz. ügy, 2005

EU	Tárgyalt kérdések	Európa Tanács
	Számítástechnikai bűnözés	A számítástechnikai bűnözéssel szembeni egyezmény
Egyéb speciális jogi eszközök		
Prümi határozat	**A különleges adatok vonatkozásában: ujjlenyomatok, DNS, huliganizmus, légi utasokat érintő információk, telekommunikációs adatok, stb.**	Korszerűsített 108. Egyezmény, 6. cikk Rendőrségi ajánlás, Gyakorlati útmutató a személyes adatok bűnüldöző szektorban történő felhasználásához
Svéd kezdeményezés (a Tanács 2008/977/IB kerethatározata)	**Az információk és bűnüldözési operatív információk cseréjének egyszerűsítése a bűnüldöző hatóságok között**	EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008
(EU) 2016/681 irányelv az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról EUB, *Digital Rights Ireland* és *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014 EUB, *Tele2 Sverige* és *Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016	**A személyes adatok megőrzése**	EJEB, *B.B. kontra Franciaország*, 5335/06. sz. ügy, 2009
Europol-rendelet Eurojust-határozat	**Szakügynökségek részéről**	Rendőrségi ajánlás
Schengen II határozat VIS-rendelet Eurodac-rendelet VIR-határozat	**Speciális közös információs rendszerek által**	Rendőrségi ajánlás EJEB, *Dalea kontra Franciaország*, 964/07. sz. ügy, 2010

Az egyén adatvédelemhez fűződő érdekei és a társadalomnak – a bűnözés elleni küzdelem és a nemzet- és közbiztonság biztosítása okán – az adatgyűjtéshez fűződő érdekei közötti egyensúly megteremtése érdekében az Európa Tanács és az EU egyedi jogi aktusokat fogadott el. Ez a szakasz egy áttekintést nyújt az Európa Tanács (8.1 szakasz) és az EU (8.2 szakasz) jogáról a rendőrségi és büntető igazságszolgáltatási területen megvalósuló adatvédelemmel kapcsolatban.

8.1 Az Európa Tanács joga a rendőrségi és büntető igazságszolgáltatási területen megvalósuló adatvédelemmel és nemzetbiztonsággal kapcsolatban

Főbb pontok

- A Korszerűsített 108. Egyezmény és az Európa Tanács rendőrségi ajánlása a rendőrségi munka valamennyi területének adatvédelmi vonatkozásaira érvényes.
- A számítástechnikai bűnözéssel szembeni egyezmény (Budapesti egyezmény) kötelező erejű nemzetközi jogi aktus, amely az elektronikus hálózatok ellen, illetve segítségével elkövetett bűncselekményekkel foglalkozik. Vonatkozik továbbá az elektronikus bizonyítékokat érintő nem számítógépes bűnözésre is.

Az Európa Tanács és az EU joga közötti egyik fontos különbség az, hogy az **Európa Tanács joga**, az uniós joggal szemben a nemzetbiztonsági területre is vonatkozik. Ez azt jelenti, hogy a részes feleknek az EJEE 8. cikkének alkalmazási körén belül kell maradnia még a nemzetbiztonsággal kapcsolatos tevékenységek esetén is. Az EJEB számos ítélete foglalkozik a nemzetbiztonsági jog és gyakorlat érzékeny területein tett állami intézkedésekkel.[726]

A rendőrségi és büntető igazságszolgáltatási terület vonatkozásában Európai szinten a Korszerűsített 108. Egyezmény a személyesadat-kezelés valamennyi területét érinti, és rendelkezései általánosságban a személyes adatok kezelését kívánják szabályozni. Következésképpen a Korszerűsített 108. Egyezmény vonatkozik

726 Lásd például: EJEB, *Klass és társai kontra Németország*, 5029/71. sz. ügy, 1978. szeptember 6.; EJEB, *Rotaru kontra Románia* [Nagykamara], 28341/95. sz. ügy, 2000. május 4.; és EJEB, *Szabó és Vissy kontra Magyarország*, 37138/14. sz. ügy, 2016. január 12.

a rendőrségi és büntető igazságszolgáltatási területen megvalósuló adatvédelemre. A genetikai adatok, a bűncselekményekkel, büntetőeljárással és a büntetőítéletekkel kapcsolatos személyes adatok kezelése, valamint a kapcsolódó biztonsági intézkedések, valamely személyt egyedileg azonosító biometrikus adatok, valamint a különleges adatok kezelése csak akkor megengedett, ha megfelelő garanciák vannak érvényben az ilyen adatok kezelése által az érintett érdekeire, jogaira és alapvető szabadságaira jelentett kockázatok ellen, nevezetesen a diszkrimináció kockázata ellen.[727]

A rendőrségi és igazságszolgáltatási hatóságok jogszabályi feladataihoz gyakran van szükség személyes adatok feldolgozására, ami súlyos következményekkel járhat az érintett egyénekre nézve. Az Európa Tanács által 1987-ben elfogadott rendőrségi ajánlás iránymutatást ad a részes feleknek arról, hogy milyen módon kell megvalósítaniuk a 108. Egyezménynek a rendőri szervek általi személyesadat-kezeléssel kapcsolatos alapelveit.[728] Az ajánlást a személyes adatok bűnüldöző szektorban történő felhasználásáról szóló, 108. Egyezmény konzultatív bizottsága által elfogadott gyakorlati útmutató egészítette ki.[729]

Példa: A *D.L. kontra Bulgária* ügyben[730] a szociális szolgáltatások keretében a felperest egy bírósági végzés alapján bentlakásos nevelőintézetben helyezték el. Az összes írásos kommunikáció és telefonos beszélgetés általános és válogatás nélküli megfigyelés tárgyát képezte. Az EJEB azt állapította meg, hogy megsértették a 8. cikket, figyelemmel arra, hogy a szóban forgó intézkedés nem volt szükséges egy demokratikus társadalomban. A Bíróság kimondta, hogy mindent meg kell tenni annak érdekében, hogy az intézetben elhelyezett kiskorúak megfelelően tudjanak kapcsolatot tartani a külvilággal, mivel az szerves részét képezi a méltó bánásmódhoz fűződő joguknak, és teljes mértéken elengedhetetlen volt a társadalomba történő visszaintegrálásuk előkészítéséhez. Ez vonatkozott épp úgy a látogatásokra, mint az írásos kommunikációra vagy telefonbeszélgetésekre. Továbbá, a megfigyelés nem tett különbséget a családtagokkal folytatott kommunikáció és a gyermek jogait képviselő

727 Korszerűsített 108. Egyezmény, 6. cikk

728 Európa Tanács, Miniszteri Bizottság (1987), Rec(87)15. sz. ajánlás a tagállamoknak a személyes adatok rendőri ágazatban való felhasználásának szabályozásáról, 1987. szeptember 17.

729 Európa Tanács, a 108. Egyezmény konzultatív bizottsága (2018), Gyakorlati útmutató a személyes adatok bűnüldöző szektorban történő felhasználásához, T-PD(2018)1.

730 EJEB, *D.L. kontra Bulgária*, 7472/14. sz. ügy, 2016. május 19.

civilszervezettel vagy ügyvédekkel folytatott kommunikáció között. Ráadásul a kommunikáció lehallgatását elrendelő határozat nem az adott eset egyedi elemzésén alapult.

Példa: A *Dragojević kontra Horvátország* ügyben[731] a felperest kábítószer kereskedelemben való részvétellel gyanúsították. Bűnösnek találták, miután egy vizsgálóbíró engedélyezte titkos megfigyelési eszközök alkalmazását a felperes telefonhívásainak lehallgatásához. Az EJEB azt állapította meg, hogy az intézkedés, amely ellen panaszt emeltek, beavatkozásnak minősült a magánélet tiszteletben tartásához és a kapcsolattartáshoz való jogba. A vizsgálóbíró által adott engedély pusztán az ügyészség azon kijelentésén alapult, hogy „a nyomozás más eszközökkel nem volt megvalósítható". Az EJEB az is megállapította, hogy a büntetőbíróságok vizsgálatukat a megfigyelési eszközök használatára korlátozták, és a kormány nem tett javaslatot rendelkezésre álló jogorvoslati lehetőségekre. Következésképpen megsértették a 8. cikket.

8.1.1 A rendőrségi ajánlás

Az EJEB állandó ítélkezési gyakorlatából kitűnik, hogy a személyes adatok rendőri vagy nemzetbiztonsági hatóságok általi tárolása és megőrzése az EJEE 8. cikkének (1) bekezdésébe ütközik. Az EJEB számos ítélete foglalkozik az ilyen beavatkozás indokoltságával.[732]

Példa: A *B.B. kontra Franciaország* ügyben [733] a felperest bizalmi helyzetben lévő személyként 15 éves kiskorúak terhére elkövetett szexuális bűncselekmények miatt ítélték el. Börtönbüntetését 2000-ben töltötte le. Egy évvel később kérte, hogy a bűnügyi nyilvántartásból töröljék az ítéletére vonatkozó adatokat, azonban kérését elutasították. 2004-ben egy francia törvény létrehozott egy szexuális bűncselekmény miatt elítélt személyeket tartalmazó nemzeti igazságszolgáltatási adatbázist, és a felperest tájékoztatták az adatbázisba való felvételéről. Az EJEB azt állapította meg, hogy egy szexuális bűncselekmény miatt elítélt személynek

731 EJEB, *Dragojević kontra Horvátország*, 68955/11. sz. ügy, 2015. január 15.

732 Lásd például: EJEB, *Leander kontra Svédország*, 9248/81. sz. ügy, 1987. március 26.; EJEB, *M.M. kontra Egyesült Királyság*, 24029/07. sz. ügy, 2012. november 13.; EJEB, *M.K. kontra Franciaország*, 19522/09. sz. ügy, 2013. április 18.; vagy EJEB, *Aycaguer kontra Franciaország*, 8806/12. sz. ügy, 2017. június 22.

733 EJEB, *B.B. kontra Franciaország*, 5335/06. sz. ügy, 2009. december 17.

egy nemzeti igazságszolgáltatási adatbázisban való szerepeltetése az EJEE 8. cikkének hatálya alá tartozik. Figyelemmel azonban arra, hogy megfelelő adatvédelmi biztosítékokat alkalmaztak – köztük azt, hogy az érintett kérheti az adatok törlését, továbbá az adatok tárolásának ideje és az adatokhoz való hozzáférés korlátozott –, megteremtették a megfelelő egyensúlyt a versengő magán- és közérdekek között. A Bíróság arra a következtetésre jutott, hogy nem sértették meg az EJEE 8. cikkét.

Példa: Az *S. és Marper kontra Egyesült Királyság* ügyekben[734] mindkét felperest bűncselekményekkel vádolták meg, de egyiket sem ítélték el. Ennek ellenére a rendőrség megtartotta és tárolta ujjlenyomataikat, sejtmintáikat és DNS-profiljukat. Törvény engedélyezte a fenti biometrikus adatok korlátlan megőrzését, ha valakit bűncselekménnyel gyanúsítottak – még akkor is, ha a gyanúsítottat a későbbiekben felmentették vagy szabadlábra helyezték. Az EJEB megállapította, hogy a személyes adatok válogatás nélküli, általános megőrzése, amely időben nem korlátozott és a felmentett egyénnek csekély lehetősége van arra, hogy kérje az adatok törlését, aránytalan beavatkozásnak minősül a felperesek magánélet tiszteletben tartásához való jogába. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Az elektronikus kommunikációval kapcsolatos egyik döntő fontosságú kérdés a hatóság magánélethez és adatvédelemhez való jogokba történő beavatkozásának kérdése. A kommunikáció megfigyelésére vagy elfogására szolgáló eszközök, köztük a lehallgató készülékek használata csak abban az esetben engedhető meg, amennyiben azt törvény írja elő, és egy demokratikus társadalomban az alábbiak érdekében szükséges intézkedésnek minősül:

- nemzetbiztonsági védelem;
- közbiztonság;
- az állam pénzügyi érdekei;
- bűncselekmények visszaszorítása; vagy

734 EJEB, *S. és Marper kontra Egyesült Királyság* [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4., 119. és 125. pont.

- az érintett vagy mások jogainak és szabadságainak védelme.

Az EJEB számos további ítélete foglalkozik a magánélethez fűződő jogba megfigyeléssel való beavatkozás indokoltságával.

Példa: Az *Allan kontra az Egyesült Királyság* ügyben[735] a hatóságok titokban felvételt készítettek egy fogvatartottnak a börtönben őt meglátogató barátjával, valamint az ugyanabban a cellában lakó rabtársával folytatott magánbeszélgetéseiről. Az EJEB megállapította, hogy az audio- és videokészülékeknek a felperes cellájában, a börtönbeli látogatóteremben és a rabtárson való elhelyezése és használata beavatkozásnak minősül a felperes magánélethez való jogába. Mivel a rejtett felvevőkészülékek rendőrség általi használatát az adott időben törvényi rendszer nem szabályozta, a beavatkozás nem felelt meg a jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: A *Roman Zakharov kontra Oroszország* ügyben[736] a felperes bírósági eljárást indított három mobilszolgáltató ellen. Azzal érvelt, hogy a telefonbeszélgetések tekintetében megsértették a magánélethez való jogát, mivel a szolgáltatók egy berendezést telepítettek, ami lehetővé tette a szövetségi biztonsági szolgálat számára, hogy előzetes bírósági engedély nélkül lehallgassa a telefonbeszélgetéseit. Az EJEB megállapította, hogy a kommunikáció lehallgatását szabályozó belföldi jogszabályok nem biztosítottak megfelelő és hatékony garanciát az önkényességgel és a visszaélés kockázatával szemben A nemzeti jog különösen nem írta elő a tárolt adatok törlését, miután elérték a tárolás célját. Továbbá noha szükség volt bírósági engedélyre, a bírósági felülvizsgálat lehetősége korlátozott volt.

Példa: A *Szabó és Vissy kontra Magyarország* ügyben[737] a felperesek azt állították, hogy a magyar jogszabályok sértik az EJEE 8. cikkét, és nem volt kellően részletes vagy pontos. Továbbá azt állították, hogy a jogszabályok nem biztosítottak megfelelő garanciákat a visszaéléssel és önkényességgel szemben. Az EJEB megállapította, hogy a magyar jog nem írta elő, hogy a megfigyelés bírósági engedélyhez kötött legyen. A Bíróság mindazonáltal megállapította, hogy miközben az igazságügyi minisztérium jóváhagyása

735 EJEB, *Allan kontra Egyesült Királyság*, 48539/99. sz. ügy, 2002. november 5.

736 EJEB, *Roman Zakharov kontra Oroszország* [Nagykamara], 47143/06. sz. ügy, 2015. december 4.

737 EJEB, *Szabó és Vissy kontra Magyarország*, 37138/14. sz. ügy, 2016. január 12.

alá tartozott, ez a felügyelet messzemenően politikai természetű volt, és alkalmatlan volt arra, hogy biztosítsa a „feltétlen szükségesség" követelményét. A nemzeti jog továbbá nem rendelkezett bírósági felülvizsgálatról, figyelemmel arra, hogy az alanyokat nem tájékoztatták. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Mivel a rendőri hatóságok által végzett adatkezelés jelentős hatással lehet az érintett személyekre, különösen szükséges, hogy az ezen a területen érvényben legyenek a személyes adatok kezelésére vonatkozó részletes adatvédelmi szabályok. Az Európa Tanács Rendőrségi Ajánlása igyekezett megoldást találni erre a problémára azzal, hogy iránymutatást adott a következőkre vonatkozóan: a személyes adatok rendőrségi munkához való gyűjtésének módja; az adatok tárolásának módja e területen; ki férhet hozzá ezekhez adatállományokhoz, beleértve a személyes adatok külföldi rendőrségi hatóságoknak való továbbítását; hogyan gyakorolják az érintettek az adatvédelemhez való jogukat; és a független hatóságok miként hajtsák végre az ellenőrzést. Az ajánlás a megfelelő adatbiztonság biztosítására irányuló kötelezettséggel is foglalkozott.

Az ajánlás nem ír elő korlátlan, válogatás nélküli személyes adat gyűjtést a rendőri hatóságok számára. A rendőri hatóságok általi személyesadat-gyűjtést az adatok azon körére korlátozza, amely valós veszély megelőzéséhez vagy egy konkrét bűncselekmény büntetőeljárás alá vonásához szükséges. Minden további adatgyűjtésnek egyedi nemzeti jogszabályon kell alapulnia. A különleges adatok kezelését azon adatokra kell korlátozni, amelyek egy konkrét nyomozással összefüggésben abszolút szükségesek.

Ha az érintett tudomása nélkül kerül sor személyes adatok gyűjtésére, az érintettet tájékoztatni kell az adatgyűjtés tényéről, amint ez a közlés már nem veszélyezteti a nyomozást. A műszaki megfigyeléssel vagy más automatizált módon történő adatgyűjtésnek egyedi jogalappal kell rendelkeznie.

Példa: A *Versini-Campinchi és Crasnianski kontra Franciaország* ügyben[738] a felperes, egy ügyvéd egy ügyfelével folytatott telefonbeszélgetést, akinek a telefonvonalát lehallgatták a vizsgálóbíró kérésére. A beszélgetés átiratából kiderült, hogy az ügyvédnő ügyvédi titoktartás alá tartozó információkat közölt. Az ügyész ezt az információt továbbította az ügyvédi

738 EJEB, *Versini-Campinchi és Crasnianski kontra Franciaország*, 49176/11. sz. ügy, 2016. június 16.

kamara tanácsának, amely megbírságolta a felperest. Az EJEB elismerte a beavatkozást a magánélet és a kapcsolattartás tiszteletben tartásához való jogba, nem csak azon személy vonatkozásában, akinek a telefonját lehallgatták, hanem a felperes esetében is, akinek a beszélgetését lehallgatták és leírták. A beavatkozás a jogszabályokkal összhangban történt és zavarok megelőzésének törvényes célját szolgálta. A felperes elérte a lehallgatott telefonbeszélgetések átirata benyújtása jogszerűségének felülvizsgálatát az ellene indított fegyelmi eljárásban. Annak ellenére, hogy nem sikerült elérnie a telefonbeszélgetés átiratának megsemmisítését, az EJEB úgy vélte, hogy hatékony vizsgálatra került sor, amely alkalmas volt arra, hogy a panaszolt beavatkozást egy demokratikus társadalomban szükséges mértékűre korlátozza. Az EJEB megállapította, hogy az az érv, miszerint az ügyvéd ellen az átirat alapján indított büntetőeljárás „kedvcsökkentő hatással" lenne az ügyvéd és ügyfele közötti kommunikáció szabadságára és ezen keresztül az utóbbi védekezéshez való jogára, nem hiteles olyan esetben, amikor maga az ügyvéd általi információközlés alkalmas arra, hogy az részéről törvénytelen viselkedésnek minősüljön. Következésképpen nem állapította meg a 8. cikk megsértését.

Az Európa Tanács rendőrségi ajánlása rendelkezik arról, hogy a személyes adatok tárolásakor világos különbséget kell tenni a következők között: közigazgatási adatok és rendőrségi adatok; a különböző típusú érintettek adatai, például gyanúsítottak, elítéltek, áldozatok és szemtanúk; valamint a konkrét tényeknek minősülő adatok és a gyanún vagy spekuláción alapuló adatok.

Szigorúan korlátozni kell azon célok körét, amelyekre felhasználhatók a rendőrségi adatok. Ennek következménye van a rendőrségi adatok harmadik felekkel való közlésére is: az ilyen adatok továbbítását vagy közlését a rendőrségi ágazaton belül annak figyelembe vételével kellene szabályozni, hogy fűződik-e jogos érdek az adatok megosztásához. Az ilyen adatok rendőrségi ágazaton kívülre történő továbbítását vagy közlését csak akkor kellene engedélyezni, ha erre vonatkozóan egyértelmű jogszabályi kötelezettség vagy engedély áll fenn.

Példa: A *Karabeyoğlu kontra Törökország* ügyben[739] megfigyelték a felperes, egy bíró telefonvonalait egy illegális szervezetre irányuló bűnügyi nyomozással összefüggésben, mert azt gyanították, hogy a szervezethez

739 EJEB, *Karabeyoğlu kontra Törökország*, 30083/10. sz. ügy, 2016. június 7.

tartozik, vagy, hogy támogatást, illetve segítséget nyújtott annak. Az eljárás megszűnését eredményező határozatot követően a bűnügyi nyomozásért felelős ügyész megsemmisítette a szóban forgó felvételeket. A vizsgálóbíró birtokában maradt azonban egy másolat, aki felhasználta a vonatkozó anyagot a felperes ellen indított fegyelmi eljárásban. Az EJEB megállapította, hogy az idevágó jogszabályt megsértették, mivel az adatokat a gyűjtés céljától eltérő célra használták fel, és azokat nem semmisítették meg a törvényi határidőn belül. A felperes magánélet tiszteletben tartásához fűződő jogába való beavatkozás a fegyelmi eljárást illetően nem volt összhangban a jogszabályokkal.

Nemzetközi továbbításra vagy közlésre kizárólag külföldi rendőri hatóságok részére kerülhet sor, és mindennek külön jogi rendelkezéseken – lehetőleg nemzetközi megállapodásokon – kell alapulnia, kivéve, ha a továbbításra vagy közlésre súlyos és közvetlen veszély kiküszöbölése érdekében van szükség.

A belföldi adatvédelmi jog betartásának biztosítása érdekében a rendőrség általi adatfeldolgozást független felügyelet alá kell helyezni. Az érintetteknek a Korszerűsített 108. Egyezményben foglalt valamennyi hozzáférési joggal rendelkezniük kell. Amennyiben az érintettek hozzáférési jogait a 108. Egyezmény 9. cikke szerint a hatékony rendőrségi nyomozás és büntetőjogi szankciók végrehajtása érdekében korlátozzák, a belföldi jognak biztosítania kell az érintett számára a jogot ahhoz, hogy a nemzeti adatvédelmi felügyeleti hatósághoz vagy egy másik független szervhez fellebbezzen.

8.1.2 A számítógépes bűnözésről szóló Budapesti Egyezmény

Mivel a bűnözői tevékenység egyre növekvő mértékben használ és érint elektronikus adatfeldolgozó rendszereket, e kihívás leküzdéséhez új büntetőjogi rendelkezésekre van szükség. Ezért az Európa Tanács – az elektronikus hálózatok ellen, illetve segítségével elkövetett bűncselekmények kérdésének kezelése céljából – elfogadta a számítógépes bűnözésről szóló egyezményt, azaz a Budapesti Egyezmény néven ismert nemzetközi jogi eszközt.[740] Ez az egyezmény azon országok számára is nyitva áll a csatlakozásra, amelyek nem tagjai az Európa Tanácsnak. 2018 kezdetéig

740 Európa Tanács, Miniszteri Bizottság (2001), A számítógépes bűnözésről szóló egyezmény, CETS 185., Budapest, 2001. november 23., hatálybalépés napja: 2004. július 1.

tizennégy Európa Tanácson kívüli állam[741] vált az egyezmény részes felévé, és hét másik tagsággal nem rendelkező ország kapott meghívást, hogy csatlakozzon.

Továbbra is a számítógépes bűnözésről szóló egyezmény a legbefolyásosabb nemzetközi szerződés, amely az interneten vagy más nemzetközi számítógépes hálózaton elkövetett jogsértésekkel foglalkozik. Arra kötelezi a részes feleket, hogy tegyék naprakésszé és hangolják össze a feltöréssel (hacking) és más biztonsági jogsértésekkel, köztük a szerzői jog megsértésével, a számítógépes csalással, a gyermekpornográfiával és más jogellenes számítástechnikai tevékenységekkel szembeni büntető jogszabályaikat. Az egyezmény eljárási jogköröket is biztosít, amelyek a számítástechnikai bűnözéssel összefüggésben a számítógépes hálózatokon való keresésre és a kommunikáció lehallgatására terjednek ki. Ezenfelül az egyezmény lehetővé teszi a hatékony nemzetközi együttműködést. Az egyezményhez fűzött kiegészítő jegyzőkönyv a számítógépes hálózatokon megjelenő rasszista és idegengyűlölő propaganda büntethetőségével foglalkozik.

Bár az egyezmény nem közvetlenül az adatvédelem előmozdítására irányuló eszköz, bünteti azokat a tevékenységeket, amelyek valószínűleg sértik az érintett saját adatainak védelméhez való jogát. Kötelezi továbbá a részes feleket, hogy fogadjanak el jogszabályi intézkedéseket, hogy lehetővé tegyék nemzeti hatóságaik számára a forgalmi és tartalmi adatok megfigyelését.[742] Ezenkívül kötelezi a részes feleket, hogy végrehajtása során irányozzák elő az emberi jogok és szabadságok megfelelő védelmét, az EJEE által garantált jogokat, köztük az adatvédelemhez való jogot is beleértve.[743] A részes felek nem kötelesek csatlakozni a 108. Egyezményhez azért, hogy csatlakozhassanak a számítógépes bűnözés elleni budapesti egyezményhez.

741 Ausztrália, Kanada, Chile, Kolumbia, a Dominikai Köztársaság, Izrael, Japán, Mauritius, Panama, Szenegál, Sri Lanka, Tonga, Tunézia és az Egyesült Államok. Lásd a 185. Egyezményt aláíró és megerősítő részes feleket bemutató táblázat 2017. júliusi állapotát.

742 Európa Tanács, Miniszteri Bizottság (2001), A számítógépes bűnözésről szóló egyezmény, CETS 185., Budapest, 2001. november 23., 20. és 21. cikk.

743 *Uo.*, 15. cikk (1) bekezdés.

8.2 Az uniós jog a rendőrségi és büntető igazságszolgáltatási területen megvalósuló adatvédelemmel kapcsolatban

Főbb pontok

- Az EU-n belül a rendőrségi és büntető igazságszolgáltatási ágazatban megvalósuló adatvédelem a tagállamok és uniós szereplők nemzeti és határokon átnyúló rendőrségi és büntető igazságszolgáltatási hatóságai általi adatkezeléssel összefüggésben egyaránt szabályozva van.
- Tagállami szinten a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvet kell átültetni a nemzeti jogba.
- Külön jogi eszközök szabályozzák az adatvédelmet a határokon átnyúló rendőrségi és bűnüldözési együttműködés, különösen a terrorizmus és a határokon átnyúló bűncselekmények terén.
- Külön adatvédelmi szabályok léteznek az Európai Rendőrségi Hivatalra (Europol) és az EU Igazságügyi Együttműködési Egységére (Eurojust), valamint az újonnan létrehozott Európai Ügyészségre vonatkozóan, amelyek a határokon átnyúló bűnüldözést segítő és támogató uniós szervek.
- Külön adatvédelmi szabályok léteznek azon közös információs rendszerekre vonatkozóan is, amelyeket uniós szinten az illetékes rendőrségi és igazságszolgáltatási hatóságok közötti, határokon átnyúló információcsere céljából hoztak létre. Fontos példák a Schengeni Információs Rendszer II (SIS II), a Vízuminformációs Rendszer (VIS) és az Eurodac, amely az uniós tagállamok valamelyikében menedékjogot kérő harmadik országbeli állampolgárok és hontalan személyek ujjlenyomatait tartalmazó központi rendszer.
- Az EU-ban folyamatban van a fenti adatvédelmi rendelkezések aktualizálása, hogy azok összhangban legyenek a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv rendelkezéseivel.

8.2.1 A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv

A személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek

védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről[744] szóló (EU) 2016/680 irányelv (a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv) célja, hogy védje a következő büntető igazságszolgáltatási célból gyűjtött és kezelt személyes adatokat:

- bűncselekmények megelőzése, nyomozása, felderítése, üldözése vagy büntetőjogi szankciók végrehajtása – többek között a közbiztonságot fenyegető veszélyekkel szembeni védelem és e veszélyek megelőzése;

- büntetőjogi szankciók végrehajtása; és

- azokban az esetekben, ahol a rendőrség vagy egyéb bűnüldözési hatóság a rá ruházott feladatként a közrend és közbiztonság fenntartása és annak érdekében jár el, hogy védelmet biztosítsanak a közbiztonságot és a jog által védett alapvető társadalmi jogokat fenyegető – esetleg bűncselekmény elkövetéséhez is vezető – veszélyekkel szemben, és megelőzzék e veszélyeket.

A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv védi a büntetőeljárásokban érintett személyek különböző kategóriáinak, így a tanúk, visszaélést bejelentő személyek, áldozatok, gyanúsítottak és bűntársak személyes adatait. A rendőrségi és büntető igazságszolgáltatási hatóságok kötelesek betartani az irányelv rendelkezéseit minden alkalommal, amikor ilyen személyes adatokat kezelnek bűnüldözési célból az irányelv személyi és tárgyi hatálya alatt egyaránt.[745]

Az adatok használata azonban bizonyos feltételek mellett más célokra is megengedett. A személyes adatok gyűjtésének céljától eltérő célból végzett adatkezelés kizárólag akkor megengedett, ha az a nemzeti vagy uniós joggal összhangban van, szükséges és arányos.[746] Egyéb célok tekintetében az általános adatvédelmi rendelet szabályai az irányadók. Az adatmegosztások naplózása és dokumentálása

744 Az Európai Parlament és a Tanács (EU) 2016/680 irányelve (2016. április 27.) a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről, HL L 119., 2016.5.4. (a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv).

745 A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv, 2. cikk (1) bekezdés.

746 *Uo.*, 4. cikk (2) bekezdés.

az illetékes hatóságok külön feladata; ennek célja, hogy segítse a panaszokból fakadó felelősség tisztázását.

A rendőrségi és büntető igazságszolgáltatási területen dolgozó illetékes hatóság közhatalmi szerv vagy nemzeti jog alapján felhatalmazott és közhatalmi jogosítványokat gyakoroló hatóság, amely közhatalmi szerv feladatait látja el,[747] pl. magánbörtönök.[748] Az irányelv alkalmazhatósága kiterjed a hazai szintű adatkezelésre és a tagállamok rendőrségei és igazságszolgáltatási hatóságai közötti határokon átnyúló adatkezelésre, valamint az illetékes hatóságok által harmadik országok és nemzetközi szervezetek felé teljesített nemzetközi adattovábbításokra.[749] Nem terjed ki a nemzetbiztonságra vagy a személyes adatok uniós intézmények, szervek, hivatalok és ügynökségek általi kezelésére.[750]

Az irányelv nagymértékben az általános adatvédelmi rendeletben megfogalmazott elvekre és meghatározásokra támaszkodik, miközben figyelembe veszi a rendőrségi és büntető igazságszolgáltatási terület sajátos jellegét. A felügyeletet ugyanazon tagállami hatóság láthatja el, amely azt az általános adatvédelmi rendelet keretében is gyakorolja. Az irányelv a rendőrségi és büntető igazságszolgáltatási hatóságok új kötelezettségeként vezette be az adatvédelmi tisztviselő kijelölését és adatvédelmi hatásvizsgálat végzését.[751] Bár ezeket az általános adatvédelmi rendelet inspirálta, az irányelv figyelembe veszi a rendőrségi és büntető igazságszolgáltatási hatóságok speciális jellegét. A kereskedelmi célú adatkezeléssel összehasonlítva, amelyet a rendelet szabályoz, a biztonsággal kapcsolatos adatkezelés bizonyos fokú rugalmasságot követelhet meg. Például az, hogy az érintettek azonos szintű védelmet élveznek a tájékoztatáshoz való jog, a saját személyes adataikhoz való hozzáféréshez vagy azok törléséhez való jog tekintetében, mint az általános adatvédelmi rendelet értelmében, azt jelentheti, hogy a bűnüldözési célból végzett megfigyelések a bűnüldözés összefüggésében eredménytelen lehet. Az irányelv ezért nem tartalmazza az átláthatóság elvét. Hasonlóan, az adattakarékosság és a célhoz kötöttség

747 *Uo.*, 3. cikk (7) bekezdés.

748 Európai Bizottság (2016), a Bizottság közleménye az Európai Parlamentnek az Európai Unió működéséről szóló szerződés 294. cikkének (6) bekezdése alapján a személyes adatoknak az illetékes hatóságok által a bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása céljából végzett kezelése tekintetében a természetes személyek védelméről és az ilyen adatok szabad áramlásáról, valamint a 2008/977/IB tanácsi kerethatározat hatályon kívül helyezéséről szóló európai parlamenti és tanácsi rendelet elfogadására vonatkozó tanácsi álláspontról, COM(2016) 213 final, Brüsszel, 2016. április 11.

749 A rendészeti és büntető szervekre vonatkozó igazságszolgáltatási adatvédelmi irányelv, V. fejezet.

750 *Uo.*, 2. cikk (3) bekezdés.

751 *Uo.*, 32. cikk, ill. 27. cikk.

elvét, amelyek előírják, hogy a személyes adatokat kizárólag az adatkezelési cél teljesítéséhez szükséges mértékre kell korlátozni, valamint azt, hogy az adatokat meghatározott és egyértelmű célokból szabad kezelni, szintén rugalmassággal kell alkalmazni a biztonsággal kapcsolatos adatkezeléseknél. Az illetékes hatóságok által egy meghatározott ügyhöz gyűjtött és tárolt adatok rendkívül hasznosak lehetnek jövőbeli ügyek megoldásánál.

Az adatkezelésre vonatkozó elvek

A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv meghatároz néhány kulcsfontosságú garanciát a személyes adatok felhasználására vonatkozóan. Megfogalmazza továbbá ezen adatok kezelését szabályozó elveket. A tagállamok biztosítják, hogy a személyes adatok:

- kezelése jogszerűen és tisztességesen történik;
- gyűjtése csak meghatározott, egyértelmű és törvényes célból történhet, és további kezelésük nem végezhető e célokkal összeegyeztethetetlen módon;
- kezelése célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek;
- pontosak és ahol szükséges, naprakésznek egyenek; minden észszerű intézkedést meg kell tenni annak érdekében, hogy az adatkezelés céljai szempontjából pontatlan személyes adatokat haladéktalanul töröljék vagy helyesbítsék;
- tárolásuk olyan formában történik, amely az érintettek azonosítását csak az adatkezelés céljainak eléréséhez szükséges ideig teszi lehetővé.
- kezelését oly módon kell végezni, hogy a megfelelő technikai vagy szervezési intézkedések alkalmazásával biztosítva legyen a személyes adatok megfelelő biztonsága, az adatok jogosulatlan vagy jogellenes kezelésével, véletlen elvesztésével, megsemmisítésével vagy károsodásával szembeni védelmet is ideértve.[752]

Az irányelv értelmében az adatkezelés csak akkor jogszerű, ha a vonatkozó feladat ellátásához szükséges mértékben történik. Továbbá ezt az illetékes hatóság

752 *Uo.*, 4. cikk (1) bekezdés.

végzi az irányelvben meghatározott célokból, és uniós vagy tagállami jog alapján.[753] Az adatok nem tárolhatók a szükségesnél hosszabb ideig, és bizonyos határidőn belül törölni vagy időszakosan felül kell vizsgálni azokat. Az adatokat csak az illetékes hatóság használhatja, és kizárólag arra a célra, amelyet az adatokat gyűjtötték, továbbították vagy rendelkezésre bocsátották.

Az érintett jogai

Az irányelv megállapítja az érintettek jogait is. Ezek közé tartoznak a következők:

- Tájékoztatáshoz való jog. A tagállamok kötelezik az adatkezelőt, hogy bocsássa az érintett rendelkezésére a következő információkat: 1) az adatkezelő személye és elérhetőségei, 2) az adatvédelmi tisztviselő elérhetőségei, 3) az adatok tervezett kezelésének célja, 4) panaszbenyújtási jog a felügyeleti hatóságnál és a felügyeleti hatóság elérhetőségei 5) az érintett azon joga, hogy kérelmezheti az adatkezelőtől a rá vonatkozó személyes adatokhoz való hozzáférést, azok helyesbítését, törlését vagy kezelésének korlátozását.[754] Ezen általános tájékoztatási kötelezettségen túl az irányelv előírja, hogy egyedi esetekben és jogai gyakorlása érdekében az adatkezelőnek tájékoztatnia kell az érintettet az adatkezelés jogalapjáról és az adatok tárolásának időtartamáról. Ha a személyes adatokat más címzettnek is továbbítja, ideértve a harmadik országokat vagy nemzetközi szervezeteket, az érintettet tájékoztatni kell az ilyen címzettek kategóriáiról. Végezetül pedig az adatkezelők kötelesek minden további tájékoztatást megadni, figyelemmel azon egyedi körülményekre, amelyek között az adatkezelés történik – például amikor az adatgyűjtés titkos megfigyelés keretében történik, vagyis az érintettnek nincs tudomása róla. Ez garantálja az érintett adatainak tisztességes kezelését.[755]

- A személyes adatokhoz való hozzáférés joga. A tagállamok kötelesek biztosítani, hogy az érintett élhessen azon jogával, hogy visszajelzést kapjon arra vonatkozóan, hogy személyes adatainak kezelése folyamatban van-e. Ha személyes adatainak kezelése folyamatban van, jogosult arra, hogy hozzáférést kapjon a kezelés alatt álló adatkategóriához.[756] Ez a jog azonban korlátozható, például azért, hogy ne gördüljenek akadályok nyomozások elé, vagy ne szenvedjen

753 *Uo.*, 8. cikk.

754 *Uo.*, 13. cikk (1) bekezdés.

755 *Uo.*, 13. cikk (2) bekezdés.

756 *Uo.*, 14. cikk.

sérelmet a bűncselekmények tekintetében a vádeljárás lefolytatása, illetve a közbiztonság védelme és mások jogainak és szabadságainak védelme.[757]

- A személyes adatok helyesbítéséhez való jog. A tagállamok kötelesek biztosítani, hogy az érintett indokolatlan késedelem nélkül helyesbítse a rá vonatkozó pontatlan személyes adatokat. Az érintett továbbá jogosult a hiányos személyes adatok kiegészítésére.[758]

- A személyes adatok törléséhez és kezelésének korlátozásához való jog. Egyes esetekben az adatkezelőnek törölnie kell a személyes adatokat. Az érintett pedig jogosult arra, hogy kérje a rá vonatkozó személyes adatok törlését, ha azok kezelése jogszerűtlenül történik.[759] Egyes esetekben a személyes adatok kezelése törlés helyett korlátozható. Erre akkor kerülhet sor, ha 1) az érintett vitatja a személyes adatok pontosságát, és azok pontossága vagy pontatlansága nem állapítható meg egyértelműen; vagy 2) a személyes adatokat bizonyítás céljából meg kell őrizni.[760]

Az adatkezelőnek az érintettet minden esetben írásban tájékoztatnia kell a helyesbítésnek, a törlésnek vagy az adatkezelés korlátozásának a megtagadásáról és a megtagadás indokairól. A tagállamok korlátozhatják a tájékoztatási kötelezettséget, többek között a közbiztonság védelme vagy mások jogainak és szabadságainak védelme érdekében – vagyis pontosan a személyes adatokhoz való hozzáférési jog korlátozásával megegyező okokból.[761]

Az érintett rendszerint jogosult tájékoztatást kapni személyes adatainak kezeléséről, jogosult hozzáférni a rá vonatkozó személyes adatokhoz, azok helyesbítését vagy törlését, illetve az adatkezelés korlátozását kérni, amely jogait közvetlenül az adatkezelővel szemben gyakorolhatja. Tartalékmegoldásként az érintett jogainak közvetett gyakorlása, az adatvédelmi felügyeleti hatóság közreműködésével is lehetséges a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv keretében, és erre akkor kerül sor, amikor az adatkezelő korlátozza az érintett jogait.[762] Az irányelv 17. cikke előírja, hogy a tagállamok olyan rendelkezése-

757 *Uo.*, 15. cikk.
758 *Uo.*, 16. cikk (1) bekezdés.
759 *Uo.*, 16. cikk (2) bekezdés.
760 *Uo.*, 16. cikk (3) bekezdés.
761 *Uo.*, 16. cikk (4) bekezdés.
762 *Uo.*, 17. cikk.

ket fogadnak el, amelyek értelmében az érintett jogainak gyakorlására a felügyeleti hatóság közreműködésével is sor kerülhet. Ezért kell az adatkezelőnek tájékoztatnia az érintettet a közvetett hozzáférés lehetőségéről.

Az adatkezelő és adatfeldolgozó kötelezettségei

A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv összefüggésében az adatkezelő az illetékes hatóság vagy más megfelelő közhatalmi jogosítványokat gyakoroló szerv és közhatalmi szerv, amely meghatározza a személyes adatok kezelésének céljait és módjait. Az irányelv számos kötelezettséget ír elő az adatkezelők számára a bűnüldözési célból kezelt személyes adatok magas szintű védelmének biztosítása érdekében.

Az illetékes hatóságoknak naplózniuk kell az automatizált adatkezelési rendszerekben elvégzett adatkezelési műveleteket. A naplózást legalább a gyűjtés, módosítás, betekintés, közlés – ideértve a továbbítást is –, az összekapcsolás és a törlés vonatkozásában el kell végezni.[763] Az irányelv előírja, hogy a betekintésre és a közlésre vonatkozó naplók lehetővé kell, hogy tegyék e műveletek indokoltságának, dátumának és időpontjának, valamint – lehetőség szerint – a személyes adatba betekintő vagy azt közlő személyek személyazonosságának, illetve az ilyen személyes adatok címzettjei személyazonosságának a megállapítását. A naplók kizárólag az adatkezelés jogszerűségének ellenőrzésére, önellenőrzésre, a személyes adatok integritásának és biztonságának szavatolására, valamint büntetőeljárások keretében használhatók fel.[764] Az adatkezelő és az adatfeldolgozó a felügyeleti hatóság kérése alapján a hatóság rendelkezésére bocsátja a naplókat.

Az adatkezelő általános kötelezettsége, hogy megfelelő technikai és szervezési intézkedéseket hajtson végre annak biztosítása és bizonyítása céljából, hogy az adatok kezelése az irányelvvel összhangban történik.[765] Az ilyen intézkedések megtervezése során figyelembe kell venni az adatkezelés jellegét, hatókörét, körülményeit és céljait, és mindenekelőtt az egyének jogaira és szabadságaira jelentett kockázatokat. Az adatkezelőknek megfelelő belső irányelveket kell elfogadniuk és olyan intézkedéseket kell végrehajtaniuk, amelyek megkönnyítik az adatvédelmi elvek, különösen a beépített és alapértelmezett adatvédelem elvének betartását.[766]

763 *Uo.*, 25. cikk (1) bekezdés.

764 *Uo.*, 25. cikk (2) bekezdés.

765 *Uo.*, 19. cikk.

766 *Uo.*, 20. cikk.

Ha az adatkezelés valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve – új technológiák alkalmazása miatt – az adatkezelőnek az adatkezelést megelőzően hatásvizsgálatot kell végeznie.[767] Az irányelv felsorolja azokat az intézkedéseket is, amelyeket az adatkezelőknek meg kell valósítaniuk az adatkezelés biztonságának garantálásához. Ezek közé tartoznak az általuk kezelt személyes adatokhoz való jogosulatlan hozzáférés megelőzése, annak biztosítása, hogy a jogosult személyek kizárólag a hozzáférési engedélyben meghatározott személyes adatokhoz férjenek hozzá, hogy az adatkezelő rendszer megfelelően működjön, és, hogy a tárolt személyes adatok a rendszer hibás működése esetén ne sérüljenek.[768] Ha adatvédelmi incidens történik, az adatkezelők kötelesek azt három napon belül bejelenteni a felügyeleti hatóságnak, ismertetve az adatvédelmi incidens jellegét, valószínűsíthető következményeit, az incidenssel érintett adatok kategóriáit, valamint az érintettek hozzávetőleges számát. Az adatvédelmi incidensről „haladéktalanul" tájékoztatni kell az érintettet is, amennyiben az incidens valószínűsíthetően kockázattal jár a jogaira és szabadságaira nézve.[769]

Az irányelv tartalmazza az elszámoltathatóság elvét, amely előírja az adatkezelők számára, hogy hajtsanak végre intézkedéseket annak biztosítására, hogy megfeleljenek ezen elvnek. Az adatkezelők kötelesek nyilvántartást vezeti a felelősségi körükbe tartozó adatkezelési tevékenységek kategóriáiról: e nyilvántartás részletes tartalmát az irányelv 24. cikke ismerteti. A nyilvántartást megkeresés alapján a felügyeleti hatóság rendelkezésére kell bocsátani, hogy ellenőrizni tudja az adatkezelő adatkezelési tevékenységeit. Az elszámoltathatóság fokozását célzó másik fontos intézkedés egy adatvédelmi tisztviselő kinevezése. Az adatkezelők kötelesek adatvédelmi tisztviselőt kinevezni, bár az irányelv lehetővé teszi, hogy a tagállamok mentesítsék e kötelezettség alól a bíróságokat és egyéb független igazságszolgáltatási hatóságot.[770] Az adatvédelmi tisztviselő feladatai hasonlóak az általános adatvédelmi rendeletben meghatározott feladatokhoz. Az adatvédelmi tisztviselő ellenőrzi az irányelvnek való megfelelést, információt szolgáltat és tanácsot ad azon alkalmazottak számára, akik az adatvédelmi jogszabályok szerinti kötelezettségeik teljesítése keretében végeznek adatkezelést. Az adatvédelmi tisztviselő tanácsot ad arra vonatkozóan, hogy szükséges-e adatvédelmi hatásvizsgálatot végezni, és a felügyeleti hatóság felé kapcsolattartóként jár el.

767 *Uo.*, 27. cikk.

768 *Uo.*, 29. cikk.

769 *Uo.*, 30. és 31. cikk.

770 *Uo.*, 32. cikk.

Adattovábbítás harmadik országok vagy nemzetközi szervezetek számára

Az általános adatvédelmi rendelethez hasonlóan az irányelv létrehozza a személyes adatok harmadik országokba, illetve nemzetközi szervezetek részére történő továbbításának feltételeit. Ha a személyes adatokat szabadon lehetne továbbítani az Unión kívüli joghatóságokba, az aláásná az uniós jogban biztosított garanciákat és erős védelmet. Maguk a feltételek azonban meglehetősen különböznek az általános adatvédelmi rendeletben meghatározottaktól. A személyes adatok harmadik országok vagy nemzetközi szervezetek számára történő továbbítása akkor engedélyezett, ha:[771]

- Az adattovábbítás az irányelv céljaiból szükséges.
- A személyes adatokat olyan harmadik országbeli adatkezelőhöz vagy olyan nemzetközi szervezet részére továbbítják, amely a rendelet értelmében illetékes hatóságnak minősül –bár egyedi és sajátos esetekben lehet eltéréseket alkalmazni.[772]
- A határokon átnyúló együttműködés keretében kapott személyes adatok harmadik országok vagy nemzetközi szervezetek számára sürgős esetekben kivételek alkalmazhatók.
- Az Európai Bizottság egy megfelelőségi határozatot fogadott el, megfelelő garanciák kerültek kialakításra vagy az adatkezelés tekintetében egyedi helyzetekben eltérés alkalmazható.
- Egy további harmadik ország vagy további nemzetközi szervezet részére történő újbóli továbbítás esetén az eredeti illetékes hatóság előzetes engedélye szükséges, amely figyelembe veszt többek között a bűncselekmény súlyosságát, valamint a személyes adatok védelmének szintjét a nemzetközi adattovábbítás második célországában.[773]

Az irányelv értelmében a személyes adatok továbbítására akkor kerülhet sor, ha a három feltétel közül az egyik teljesül. Az első akkor teljesül, amikor az Európai

771 *Uo.*, 35. cikk.

772 *Uo.*, 39. cikk.

773 *Uo.*, 35. cikk (1) bekezdés.

Bizottság kiad egy megfelelőségi határozatot. A határozat vonatkozhat a harmadik ország teljes területére, vagy a harmadik ország meghatározott ágazataira, vagy egy nemzetközi szervezetre. Ez azonban csak akkor történhet, ha megfelelő szintű védelem biztosított, és teljesülnek az irányelvben meghatározott feltételek.[774] Ilyen esetekben a személyes adatok továbbítása nem kötött a tagország engedélyéhez.[775] Az Európai Bizottságnak ellenőriznie kell azokat a fejleményeket, amelyek érinthetik a megfelelőségi határozat működését. Ezenkívül a határozatnak tartalmaznia kell egy mechanizmust annak időszakos felülvizsgálatára. A Bizottság hatályon kívül helyezheti, módosíthatja vagy felfüggesztheti a határozatot, amennyiben a rendelkezésre álló információk alapján megállapítja, hogy a harmadik ország vagy nemzetközi szervezet már nem biztosít megfelelő szintű védelmet. Ilyen esetben a Bizottságnak egyeztetést kell folytatnia a harmadik országgal vagy nemzetközi szervezettel a helyzet orvoslása érdekében.

Megfelelőségi határozat hiányában az adattovábbítás alapulhat megfelelő garanciákon. Ezeket jogilag kötelező érvényű okiratokban kell rögzíteni, vagy az adatkezelő végezhet önértékelést, amelyben megvizsgálja a személyes adatok továbbításának körülményeit és megállapítja, hogy megfelelő garanciák állnak fenn. Az önértékelésnek figyelembe kell vennie az Europol vagy az Eurojust és a harmadik ország vagy nemzetközi szervezet között létrejött esetleges együttműködési megállapodásokat, a titoktartási kötelezettség meglétét és a célhoz kötöttséget, valamint az arra vonatkozó biztosítékokat, hogy az adatokat nem használják fel semmilyen kegyetlen és embertelen bánásmódhoz, ideértve a halálbüntetést.[776] Ez utóbbi esetben az adatkezelőnek tájékoztatnia kell az illetékes felügyeleti hatóságot az e kategóriába tartozó továbbított adatok kategóriáiról.[777]

Amennyiben nem került megfelelőségi határozat elfogadásra, illetve nem kerültek megfelelő garanciák kialakításra, az irányelvben megállapított egyes esetekben ennek ellenére engedélyezhető az adattovábbítás. Ezek közé tartozik többek között az érintett vagy egy másik személy létfontosságú érdekeinek védelme, valamely tagállam vagy harmadik ország közbiztonságának fenntartását közvetlenül és komolyan fenyegető veszély elhárítása.[778]

774 *Uo.*, 36. cikk.

775 *Uo.*, 36. cikk (1) bekezdés.

776 *Uo.*, (71) preambulumbekezdés.

777 *Uo.*, 37. cikk (1) bekezdés.

778 *Uo.*, 38. cikk (1) bekezdés.

Egyedi és speciális esetekben az illetékes hatóságok továbbíthatják az adatokat olyan harmadik országbeli címzetteknek, akik nem minősülnek illetékes hatóságnak, ha a fenti három feltétel teljesülése mellett a 39. cikkben rögzített további feltételek is teljesülnek. Így különösen az adattovábbítás feltétlenül szükséges az adatokat továbbító illetékes hatóság feladatának ellátásához, amely felelős annak megállapítására, hogy az egyéneknek az adattovábbítást igénylő közérdekkel szemben nincs olyan alapvető joga és szabadsága, amely elsőbbséget élvez. Az ilyen adattovábbítást dokumentálni kell, és az adatokat továbbító illetékes hatóságnak tájékoztatnia kell az illetékes felügyeleti hatóságot.[779]

Végezetül, és a harmadik országgal vagy nemzetközi szervezettel kapcsolatosan, az irányelv előírja nemzetközi együttműködési mechanizmusok kialakítását is a jogszabályok hatékony érvényesítésének elősegítésére, és így segíti az adatvédelmi felügyeleti hatóságokat a külföldi partner hatóságokkal való együttműködésben.[780]

Független felügyelet és az érintettek jogorvoslati lehetőségei

Minden tagállamnak gondoskodnia kell arról, hogy az irányelv szerint elfogadott rendelkezések alkalmazását egy vagy több független nemzeti felügyeleti hatóság segítse tanácsadással és ellenőrizze.[781] Az irányelv alkalmazásában létrehozott felügyeleti hatóság lehet azonos az általános adatvédelmi rendelet alapján létrehozott felügyeleti hatósággal, azonban a tagállamok szabadon jelölhetnek ki másik hatóságot is, feltéve, hogy az megfelel a függetlenség kritériumának. A felügyeleti hatóságok az említetteken kívül befogadják az illetékes hatóságok által végzett személyesadat-kezeléssel összefüggően az adott személyt megillető jogok és szabadságok védelmével kapcsolatban e személy által benyújtott kérelmeket.

Amennyiben kényszerítő okok miatt az érintett e jogainak gyakorlását megtagadják, az érintettnek rendelkeznie kell fellebbezési joggal az illetékes nemzeti felügyeleti hatósághoz és/vagy a bírósághoz. Amennyiben egy személy az irányelvet végrehajtó nemzeti rendelkezéseket sértő intézkedés eredményeként kárt szenved, az elszenvedett kárért az adatkezelőtől vagy a tagállami jog szerint illetékes bármely más hatóságtól kártérítésre jogosult.[782] Az érintettnek általánosságban jogot

779 *Uo.*, 37. cikk (3) bekezdés.

780 *Uo.*, 40. cikk.

781 *Uo.*, 41. cikk.

782 *Uo.*, 56. cikk.

kell biztosítani arra, hogy az irányelvet végrehajtó nemzeti jogszabályok szerint őt megillető jogok megsértése esetén bírósági jogorvoslatot vehessen igénybe.[783]

8.3 A büntetőügyeknél alkalmazott adatvédelemre vonatkozó egyéb speciális jogi eszközök

A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv mellett a tagállamok birtokában lévő adatok konkrét területeken történő cseréjét számos jogi eszköz szabályozza. Ilyen például a Tanács 2009/315/IB kerethatározata a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról, a Tanács 2000/642/IB határozata a tagállamok pénzügyi hírszerző egységeinek az információcsere terén folytatott együttműködésére vonatkozó rendelkezésekről, valamint a Tanács 2006/960/IB kerethatározata (2006. december 18.) az Európai Unió tagállamainak bűnüldöző hatóságai közötti, információ és bűnüldözési operatív információ cseréjének leegyszerűsítéséről.[784]

Lényeges, hogy az illetékes hatóságok közötti, határokon átnyúló együttműködés[785] egyre nagyobb mértékben együtt jár a bevándorlási adatok cseréjével. Ez a jogi terület nem tartozik a rendőrségi és igazságszolgáltatási kérdések közé, de számos vonatkozásban lényeges a rendőrségi és igazságszolgáltatási hatóságok munkája szempontjából. Ugyanez igaz az EU-ba bevitt vagy onnan kivitt árukkal kapcsolatos adatokra is. A schengeni térségen belüli belső határellenőrzés megszüntetése megnövelte a csalás kockázatát, aminek következtében a tagállamoknak intenzívebbé kell tenniük az együttműködést – különösen a határokon átnyúló információcsere fokozásával –, hogy eredményesebben derítsék fel és vonják büntetőeljárás alá a nemzeti és az uniós vámszabálysértéseket. Ezen túlmenően az elmúlt években

783 *Uo.*, 54. cikk.

784 Az Európai Unió Tanácsa (2009), A Tanács 2009/315/IB kerethatározata (2009. február 26.) a bűnügyi nyilvántartásból származó információk tagállamok közötti cseréjének megszervezéséről és azok tartalmáról, HL L 93., 2009.4.7.; Az Európai Unió Tanácsa (2000), A Tanács 2000/642/IB határozata (2000. október 17.) a tagállamok pénzügyi hírszerző egységeinek az információcsere terén folytatott együttműködésére vonatkozó rendelkezésekről, HL L 271., 2000.10.24.; A Tanács 2006/960/IB kerethatározata (2006. december 18.) az Európai Unió tagállamainak bűnüldöző hatóságai közötti, információ és bűnüldözési operatív információ cseréjének leegyszerűsítéséről, HL L 386., 2006.12.29.

785 Európai Bizottság (2012), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak – Az EU-n belüli bűnüldözési együttműködés erősítése: az európai információcsere-modell, COM(2012) 735 final, Brüsszel, 2012. december 7.

a világban megnövekedett a nemzetközi utazással is járó súlyos és szervezett bűncselekmények, illetve a terrorista bűncselekmények száma, és ez rámutatott számos esetben a fokozott határokon átnyúló rendészeti és bűnüldözési együttműködés szükségességére.[786]

A prümi határozat

A nemzeti szinten tárolt adatok cseréjével megvalósuló, intézményesített határokon átnyúló együttműködés egyik példája a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló 2008/615/IB tanácsi határozat (prümi határozat), a benne foglalt végrehajtási rendelkezésekkel együtt, amely 2008-ban az uniós jogba emelte a Prümi Szerződést.[787] A Prümi Szerződés egy 2005-ben létrejött nemzetközi rendőrségi együttműködési megállapodás, amelyet Ausztria, Belgium, Franciaország, Hollandia, Luxemburg, Németország és Spanyolország írt alá.[788]

A prümi határozat célja, hogy segítséget nyújtson az aláíró tagállamoknak három területen – a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció terén – a bűncselekmények megelőzését és az ellenük való küzdelmet szolgáló fokozottabb információcsere megvalósításában. E célból a határozat a következőkkel kapcsolatban állapít meg rendelkezéseket:

- automatizált hozzáférés DNS-profilokhoz, ujjlenyomatadatokhoz és bizonyos nemzeti gépjármű-nyilvántartási adatokhoz;
- határon átnyúló dimenzióval rendelkező nagyszabású eseményekkel kapcsolatos adatok átadása;
- információátadás terrorcselekmények megelőzésére;

786 Lásd: Európai Bizottság (2011), Javaslat európai parlamenti és tanácsi irányelvre az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében, COM(2011) 32 végleges, Brüsszel, 2011. február 2.

787 Az Európai Unió Tanácsa (2008), A Tanács 2008/615/IB határozata (2008. június 23.) a különösen a terrorizmus és a határokon átnyúló bűnözés elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről, HL L 210., 2008.8.6.

788 A Belga Királyság, a Németországi Szövetségi Köztársaság, a Spanyol Királyság, a Francia Köztársaság, a Luxemburgi Nagyhercegség, a Holland Királyság és az Osztrák Köztársaság között létrejött, különösen a terrorizmus, a határokon átnyúló bűnözés, valamint az illegális migráció elleni küzdelemre irányuló, határokon átnyúló együttműködés megerősítéséről szóló szerződés.

- egyéb intézkedések a határon átnyúló rendőrségi együttműködés megerősítésére.

A prümi határozat alapján rendelkezésre bocsátott adatbázisokat teljes mértékben a nemzeti jog szabályozza, azonban az adatok cseréjére a határozat is irányadó, amelynek a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvvel való összeegyeztethetőségét még vizsgálni kell. A szóban forgó adatáramlások felügyeletét ellátó illetékes szervek a nemzeti adatvédelmi felügyeleti hatóságok.

A Tanács 2006/960/IB kerethatározata – a svéd kezdeményezés

A Tanács 2006/960/IB kerethatározata (svéd kezdeményezés)[789] a nemzeti szinten a bűnüldöző hatóságok által tárolt adatok cseréje tekintetében megvalósuló határokon átnyúló együttműködés egy másik példája. A svéd kezdeményezés kifejezetten az információk és bűnüldözési operatív információk cseréjére fókuszál, és 8. cikkében konkrét adatvédelmi szabályokat állapít meg.

A határozat szerint a kicserélt információk és a bűnüldözési operatív információk az információkat fogadó tagállam nemzeti adatvédelmi rendelkezéseinek hatálya alá tartozik, és ugyanazok a szabályok vonatkoznak rájuk, mint az adott tagállamban gyűjtött információkra. A 8. cikk tovább megy azzal, hogy kimondja, információ és bűnüldözési operatív információ szolgáltatásakor az illetékes bűnüldöző hatóság a nemzeti jogának megfelelően feltételeket állapíthat meg a fogadó illetékes bűnüldöző hatóság felé az információ felhasználására vonatkozóan. Ezek a feltételek vonatkozhatnak azon nyomozás vagy bűnüldözési operatív műveletek eredményéről történő beszámolásra is, amelyek érdekében szükség volt az információ és a bűnüldözési operatív információ cseréjére. Amikor azonban a nemzeti jog kivételeket tesz lehetővé az információk felhasználásának korlátozására vonatkozóan (pl. igazságszolgáltatási hatóságok, jogalkotó testületek, stb. számára), az információ és bűnüldözési operatív információ csak a szolgáltató tagállammal folytatott előzetes konzultációt követően használható fel.

A szolgáltatott információ és bűnüldözési operatív információ a következő célokból használható fel:

789 Az Európai Unió Tanácsa (2006), A Tanács 2006/960/IB kerethatározata (2006. december 18.) az Európai Unió tagállamainak bűnüldöző hatóságai közötti, információ és bűnüldözési operatív információ cseréjének leegyszerűsítéséről, HL L 386., 2006.12.29.

- azon célokra, amelyek érdekében azokat szolgáltatták; vagy
- a közbiztonságot közvetlenül és súlyosan fenyegető esemény megelőzése.

Az egyéb célokból történő adatkezelés megengedhető, de kizárólag a közlő tagállam előzetes engedélyével.

A svéd kezdeményezés továbbá kimondja, hogy a kezelt személyes adatokat védeni kell, többek között a következő nemzetközi eszközökkel összhangban:

- Európa Tanács, Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során;[790]
- Az Egyezmény 2001. november 8-i kiegészítő jegyzőkönyve a felügyeleti hatóságokra és a határokon átnyúló adatáramlásra vonatkozóan;[791]
- Az Európa Tanácsnak a személyes adatok rendőrségi ágazatban való felhasználásának szabályozására irányuló R(87) 15. sz. ajánlása.[792]

Az uniós PNR-irányelv

Az utasnyilvántartási adatállomány (PNR) adatai a légiutasok légi fuvarozók helyfoglalási és indulás-ellenőrzési rendszerei által saját kereskedelmi céljaik érdekében gyűjtött és tárolt adataira vonatkoznak. Ezek az adatok különféle típusú információkat tartalmaznak, mint például az utazások időpontjai, az utazások útvonalai, a jegyek adatai, az elérhetőségek, azon utazásközvetítők, akiknek a közreműködésével a repülőutakat lefoglalták, az alkalmazott fizetési mód, az ülőhely száma és a poggyászra vonatkozó információk.[793] A PNR-adatok kezelése segíthet a bűnül-

790 Európa Tanács (1981), Egyezmény az egyének védelméről a személyes adatok gépi feldolgozása során, ETS 108.

791 Európa Tanács (2011), Kiegészítő jegyzőkönyv a személyes adatok gépi feldolgozása során az egyének védelméről szóló egyezményhez, az adatvédelmi hatóságokra és az országhatárokat átlépő adatáramlásra vonatkozóan, ETS 108.

792 Európa Tanács (1987), A Miniszteri Bizottság R(87)15. sz. ajánlása a tagállamok részére a személyes adatok rendőrségi ágazatban való felhasználásának szabályozásáról (elfogadták a miniszterhelyettesek 1987. szeptember 17-i ülésén).

793 Európai Bizottság (2011), Javaslat európai parlamenti és tanácsi irányelvre az utas-nyilvántartási adatállomány (PNR) felhasználásáról a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, kivizsgálása és büntetőeljárás alá vonása érdekében, COM(2011) 32 végleges, Brüsszel, 2011. február 2.

dözési hatóságoknak abban, hogy azonosítsák az ismert vagy potenciális gyanúsítottakat, és az utazási szokások, valamint egyéb, tipikusan a bűnöző tevékenységekkel összefüggő mutatók alapján vizsgálatokat folytassanak. A PNR-adatok elemzése lehetővé teszi az utazási útvonalak és a bűnözési tevékenységekben érintett gyanúsított személyek kapcsolatainak utólagos lekövetését, ami lehetővé teheti a bűnüldözési hatóságok számára a bűnhálózatok azonosítását.[794] Az EU néhány megállapodást kötött harmadik országokkal a PNR-adatok cseréjére vonatkozóan a 7. fejezetben ismertetettek szerint. Ezenkívül az az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról szóló (EU) 2016/681 irányelvvel (uniós PNR-irányelv) bevezette a PNR-adatok kezelését.[795] Ez az irányelv meghatározza a légi fuvarozók azon kötelezettségét, hogy továbbítsák a PNR-adatokat az illetékes hatóságoknak, továbbá szigorú adatvédelmi garanciákat állapít meg az ilyen adatok kezelése és gyűjtése tekintetében. Az uniós PNR-irányelv az EU-ba irányuló, valamint az EU-ból induló nemzetközi járatokra vonatozik, azonban a tagállamok dönthetnek úgy, hogy az Unión belüli járatokra is alkalmazzák.[796]

A gyűjtött PNR-adatok kizárólag az uniós PNR-irányelvben megengedett információkat tartalmazhatják. Ezeket az adatokat az egyes tagállamokban biztonságos helyen, egyetlen információs egységnél kell tárolni. A PNR-adatokat hat hónappal a továbbítást követően személyazonosításra alkalmatlanná kell tenni, és legfeljebb öt évig meg kell őrizni.[797] A PNR-adatok cseréjére a tagállamok között; a tagállamok és az Europol között; valamint – kizárólag eseti alapon – a tagállamok és harmadik országok között kerül sor.

A PNR-adatok továbbításának és kezelésének, valamint az érintettek számára biztosított jogoknak meg kell felelniük a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv előírásainak, és biztosítani kell a magánélet és a személyes adatok Charta, Korszerűsített 108. Egyezmény, valamint az EJEE által megkövetelt magas szintű védelmét.

794 Európai Bizottság (2015), Tájékoztató: A terrorizmus elleni küzdelem uniós szinten, a Bizottság fellépéseinek, intézkedéseinek és kezdeményezéseinek áttekintése, Brüsszel, 2015. január 11.

795 Az Európai Parlament és a Tanács (EU) 2016/681 irányelve (2016. április 27.) az utas-nyilvántartási adatállománynak (PNR) a terrorista bűncselekmények és súlyos bűncselekmények megelőzése, felderítése, nyomozása és a vádeljárás lefolytatása érdekében történő felhasználásáról, HL L 119., 2016.5.4.

796 PNR-irányelv, 1. cikk (1) bekezdés és 2. cikk (1) bekezdés.

797 *Uo.*, 12. cikk (1) bekezdés és 12. cikk (2) bekezdés.

A rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv alapján illetékes független, nemzetközi felügyeleti hatóságok feladata továbbá, hogy ellenőrizze a tagállamok által az uniós PNR-irányelv értelmében elfogadott rendelkezések alkalmazását, valamint hogy tanácsot adjanak azzal kapcsolatban.

A távközlési adatok megőrzése

Az adatmegőrzési irányelv[798] – amelyet a bíróság 2014. április 8-án érvénytelennek nyilvánított a *Digital Rights Ireland* ügyben – kötelezte a hírközlési szolgáltatókat, hogy a súlyos bűncselekmények elleni küzdelem céljából legalább hat, legfeljebb 24 hónapig tartsák rendelkezésre a metaadatokat, függetlenül attól, hogy a szolgáltatónak számlázási célból vagy a szolgáltatás technikai nyújtásához szüksége van-e még ezekre az adatokra.

A távközlési adatok megőrzése egyértelműen ellentétes az adatvédelemhez való joggal.[799] Azt, hogy ez a jogba való beavatkozás indokolt-e vagy sem, az uniós tagállamokban lefolytatott számos bírósági eljárás során tárgyalták.[800]

Példa: A *Digital Rights Ireland* és *Kärntner Landesregierung és társai* ügyben[801] a Digital Rights csoport, illetve M. Seitlinger eljárást indított Írországban a legfelsőbb bíróságon, illetve Ausztriában az alkotmánybíróságon, vitatva az elektronikus telekommunikációs adatok megőrzését engedélyező nemzeti intézkedések jogszerűségét. A Digital Rights arra kérte az ír bíróságot, hogy nyilvánítsa érvénytelennek a 2006/24 irányelvet, valamint a nemzeti büntetőtörvény terrorista bűncselekményekre vonatkozó részét. Hasonlóan

798 Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról, HL L 105., 2006.4.13.

799 Az európai adatvédelmi biztos 2011. május 31-i véleménye a Tanácsnak és az Európai Parlamentnek szóló, az adatvédelmi irányelvre (2006/24/EK irányelv) vonatkozó bizottsági értékelő jelentésről, 2011. május 31.

800 Németország, Szövetségi Alkotmánybíróság (*Bundesverfassungsgericht*), 1 BvR 256/08. sz. ügy, 2010. március 2.; Románia, Szövetségi Alkotmánybíróság (*Curtea Constituțională a României*), 1258. sz. ügy, 2009. október 8.; Cseh Köztársaság, Alkotmánybíróság (*Ústavní soud České republiky*), 94/2011 Coll. sz. ügy, 2011. március 22.

801 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8., 65. pont.

M. Seitlinger és több mint 11 000 további felperes kifogásolta a 2006/24 irányelvet átültető, a telekommunikációra vonatkozó osztrák jogszabály egy rendelkezését, és annak megsemmisítését kérte.

Az előzetes döntéshozatalra irányuló kérelmek vizsgálata során az EUB érvénytelennek nyilvánította az adatmegőrzési irányelvet. Az EUB véleménye szerint azok az adatok, amelyeket az irányelv alapján meg lehetett őrizni, együttesen véve pontos információt szolgáltattak az egyénekről. Az EUB továbbá megvizsgálta a magánélet tiszteletben tartásához és a személyes adatok védelméhez fűződő alapjogokba való beavatkozás súlyosságát. Megállapította, hogy az adatok megőrzése egy közérdekű célt, nevezetesen súlyos bűnözés elleni küzdelmet, így pedig a közbiztonságot szolgálta. Mindazonáltal az EUB kimondta, hogy az uniós jogalkotó az irányelv elfogadásával megsértette az arányosság elvét. Bár az irányelv arányos lehet a szükséges cél eléréséhez, „széles körben és különösen súlyosan beavatkozik ezen alapvető jogokba, anélkül hogy e beavatkozást pontosan körülhatárolnák olyan rendelkezések, amelyek lehetővé teszik, hogy az ténylegesen a feltétlenül szükséges mértékre korlátozódjon."

Az adatmegőrzés, az adatmegőrzésre vonatkozó külön szabályozás hiányában, a telekommunikációs adatok 2002/58/EK irányelv (elektronikus hírközlési adatvédelmi irányelv)[802] szerinti bizalmas jellege alóli kivételként megelőző intézkedésként megengedett lehet, azonban kizárólag a súlyos bűnözés elleni küzdelem céljából. Az ilyen adatmegőrzést a feltétlenül szükségesre kell korlátozni a megőrzött adatok kategóriát, az érintett kommunikáció módját, az érintett személyeket és a megőrzés választott időtartamát illetően. A nemzeti hatóságok szigorú feltételek mellett férhetnek hozzá a megőrzött adatokhoz, beleértve a független hatóság általi előzetes felülvizsgálatot is. Az adatokat az EU-n belül kell megőrizni.

Példa: A *Digital Rights Ireland* és *Kärntner Landesregierung és társai*[803] ítéletet követően két másik ügyet is az EUB elé vittek Svédországban és az Egyesült Királyságban az elektronikus hírközlési szolgáltatásokat nyújtók

802 Az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló, 2002. július 12-i 2002/58/EK európai parlamenti és tanácsi irányelv (elektronikus hírközlési adatvédelmi irányelv).

803 EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

számára az érvénytelenné nyilvánított adatmegőrzési irányelv szerint előírt, a távközlési adatok megőrzésére vonatkozó általános kötelezettséggel kapcsolatban. A *Tele2 Sverige* és *Home Department kontra Tom Watson és társai* ügyben[804] az EUB ítélete szerint az a nemzeti szabályozás, amely előírja az adatok általános és különbségtétel nélküli megőrzését anélkül, hogy szükségessé tenné kapcsolat meglétét a megőrzendő adatok és a közbiztonság elleni fenyegetés között, és anélkül, hogy bármilyen feltételt – pl. megőrzési idő, földrajzi terület, súlyos bűncselekményben valószínűsíthetően érintett személyek csoportja – előírna, túllépi a feltétlenül szükséges mértéket és nem tekinthető indokoltnak egy demokratikus társadalomban, ahogy azt az EU Alapjogi Chartája fényében értelmezett 2002/58/EK irányelv megköveteli.

Kilátások

2017 januárjában az Európai Bizottság rendeletre irányuló javaslatot tett közzé a magánélet tiszteletben tartását és a személyes adatok védelmét illetően az elektronikus hírközlésekben, amelynek célja a 2002/58/EK irányelv hatályon kívül helyezése és felváltása.[805] A javaslat nem tartalmaz konkrét rendelkezéseket az adatmegőrzésre vonatkozóan. Rendelkezik azonban arról, hogy a tagállamok jogszabályban korlátozhatják a rendeletben rögzített egyes kötelezettségeket és jogokat, amennyiben az egy demokratikus társadalomban szükséges és arányos intézkedésnek minősül, konkrét közérdekek, beleértve a nemzetbiztonság, a védelem és a közbiztonság védelme, valamint bűncselekmények megelőzése, nyomozása, felderítése, a vádeljárás lefolytatása vagy büntetőjogi szankciók végrehajtása érdekében.[806] Ezért a tagállamok fenntarthatnának vagy létrehozhatnának célzott adatmegőrzési intézkedéseket meghatározó nemzeti adatmegőrzési keretet, amennyiben az ilyen keret megfelel az uniós jogszabályoknak és figyelembe veszi az EUB-nek az elektronikus hírközlési adatvédelmi irányelv és az EU Alapjogi Chartájának értelmezésére

804 EUB, *Tele2 Sverige AB kontra Post- och telestyrelsen és Secretary of State for the Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016. december 21.

805 Európai Bizottság (2017), Javaslat – Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), COM(2017) 10 final, Brüsszel, 2017. január 10.

806 *Uo.*, (26) preambulumbekezdés.

vonatkozó ítélkezési gyakorlatát.[807] A kézikönyv megszövegezése idején folyamatban voltak az egyeztetések a rendelet elfogadására vonatkozóan.

EU– USA keretmegállapodás a bűnüldözési célból kicserélt személyes adatok védelméről

2017. február 1-jén hatályba lépett az EU és az USA közötti, a bűncselekmények megelőzésével, kivizsgálásával, felderítésével és büntetőeljárás alá vonásával kapcsolatos személyes adatok védelméről szóló keretmegállapodás.[808] Az EU és az USA közötti keretmegállapodás célja magas szintű adatvédelmet biztosítani az uniós polgárok számára, az uniós és az amerikai bűnüldöző hatóságok közötti együttműködés erősítése mellett. A megállapodás kiegészíti a meglévő EU–USA, valamint a tagállamok és az USA bűnüldözési hatóságai közötti megállapodásokat, ugyanakkor segít egyértelmű és harmonizált adatvédelmi szabályokat is érvénybe léptetni az e területen a jövőben kötendő megállapodások számára. E tekintetben a megállapodás célja, hogy hosszú távú jogi keretet hozzon létre az információcsere megkönnyítése érdekében.

A megállapodás önmagában nem biztosít megfelelő jogalapot a személyes adatok cseréjéhez, azonban ehelyett megfelelő adatvédelmi garanciákat biztosít az érintett egyének számára. A megállapodás kiterjed a bűncselekmények – ezen belül a terrorcselekmények – megelőzésének, nyomozásának, felderítésének és a vádeljárás lefolytatásának céljából szükséges minden adatkezelési tevékenységre.[809]

A megállapodás több garanciát határoz meg annak biztosítására, hogy a személyes adatokat kizárólag a megállapodásban meghatározott célokból használják fel. Különösen a következő védelmet biztosítja az uniós polgárok számára:

807 Lásd az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről szóló rendeletre irányuló javaslat indokolását, COM(2017) 10 final, 1.3. pont.

808 Lásd: az EU Tanácsa (2016), „Az uniós polgárok fokozott adatvédelmi jogai a bűnüldözési együttműködés terén: A EU és az USA keretmegállapodást ír alá", 305/16. sajtóközlemény, 2016. június 2.

809 Megállapodás az Amerikai Egyesült Államok és az Európai Unió között a bűncselekmények megelőzésével, nyomozásával, felderítésével és a vádeljárás lefolytatásával kapcsolatos személyes adatok védelméről, 2016. május 18., (ERED. angol) 8557/16, 3. cikk (1) bekezdés. Lásd még a Bizottság 2010. május 26-i közleményét (MEMO/10/216) az EU és USA között folytatott adatvédelmi tárgyalásokról és az EU Bizottságának sajtóközleményét az EU-USA közötti adatvédelmi megállapodás magas szintű adatvédelmi előírásairól, 2010. május 26., IP/10/609.

- az adatok felhasználásának korlátozása: a személyes adatokat kizárólag bűncselekmények megelőzése, nyomozása, felderítése és a vádeljárás lefolytatása céljából lehet felhasználni;

- önkényes és indokolatlan megkülönböztetés elleni védelem;

- adattovábbítás harmadik fél részére: minden nem USA-beli, nem uniós országbeli vagy nemzetközi szervezet számára történő adattovábbítás az adatokat eredetileg továbbító ország illetékes hatóságának előzetes jóváhagyásához kötött;

- adatminőség: a személyes adatokat azok pontosságának, relevanciájának, időszerűségének és teljességének szem előtt tartásával kell megőrizni;

- az adatkezelés biztonsága, beleértve az adatvédelmi incidensek bejelentését;

- különleges adatok kezelése kizárólag a jogszabályokkal összhangban, megfelelő garanciák mellett megengedett;

- megőrzési idők: a személyes adatok nem őrizhetők meg a szükséges és megfelelő időtartamnál tovább;

- hozzáféréshez és helyesbítéshez való jog: minden egyén jogosult – meghatározott feltételek mellett – hozzáférni a róla tárolt személyes adatokhoz, és kérheti az adatok helyesbítését, amennyiben pontatlanok azok;

- az automatizált döntésekhez megfelelő garanciák szükségesek, többek között az emberi beavatkozás igénylésének lehetősége;

- hatékony felügyelet, beleértve az EU és az USA felügyeleti szervei közötti együttműködést; és

- bírósági jogorvoslat és érvényesíthetőség: az uniós polgárok jogosultak[810] bírósági jogorvoslatot kérni az amerikai bíróságok előtt, amennyiben az USA hatóságok megtagadják a személyes adataikhoz való hozzáférést vagy azok helyesbítését, vagy törvénytelenül nyilvánosságra hozzák azokat.

810 Az USA bírósági jogorvoslatról szóló törvényét Obama elnök 2016. február 24-én léptette aláírásával hatályba.

A „keretmegállapodás” alapján továbbá létrehoztak egy rendszert, amely értesíti az érintett személyek tagállama szerinti illetékes hatóságokat az adatvédelmi incidensekről. A megállapodás által biztosított jogi garanciák biztosítják az uniós polgárokkal szembeni egyenlő bánásmódot az USA-ban, amennyiben adatvédelmi incidens történik.[811]

8.3.1 Adatvédelem az EU igazságszolgáltatási és bűnüldözési ügynökségeinél

Europol

Az Europol az EU hágai székhelyű bűnüldözési ügynöksége, amelynek minden tagállamban vannak nemzeti egységei (EUROPOL nemzeti egységek). Az Europolt 1998-ban hozták létre, jelenlegi jogállása, mint uniós intézmény, a Bűnüldözési Együttműködés és Képzés Európai Ügynökségéről szóló rendeleten (Europol-rendelet) alapszik.[812] Az Europol célja az Europol-rendelet I. mellékletében felsorolt, két vagy több tagállamot érintő szervezett bűncselekmények, terrorizmus és a szervezett bűnözés más formáinak megelőzése és kivizsgálása. Feladatai teljesítéséhez információkat cserél, és az EU hírszerzési elemzéseket és fenyegetés értékeléseket készítő információs központjaként szolgál.

Céljainak eléréséhez az Europol létrehozta az Europol Információs Rendszert, amely adatbázison keresztül a tagállamok – EUROPOL nemzeti egységeik (ENU-k) útján – kicserélhetik a bűnügyi hírszerzési adatokat és információkat. Az Europol Információs Rendszer a következőkkel kapcsolatos adatok rendelkezésére bocsátására használható: az Europol hatáskörébe tartozó bűncselekménnyel gyanúsított vagy ilyen bűncselekményért elítélt személyek; illetve olyan személyek, akikkel kapcsolatban tényszerű jelek alapján feltételezhető, hogy ilyen bűncselekményt fognak

811 Az európai adatvédelmi biztos kiadott egy véleményt az EU–USA közötti megállapodásról, amelyben többek között a következő módosításokat javasolja: 1) az adatok szükséges és megfelelő időtartamig történő megőrzésével foglalkozó cikk kiegészítése egy „arra a meghatározott célra, melynek érdekében átadásra kerültek” fordulattal, és 2) a különleges adatok tömeges továbbításának – amely lehetséges lehet – kivétele. Lásd: Európai adatvédelmi biztos, Előzetes vélemény az Amerikai Egyesült Államok és az Európai Unió között a személyes adatoknak a bűnügyek megakadályozása, kivizsgálása, felderítése, illetve büntetőeljárás alá vonása céljából történő átadásáról és feldolgozásáról szóló megállapodásról, 1/2016. sz. vélemény.

812 Az Európai Parlament és a Tanács (EU) 2016/794 rendelete (2016. május 11.) a Bűnüldözési Együttműködés Európai Uniós Ügynökségéről (Europol), valamint a 2009/371/IB, a 2009/934/IB, a 2009/935/IB, a 2009/936/IB és a 2009/968/IB tanácsi határozat felváltásáról és hatályon kívül helyezéséről, HL L 135., 2016.5.24.

elkövetni. Az Europol és az ENU-k közvetlenül felvehetnek adatokat az Europol Információs Rendszerbe, és le is kérdezhetnek adatokat onnan. Csak az a fél módosíthatja, javíthatja vagy törölheti az adatokat, aki felvitte azokat a rendszerbe. Az uniós szervek, harmadik országok és nemzetközi szervezetek szintén szolgáltathatnak információkat az Europolnak.

Az Europol nyilvánosan elérhető forrásokból, például az internetről is gyűjthet információkat, köztük személyes adatokat. A személyes adatok továbbítása uniós testületeknek kizárólag akkor megengedett, ha az az Europol vagy a fogadó uniós szerv feladatainak ellátásához szükséges. A személyes adatok továbbítása harmadik ország vagy nemzetközi szervezet részére kizárólag akkor megengedett, ha az Európai Bizottság úgy határoz, hogy az adott ország vagy nemzetközi szervezet megfelelő szintű adatvédelmet biztosít („megfelelőségi határozat"), vagy ha nemzetközi vagy együttműködési megállapodás van érvényben. Az Europol fogadhat személyes adatokat magán felektől és magánszemélyektől, és kezelheti azokat azzal a szigorú feltétellel, hogy a szóban forgó adatokat az Europol valamely nemzeti egysége továbbította annak nemzeti jogával összhangban, egy harmadik országbeli kapcsolattartó pont vagy egy olyan nemzetközi szervezet továbbította, amellyel együttműködési megállapodás alapján kialakult együttműködési kapcsolat áll fenn, vagy egy megfelelőségi határozat alá tartozó harmadik országbeli hatóság vagy nemzetközi szervezet, vagy egy olyan harmadik ország vagy nemzetközi szervezet továbbította, amellyel az EU nemzetközi megállapodást kötött. Valamennyi információcserére biztonságos információcsere-hálózati alkalmazáson (SIENA) keresztül kerül sor.

Az új fejleményekre reagálva szakosodott központokat hoztak létre az Europolnál. 2013-ban létrehozták az Europolnál a Számítástechnikai Bűnözés Elleni Európai Központot.[813] A központ az EU számítástechnikai bűnözéssel kapcsolatos információs központja, amely lehetővé teszi a gyors reagálást online bűncselekmények elkövetése esetén, fejleszti és kialakítja a digitális igazságszolgáltatási képességeket, és közvetíti a számítástechnikai bűnözéssel kapcsolatos nyomozások során bevált gyakorlatokat. A központ elsősorban olyan számítástechnikai bűncselekményekkel foglalkozik, amelyek(et):

- szervezett csoportok követnek el bűncselekményekből származó tetemes nyereség érdekében (pl. az online csalás);

813 Lásd még az európai adatvédelmi biztos 2012-es véleményét a Számítástechnikai Bűnözés Elleni Európai Központ létrehozásáról szóló, a Tanácshoz és az Európai Parlamenthez intézett bizottsági közleményről, Brüsszel, 2012. június 29.

- súlyos kárt okoznak áldozataiknak, így például a gyermekek szexuális kizsákmányolása;

- az Unión belüli kritikus információs vagy kommunikációs technológiai rendszereket érintik.

A Terrorizmus Elleni Küzdelem Európai Központját (ECTC) 2016 januárjában hozták létre abból a célból, hogy operatív támogatást nyújtson a tagállamoknak a terrorista bűncselekményekkel kapcsolatos nyomozásokban. Az alkalmazás összeveti az éles operatív adatokat az Europol már meglévő adataival, ezzel gyorsan fényt derít a pénzügyi szálakra, és elemzi az összes rendelkezésre álló nyomozati adatot, hogy segítsen strukturált képet alkotni valamely terroristahálózatról.[814]

A Migránscsempészés Elleni Küzdelem Európai Központját (EMSC) a Tanács 2015. novemberi ülését követően 2016 februárjában hozták létre abból a célból, hogy támogassa a tagállamokat a migránscsempészetben érintett bűnözői hálózatok felderítésében és felszámolásában. Az uniós regionális akciócsoportok hivatalai (Catania [Olaszország] és Piraeus [Görögország]) támogató információs központként szolgálnak, amelyek számos területen nyújtanak segítséget a nemzeti hatóságoknak, beleértve a hírszerzési információk megosztását, a bűnügyi nyomozási szolgáltatásokat és az embercsempész bűnhálózatok büntetőeljárás alá vonását.[815]

Az Europol tevékenységeit szabályozó adatvédelmi rendszer megerősített, és az uniós intézmények adatvédelmi rendeletének elveire támaszkodik[816], továbbá összhangban van a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvvel, a Korszerűsített 108. Egyezménnyel és a Rendőrségi ajánlással.

A bűncselekmény áldozatait, a tanúkat vagy más, a bűncselekményről információval szolgálni képes személyeket, vagy a 18 éven aluli személyeket érintő személyes adatokat az Europol csak akkor kezelheti, ha ez a céljai körébe tartozó bűncselekmények megelőzéséhez vagy az ellenük való küzdelemhez feltétlenül szükséges és azokkal arányos.[817] Tilos a különleges adatok kezelése, kivéve, ha ez az Europol céljai

814 Lásd az Europol weboldalát a Terrorizmus Elleni Küzdelem Európai Központjára vonatkozóan.

815 Lásd az Europol weboldalát az Embercsempészés Elleni Európai Központra vonatkozóan.

816 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

817 Europol-rendelet, 30. cikk (1) bekezdés.

körébe tartozó bűncselekmények megelőzéséhez vagy az ellenük való küzdelemhez feltétlenül szükséges és azokkal arányos, és ha ezek az adatok az Europol által már kezelt egyéb személyes adatokat egészítenek ki.[818] Mindkét esetben kizárólag az Europol vizsgálhatja meg a releváns adatokat.[819]

Az adatok tárolása csak a kezelésük céljához szükséges és azzal arányos ideig lehetséges, és a további tárolás szükségességét háromévente felül kell vizsgálni, amely nélkül az adatokat automatikusan törölni kell.[820]

Az Europol meghatározott feltételek mellett közvetlenül továbbíthat személyes adatokat valamely uniós szervnek, harmadik országbeli hatóságnak vagy nemzetközi szervezetnek.[821] Ha az adatvédelmi incidens feltételezhetően súlyosan és hátrányosan érinti az érintett jogait és szabadságait, indokolatlan késedelem nélkül tájékoztatni kell az érintettet az adatvédelmi incidensről.[822] Tagállami szinten egy nemzeti felügyeleti hatóságot kell kijelölni a személyes adatok Europol általi kezelésének ellenőrzésére.[823]

Az európai adatvédelmi biztos feladata, hogy a személyes adatoknak az Europol általi kezelése tekintetében nyomon kövesse és biztosítsa a természetes személyek alapvető jogainak és szabadságainak védelmét, valamint tanácsokkal lássa el az Europolt és az érintetteket a személyes adatok kezelését érintő valamennyi kérdésben. E célból az európai adatvédelmi biztos kivizsgáló és panaszkezelő szervként szolgál, és a nemzeti felügyeleti hatóságokkal szorosan együttműködve jár el.[824] Az európai adatvédelmi biztos és a nemzeti felügyeleti hatóságok évente legalább kétszer üléseznek a koordinációs testületben, amely tanácsadó szerepet tölt be.[825] A tagállamok kötelesek jogszabállyal egy felügyeleti hatóságot létrehozni, amely ellenőrzi, hogy megengedhető-e a személyes adatoknak az érintett tagállam által az Europol felé történő továbbítása, lekérdezése és az Europollal való közlése, továbbá megvizsgálása.[826] A tagállamok kötelesek továbbá biztosítani, hogy

818 *Uo.*, 30. cikk (2) bekezdés.
819 *Uo.*, 30. cikk (3) bekezdés.
820 *Uo.*, 31. cikk.
821 *Uo.*, 24. cikk, ill. 25. cikk.
822 *Uo.*, 35. cikk.
823 *Uo.*, 42. cikk.
824 *Uo.*, 43. cikk és 44. cikk.
825 *Uo.*, 45. cikk.
826 *Uo.*, 42. cikk (1) bekezdés.

a nemzeti felügyeleti hatóság az Europol-rendeletben meghatározott feladatuk ellátása és kötelezettségeik teljesítése során függetlenül járjon el.[827] Az adatkezelés jogszerűségének ellenőrzése, az önellenőrzés, valamint az adatok sértetlenségének és megfelelő biztonságának biztosítása céljából az Europol nyilvántartást vagy dokumentációt vezet az általa végzett személyesadat-kezelésről. Az ilyen naplók az automatizált adatkezelő rendszerekben végzett és az adatok gyűjtésével, módosításával, betekintésével, közlésével, összekapcsolásával, illetve törlésével kapcsolatos adatkezelési műveletekre vonatkozó információkat tartalmaznak.[828]

Az európai adatvédelmi biztos határozatai ellen az Európai Unió Bírósága előtt lehet keresetet indítani.[829] Minden olyan egyén, aki jogszerűtlen adatkezelési művelet eredményeképpen kárt szenvedett, az elszenvedett kárért kártérítésre jogosult az Europol-tól, vagy azon tagállamtól, amelyben a kárt okozó esemény történt, az első esetben az Europol ellen az Európai Unió Bíróságán, a második esetben pedig a tagállam illetékes nemzeti bíróságán indított keresettel.[830] Ezenkívül a nemzeti parlamentek és az Európai Parlament szakosodott közös parlamenti ellenőrző csoportja jogosult megvizsgálni az Europol tevékenységeit.[831] Minden magánszemély hozzáférési joggal rendelkezik az Europol által tárolt, rá vonatkozó személyes adatokhoz, továbbá a szóban forgó személyes adatok ellenőrzését, javítását vagy törlését is kérheti. Ezekre mentességek és korlátozások vonatkozhatnak.

Eurojust

A 2002-ben létrehozott Eurojust hágai székhelyű uniós szerv. Legalább két tagállamot érintő, súlyos bűncselekményekkel kapcsolatos nyomozás és büntetőeljárás terén előmozdítja az igazságügyi együttműködést.[832] Az Eurojust illetékességi körébe az alábbiak tartoznak:

827 *Uo.*, 42. cikk (1) bekezdés.

828 *Uo.*, 40. cikk.

829 *Uo.*, 48. cikk.

830 *Uo.*, 50. cikk.

831 *Uo.*, 51. cikk.

832 Az Európai Unió Tanácsa (2002), A Tanács 2002/187/IB határozata (2002. február 28.) a bűnözés súlyos formái elleni fokozott küzdelem céljából az Eurojust létrehozásáról, HL L 63., 2002.3.6.; Az Európai Unió Tanácsa (2003), A Tanács 2003/659/IB határozata (2003. június 18.) a bűnözés súlyos formái elleni fokozott küzdelem céljából az Eurojust létrehozásáról szóló 2002/187/IB határozat módosításáról, HL L 245., 2003.9.29.; Az Európai Unió Tanácsa (2009), A Tanács 2009/426/IB határozata (2008. december 16.) az Eurojust megerősítéséről és az Eurojust létrehozásáról a bűnözés súlyos formái elleni fokozott küzdelem céljából szóló 2002/187/IB határozat módosításáról, HL L 138., 2009.6.4. (Eurojust-határozat).

- a nyomozások és a büntetőeljárások terén a tagállamok hatáskörrel rendelkező hatóságai közötti koordináció és együttműködés ösztönzése és fejlesztése;

- az igazságügyi együttműködésre irányuló megkeresések és határozatok végrehajtásának előmozdítása.

Az Eurojust feladatait nemzeti tagok látják el. Minden tagállam egy-egy, a nemzeti jog hatálya alá tartozó bírót vagy ügyészt delegál az Eurojustba, aki rendelkezik az igazságügyi együttműködés ösztönzését és fejlesztését szolgáló feladatok teljesítéséhez szükséges hatáskörökkel. Ezenfelül a nemzeti tagok közösen testületként látják el az Eurojust speciális feladatait.

Az Eurojust a célkitűzéseinek eléréséhez szükséges mértékben személyes adatokat is feldolgozhat. Ez az adatkezelési tevékenység azonban olyan személyekkel kapcsolatos konkrét adatokra korlátozódik, akiket az Eurojust hatáskörébe tartozó bűncselekmény elkövetésével vagy ilyen bűncselekmény elkövetésében való részvétellel gyanúsítanak, illetve akiket ilyen bűncselekmény miatt elítéltek. Az Eurojust a hatáskörébe tartozó bűncselekmények tanúira és sértettjeire vonatkozó bizonyos információkat is feldolgozhat.[833] Rendkívüli körülmények között az Eurojust – korlátozott ideig – a bűncselekmény körülményeire vonatkozóan szélesebb körű személyesadat-kezelést is végezhet, amennyiben ezek az adatok közvetlenül érintik a folyamatban lévő nyomozást. Az Eurojust a hatáskörének keretein belül más uniós intézményekkel, szervekkel és ügynökségekkel is együttműködhet, és velük személyes adatokat cserélhet. Az Eurojust harmadik országokkal és szervezetekkel is együttműködhet, és személyes adatokat cserélhet.

Az adatvédelem terén az Eurojustnak legalább olyan szintű védelmet kell biztosítania, amely egyenértékű a Korszerűsített 108. Egyezményében, illetve későbbi módosításaiban foglalt elvek alkalmazásából eredő védelemmel. Adatcsere esetén egyedi szabályokat és korlátozásokat kell betartani, amelyeket vagy együttműködési megállapodásban, vagy munkavégzésre vonatkozó rendelkezésben állapítanak meg az Eurojustra vonatkozó tanácsi határozatoknak és az Eurojust adatvédelmi szabályzatának megfelelően.[834]

833 A 2002/187/IB tanácsi határozatnak a 2003/659/IB tanácsi határozattal és a 2009/426/IB tanácsi határozattal történt módosítása egységes szerkezetbe foglalt változata, 15. cikk (2) bekezdés.

834 Az Eurojust személyes adatok feldolgozására és védelmére vonatkozó eljárási szabályzatával kapcsolatos rendelkezések, HL C 68., 2005.3.19.

Független közös ellenőrző szervet (JSB) hoztak létre az Eurojustnál, amely az Eurojust által végzett személyes adat feldolgozást kíséri figyelemmel. Magánszemélyek a közös ellenőrző szervhez nyújthatnak be fellebbezést, ha nem értenek egyet az adataikhoz való hozzáférés, adataik helyesbítése, zárolása vagy törlése iránti kérésükre az Eurojust által hozott határozattal. Ha az Eurojust jogellenesen dolgoz fel személyes adatokat, a székhelye szerinti tagállam – Hollandia – nemzeti jogának megfelelően felel az érintettnek okozott minden kárért.

Kilátások

Az Európai Bizottság 2013 júliusában az Eurojust reformjára vonatkozó rendeletre irányuló javaslatot terjesztett elő. Ezt a javaslatot egy másik javaslat kísérte, amely az Európai Ügyészség létrehozására irányult (lásd alább). Ennek a rendeletnek a célja, hogy oly módon egyszerűsítse a funkciókat és a szervezet felépítését, hogy azok összhangban legyenek a Lisszaboni Szerződéssel. A reform célja továbbá, hogy egyértelműen különválassza az Eurojust operatív feladatait – amelyeket az Eurojust testülete lát el – és adminisztratív feladatait. Ez lehetővé teszi majd a tagállamoknak, hogy jobban összpontosítsanak az operatív feladatokra. Létrehozásra kerül egy új végrehajtó bizottság, hogy segítse a testület munkáját az adminisztratív feladatok ellátása során.[835]

Az Európai Ügyészség

A tagállamok kizárólagos hatáskörébe tartozik a csalás terén elkövetett bűncselekmények és az uniós költségvetés helytelen alkalmazásának büntetőeljárás alá vonása, amelynek határokon átnyúló vonzatai is lehetnek. Egyre fontosabb – különösen a folyamatos gazdasági válság következtében – hogy az ilyen bűncselekmények elkövetőit felkutassák, velük szemben a nyomozást folytassanak le és bíróság elé állítsák őket.[836] Az Európai Bizottság javaslatot tett egy független európai ügyészség létrehozására irányuló rendeletre[837] abból a célból, hogy üldözze az Unió pénzügyi érdekeit sértő bűncselekményeket. Az Európai Ügyészséget fokozott együttműködési eljáráson keresztül hozza létre, amely lehetővé teszi legalább hat tagállam számára, hogy megerősített együttműködést építsenek ki az uniós

835 Lásd az Európai Bizottság Eurojustról szóló weboldalát.

836 Lásd: Európai Bizottság (2013), A Bizottság javaslata az Európai Ügyészség létrehozásáról szóló tanácsi rendeletre, COM(2013) 534 final, Brüsszel, 2013. július 17., 1. o., és a Bizottság Európai Ügyészségről szóló weboldala.

837 Európa Bizottság (2013), A Bizottság javaslata az Európai Ügyészség létrehozásáról szóló tanácsi rendeletre, COM(2013) 534 final, Brüsszel, 2013. július 17.

struktúrán belül a több uniós ország bevonása nélkül.[838] Belgium, Bulgária, Ciprus, a Cseh Köztársaság, Észtország, Finnország, Franciaország, Görögország, Horvátország, Lettország, Litvánia, Luxemburg, Németország, Portugália, Románia, Spanyolország, Szlovákia és Szlovénia mind csatlakozott a megerősített együttműködéshez, Ausztria és Olaszország pedig kifejezte csatlakozási szándékát.[839]

Az Európai Ügyészség hatásköre kiterjed majd az uniós csalások és az EU pénzügyi érdekeit érintő egyéb bűncselekmények kivizsgálására és büntetőeljárás alá vonására abból a célból, hogy hatékonyan koordinálja a nyomozásokat és a büntetőeljárás alá vonásokat a különböző nemzeti jogrendek között, és hogy javítsa az erőforrások felhasználását és az információcserét európai szinten.[840]

Az Európai Ügyészség vezetője egy európai ügyész lesz, és minden tagállamban legalább egy delegált európai ügyész lesz, aki az adott tagállamban felel a nyomozások lefolytatásáért és büntetőeljárás alá vonásért.

A javaslat erős garanciákat határoz meg az Európai Ügyészség nyomozásaiban érintett személyek nemzeti jogban, uniós jogban, és az EU Alapjogi Chartájában rögzített jogainak garantálása érdekében. A többnyire alapjogokat érintő vizsgálati intézkedéseket előzetesen jóvá kell hagyatni egy nemzeti bírósággal.[841] Az Európai Ügyészség nyomozásai a nemzeti bíróságok bírósági felülvizsgálata alá fog tartozni.[842]

Az uniós intézmények adatvédelmi rendelete[843] alkalmazandó lesz majd az Európai Ügyészség által az adminisztratív jellegű személyes adatok tekintetében végzett adatkezelésre. Az operatív ügyekkel kapcsolatos személyes adatok kezeléséhez, csakúgy, mint az Europol esetében, az Európai Ügyészségnek is lesz az Europol és Eurojust tevékenységeit szabályozóhoz hasonló külön adatvédelmi rendszere, figyelemmel arra, hogy az Európai Ügyészség funkciói tagállami szinten érintik

838 Az EU működéséről szóló szerződés, 86. cikk (1) bekezdés és 329. cikk (1) bekezdés.

839 Lásd: az Európai Unió Tanácsa (2017), 20 tagállam megállapodott az Európai ügyészség létrehozásának részleteiről, sajtóközlemény, 2017. június 8.

840 Európa Bizottság (2013), A Bizottság javaslata az Európai Ügyészség létrehozásáról szóló tanácsi rendeletre, COM(2013) 534 final, Brüsszel, 2013. július 17., 1. o. és 51–51.o. Lásd a Bizottság weboldalát az Európai Ügyészségről.

841 Európa Bizottság (2013), A Bizottság javaslata az Európai Ügyészség létrehozásáról szóló tanácsi rendeletre, COM(2013) 534 final, Brüsszel, 2013. július 17., 26. cikk (4) bekezdés.

842 *Uo.*, 36. cikk.

843 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

majd a bűnüldöző hatóságok és nemzeti ügyészségek által tárolt személyes adatok kezelését. Az Európai Ügyészségre vonatkozó adatvédelmi szabályok ezért szinte azonosak a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvben foglalt szabályokkal. Az Európai Ügyészség létrehozására irányuló javaslat szerint a személyes adatok kezelését a jogszerűség és tisztességesség, a célhoz kötöttség, az adattakarékosság, pontosság, integritás és bizalmas jelleg elvének betartásával kell végezni. Az Európai Ügyészség köteles, amennyire lehet, világos különbséget tenni a különböző típusú érintettek – így például a bűncselekményért elítéltek, a pusztán gyanúsítottak, áldozatok és tanúk – személyes adatai között. Törekednie kell továbbá arra, hogy ellenőrizze a kezelt személyes adatok minőségét, és amennyiben lehetséges, különbséget tegyen a tényeken alapuló és a személyes értékelésen alapuló személyes adatok között.

A javaslat tartalmaz rendelkezéseket az egyének jogaira, nevezetesen a tájékoztatáshoz való jogra, a személyes adatokhoz való hozzáférés jogára, a helyesbítéshez és törléshez való jogra, valamint az adatkezelés korlátozására való jogra vonatkozóan, és rendelkezik arról, hogy az ilyen jogok közvetetten, az európai adatvédelmi biztoson keresztül is gyakorolhatók. Kitér továbbá az adatkezelés biztonságára és az elszámoltathatóság elvére, és előírja az Európai Ügyészség számára, hogy hajtson végre megfelelő technikai és szervezési intézkedéseket az adatkezelés által jelentett kockázatokkal arányos biztonsági szint biztosítására, vezessen nyilvántartást valamennyi adatkezelési tevékenységről és az adatkezelés előtt végezzen adatvédelmi hatásvizsgálatot azokban az esetekben, amikor az adatkezelés típusa (például adatkezelés új technológiák alkalmazásával) valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve. Végezetül pedig a javaslat rendelkezik arról, hogy a testület nevezzen ki adatvédelmi tisztviselőt, akit megfelelően be kell vonni a személyes adatok védelméhez kapcsolódó minden kérdésbe, és biztosítania kell, hogy az Európai Ügyészség betartsa az alkalmazandó adatvédelmi jogszabályokat.

8.3.2 Adatvédelem az uniós szintű közös információs rendszerekben

A tagállamok közötti információcserére és a határokon átnyúló bűncselekmények elleni küzdelemre szakosodott uniós hatóságok – például az Europol, Eurojust és az EPPO – létrehozásán túl számos közös információs rendszert hoztak létre uniós szinten, hogy meghatározott bűnüldözési célokra – köztük a határvédelem, bevándorlás és menekültügy, valamint a vámügy területén – lehetővé tegyék és

megkönnyítsék az együttműködést és az adatcserét a hatáskörrel rendelkező nemzeti és uniós hatóságok számára. Mivel a schengeni térséget először az unós jogtól független nemzetközi megállapodással hozták létre, a Schengeni Információs Rendszer (SIS) többoldalú megállapodások nyomán alakult ki és később vonták csak az uniós jog alá. A Vízuminformációs Rendszert (VIS), az Eurodac-ot, az Eurosur-t és a váminformációs rendszert (CIS) az uniós jog által szabályozott eszközként hozták létre.

E rendszerek feletti felügyeletet a nemzetközi felügyeleti hatóságok és az európai adatvédelmi biztos közösen gyakorolják. Ezek a hatóságok együttműködnek a felügyeleti koordinációs csoportokkal a magas szintű védelem biztosítása érdekében. Ez a következő nagyméretű IT-rendszereket foglalja magában: 1) Eurodac; 2) Vízuminformációs Rendszer; 3) Schengeni Információs Rendszer; 4) váminformációs rendszer és 5) a belső piaci információs rendszer.[844] A felügyeleti koordinációs csoportok rendszerint évente kétszer üléseznek egy megválasztott elnök irányítása alatt, és iránymutatásokat fogadnak el, határokon átnyúló ügyeket vitatnak meg, vagy ellenőrzésekre vonatkozó közös kereteket fogadnak el.

A 2012-ben létrehozott, nagyméretű informatikai rendszerekkel foglalkozó európai ügynökség (eu-LISA)[845] feladata a második generációs Schengeni Információs Rendszer (SIS II), a Vízuminformációs Rendszer (VIS) és az Eurodac üzemeltetési igazgatása. Az eu-LISA alapfeladata az információtechnológiai rendszerek hatékony, biztonságos és folyamatos működésének biztosítása. Feladatai közé tartozik ezenkívül, hogy elfogadja a rendszerek biztonságossága és az adatbiztonság szavatolásához szükséges intézkedéseket.

A Schengeni Információs Rendszer

1985-ben a korábbi Európai Közösség több tagállama, a Benelux Unió államai, Németország és Franciaország között megállapodás jött létre a közös határaikon történő ellenőrzések fokozatos megszüntetéséről (Schengeni Megállapodás), amelynek célja a személyek szabad, a schengeni területen belül határellenőrzéstől mentes mozgását biztosító térség létrehozása volt.[846] A nyitott határokból fakadó, a közbiz-

844 Lásd az Európai adatvédelmi biztos weboldalát a felügyeleti koordinációra vonatkozóan.

845 Az Európai Parlament és a Tanács 1077/2011/EU rendelete (2011. október 25.) a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző európai ügynökség létrehozásáról, HL L 286., 2011.11.1.

846 Megállapodás a Benelux Gazdasági Unió államai, a Németországi Szövetségi Köztársaság és a Francia Köztársaság kormányai között a közös határaikon történő ellenőrzések fokozatos megszüntetéséről, HL L 239., 2000.9.22.

tonságot fenyegető veszély ellensúlyozására megerősített határellenőrzést vezettek be a schengeni térség külső határain, és szoros együttműködést hoztak létre a nemzeti rendőri és igazságügyi hatóságok között.

Mivel a Schengeni Megállapodáshoz további államok is csatlakoztak, a schengeni rendszert végül az Amszterdami Szerződéssel beépítették az uniós jogi keretbe.[847] E határozat végrehajtására 1999-ben került sor. A Schengeni Információs Rendszer legújabb verziója, az ún. SIS II, 2013. április 9-én kezdte meg működését. Jelenleg az uniós tagállamok többségét,[848] valamint Izlandot, Liechtensteint, Norvégiát és Svájcot is kiszolgálja.[849] Az Europol és az Eurojust is rendelkezik hozzáféréssel a SIS II-höz.

A SIS II egy központi rendszerből (C-SIS), a tagállamokban található nemzeti rendszerekből, valamint a központi rendszer és a nemzeti rendszerek közötti kommunikációs infrastruktúrából áll. A C-SIS a tagállamok által a rendszerbe bevitt, személyekre és tárgyakra vonatkozó adatokat tartalmaz. A SIS-t az egész schengeni övezetben megtalálható nemzeti határellenőrzési, rendőri, vám-, vízum- és igazságszolgáltatási hatóságok használják. Minden tagállam a C-SIS nemzeti másolatát, a „nemzeti schengeni információs rendszerek" (N-SIS) néven ismert rendszereket üzemelteti, amelyeket folyamatosan frissítenek, így a C-SIS is frissül. A SIS különböző típusú figyelmeztető jelzéseket ad ki:

- a személy nem jogosult a schengeni területre való belépésre vagy az ott tartózkodásra; vagy
- a személyt vagy tárgyat igazságszolgáltatási vagy bűnüldöző hatóságok keresik (pl. európai elfogatóparancs, rejtett ellenőrzés iránti kérelmek); vagy
- a személy eltűnését jelentették; vagy

847 Európai Közösségek (1997), Amszterdami Szerződés az Európai Unióról szóló szerződés, az Európai Közösségeket létrehozó szerződések és egyes kapcsolódó okmányok módosításáról, HL C 340., 1997.11.10.

848 Ciprus, Horvátország és Írország előkészítő tevékenységeket végeznek a SIS II-höz való csatlakozás érdekében, azonban még nem képezik részét annak. Lásd a Schengeni Információs Rendszerre vonatkozó tájékoztatást az Európai Bizottság Migrációügyi és Uniós Belügyi Főigazgatóságának weboldalán.

849 Az Európai Parlament és a Tanács 1987/2006/EK rendelete (2006. december 20.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról, HL L 381., 2006.12.28.; az Európai Unió Tanácsa (2007), A Tanács 2007/533/IB határozata (2007. június 12.) a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról, HL L 205., 2007.8.7.

- az árukat, köztük bankjegyeket, gépjárműveket, tehergépjárműveket, lőfegyvereket és azonosító okmányokat ellopott vagy elveszett dologként bejelentették.

Figyelmeztető jelzés esetén nyomon követést kell kezdeményezni a SIRENE-irodákon keresztül. A SIS II-nek új funkciói is vannak, mint pl. a lehetőség a következők bevitelére a rendszerbe: biometrikus adatok, köztük ujjlenyomatok és fényképek; a figyelmeztető jelzések új kategóriái: pl. ellopott hajók, légi járművek, konténerek vagy fizetőeszközök; fokozott figyelmeztető jelzések személyekre és tárgyakra vonatkozóan; átadás vagy kiadatás céljából körözött személyekre vonatkozó európai elfogatóparancsok (EEP) másolatai.

A SIS II rendszer két egymást kiegészítő jogi aktuson alapul: a SIS II határozaton[850] és a SIS II rendeleten.[851] Az uniós jogalkotó különböző jogalapot alkalmazott a határozat és a rendelet elfogadásához. A határozat az SIS II alkalmazását szabályozza a büntetőügyekben folytatott rendőrségi és igazságszolgáltatási együttműködés által lefedett célok tekintetében (az EU korábbi harmadik pillére EU). A rendelet a vízumokról, menekültügyről, bevándorlásról és a személyek szabad mozgására vonatkozó egyéb politikák alá tartozó figyelmeztető jelzésekkel kapcsolatos eljárásokra vonatkozik (a korábbi első pillér). A riasztási eljárásokat minden egyes pillér tekintetében külön jogi aktussal kellett szabályozni, figyelemmel arra, hogy a két jogi aktust még a Lisszaboni Szerződés és a pilléres szerkezet eltörlése előtt fogadták el.

Mindkét jogi aktus tartalmaz adatvédelmi szabályokat. Az SIS II határozat tiltja a különleges adatok kezelését.[852] A személyes adatok kezelése a Korszerűsített 108. Egyezmény hatálya alá tartozik.[853] Továbbá a személyeknek joguk van hozzáférni a SIS II rendszerben rögzített és rájuk vonatkozó személyes adatokhoz.[854]

A SIS II rendelet szabályozza a figyelmeztető jelzések rendszerben történő rögzítésének és feldolgozásának feltételeit és eljárásait a nem uniós állampolgárok belépésének vagy tartózkodásának megtagadását illetően. Szabályokat állapít meg

850 A Tanács 2007. június 12-i 2007/533/IB határozata a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról, HL L 205., 2007.8.7.

851 Az Európai Parlament és a Tanács 2006. december 20-i 1987/2006/EK rendelete a Schengeni Információs Rendszer második generációjának (SIS II) létrehozásáról, működtetéséről és használatáról, HL L 381., 2006.12.28.

852 SIS II határozat, 56. cikk; SIS II rendelet, 40. cikk.

853 SIS II határozat, 57. cikk.

854 *Uo.*, 58. cikk; SIS II rendelet, 41. cikk.

továbbá a kiegészítő információk cseréjére vonatkozóan valamely tagállamba történő belépés vagy ott tartózkodás céljából.[855] A rendelet az adatvédelemre vonatkozó szabályokat is tartalmaz. Az általános adatvédelmi rendelet 9. cikkének (1) bekezdése szerinti különleges adatok kezelése nem megengedett.[856] A SIS II rendelet megállapít bizonyos jogokat az érintettek számára, amelyek a következők:

- az érintettre vonatkozó személyes adatokhoz való hozzáférés joga;[857]
- a ténylegesen pontatlan adatok helyesbítéséhez való jog;[858]
- a jogszerűtlenül tárolt adatok törléséhez való jog;[859] és
- tájékoztatáshoz való jog, ha figyelmeztető jelzést adtak ki az érintett ellen. A tájékoztatást írásban kell megadni a figyelmeztető jelzés alapjául szolgáló nemzeti határozat egy csatolt példányával vagy a határozatra való hivatkozással.[860]

A tájékoztatást nem kell megadni, ha 1) a személyes adatot nem az érintett harmadik országbeli állampolgártól szerezték be és a tájékoztatás lehetetlennek bizonyul, vagy aránytalan erőfeszítéssel járna, 2) az érintett már rendelkezik az információval vagy 3) a nemzeti jog lehetővé teszi e jog korlátozását, többek között a nemzetbiztonság védelme vagy bűncselekmények megelőzése érdekében.[861]

A SIS II határozat és SIS II rendelet esetében is az egyének SIS II rendszerre vonatkozó hozzáférési joga bármely tagállamban gyakorolható, és azt az adott tagállam nemzeti jogával összhangban kell biztosítani.[862]

855 SIS II rendelet, 2. cikk.
856 *Uo.*, 40. cikk.
857 *Uo.*, 41. cikk (1) bekezdés.
858 *Uo.*, 41. cikk (5) bekezdés.
859 *Uo.*, 41. cikk (5) bekezdés.
860 *Uo.*, 42. cikk (1) bekezdés.
861 *Uo.*, 42. cikk (2) bekezdés.
862 *Uo.*, 41. cikk (1) bekezdés; SIS II határozat, 58. cikk.

Példa: A *Dalea kontra Franciaország* ügyben[863] a felperestől megtagadták a francia beutazó vízumot, mivel a francia hatóságok bejelentették a Schengeni Információs Rendszerben, hogy a felperes beutazási kérelmét el kell utasítani. A felperes sikertelenül kérte a francia adatvédelmi hatóságtól, majd az Államtanácstól az adataihoz való hozzáférést, továbbá adatainak helyesbítését vagy törlését. Az EJEB megállapította, hogy a felperes Schengeni Információs Rendszerbe történt bejelentése megfelelt a jogszabályoknak, és a nemzetbiztonság védelmének törvényes célját szolgálta. Mivel a felperes nem mutatta ki, hogy ténylegesen milyen hátrányt szenvedett a schengeni övezetbe való belépésének meghiúsulása miatt, és mivel megfelelő intézkedések álltak rendelkezésre arra, hogy megvédjék őt az önkényes döntéshozataltól, a magánélet tiszteletben tartásához való jogába való beavatkozás arányos volt. A felperes 8. cikk szerinti panaszát ezért elfogadhatatlannak nyilvánították.

A hatáskörrel rendelkező nemzeti felügyeleti hatóság minden tagállamban felügyeletet gyakorol a hazai N-SIS felett. A nemzeti felügyeleti hatóságnak biztosítania kell, hogy legalább négyévente sor kerül a belföldi N-SIS-en belül az adatfeldolgozó tevékenységek ellenőrzésére.[864] A nemzeti felügyeleti hatóságok és az európai adatvédelmi biztos együttműködnek egymással, és biztosítják az N-SIS összehangolt felügyeletét, míg az európai adatvédelmi biztos felel a C-SIS felügyeletéért. Az átláthatóság érdekében kétévente közös tevékenységi jelentést küldenek az Európai Parlamentnek, a Tanácsnak és az eu-LISA-nak. A SIS II felügyeleti koordinációs csoportot azért hozták létre, hogy biztosítsa a SIS felügyeletének koordinációját. A csoport évente kétszer ülésezik. Tagjai az európai adatvédelmi biztos és azon tagállamok felügyeleti hatóságainak a képviselői, amelyek végrehajtották a SIS II-t, továbbá Izland, Lichtenstein, Norvégia és Svájc, mivel a SIS rájuk is vonatkozik, ugyanis ezek az országok is a schengeni rendszer tagjai.[865] Ciprus, Horvátország és Írország még nem részesei a SIS II rendszernek, ezért csak megfigyelőként vesznek részt a felügyeleti koordinációs csoport munkájában. A felügyeleti koordinációs csoport összefüggésében az európai adatvédelmi biztos és a nemzeti felügyeleti hatóságok aktívan együttműködnek: kicserélik egymás között a vonatkozó információkat, közös ellenőrzések és vizsgálatok lefolytatásában egymást segítik, segítséget nyújtanak egymásnak az ellenőrzése és vizsgálatok lefolytatásában, összehangolt javaslatokat dolgoznak ki a problémák közös megoldására és szükség

863 EJEB, *Dalea kontra Franciaország*, 964/07. sz. ügy, 2010. február 2.

864 SIS II rendelet, 60. cikk (2) bekezdés.

865 Lásd az európai adatvédelmi biztos weboldalát a Schengeni Információs Rendszerre vonatkozóan.

szerint előmozdítják az adatvédelmi jogokkal kapcsolatos ismeretek terjesztését.[866] A SIS II felügyeleti koordinációs csoport irányelveket is elfogad, hogy segítse az érintetteket. Egy példa erre az érintetteket a hozzáférési joguk gyakorlásában segítő útmutató.[867]

Kilátások

2016-ban az Európai Bizottság elvégezte a SIS[868] értékelését, amely kimutatta, hogy nemzeti mechanizmusokat léptettek életbe annak érdekében, hogy lehetővé tegyék az érintettek számára, hogy hozzáférjenek a SIS II-ben tárolt személyes adataikhoz, helyesbítsék vagy töröltessék azokat, vagy a pontatlan adatokkal összefüggésben kártérítést igényeljenek. A SIS II hatékonyságának és eredményességének javítása érdekében az Európai Bizottság három rendeletre irányuló javaslatot terjesztett elő:

- egy a SIS határellenőrzések terén történő létrehozásáról, működtetéséről és használatáról szóló rendelet, amely hatályon kívül helyezi a SIS II rendeletet;

- egy a SIS büntetőügyekben folytatott rendőrségi és igazságszolgáltatási együttműködés terén történő létrehozásáról, működtetéséről és használatáról szóló rendelet, amely hatályon kívül helyezi a SIS II határozatot;

- egy a SIS harmadik országok jogellenesen tartózkodó állampolgárainak visszaküldése terén történő használatáról szóló rendeletet.

Fontos, hogy a javaslatok megengedik a biometrikus adatok SIS II rendszernek már most is részét képező fényképeken és ujjlenyomatokon kívüli egyéb kategóriáinak kezelését. Arcképet és ujjlenyomatokat, tenyérnyomatokat és DNS-profilokat is tárolnak majd a SIS adatbázisban. Ezenkívül, miközben a SIS II rendelet és a SIS II határozat biztosította annak lehetőségét, hogy ujjlenyomat alapján történő kereséssel lehessen azonosítani egy személyt, a javaslatok ezt a keresést kötelezővé teszik akkor, ha az illető személyazonossága más módon nem állapítható meg. A rendszerben való kereséshez és az egyének azonosításához arcképet, ujjlenyomatokat és

866 SIS II rendelet, 46. cikk és SIS II határozat, 62. cikk.

867 Lásd: SIS II felügyeleti koordinációs csoport, *A Schengeni Információs Rendszer Útmutató a hozzáférési jog gyakorlásához*, amely elérhető az európai adatvédelmi biztos weboldalán.

868 Európai Bizottság (2016), A Bizottság jelentése a Tanácsnak és az Európai Parlamentnek az 1987/2006/EK rendelet 24. cikkének (5) bekezdésével, 43. cikkének (3) bekezdésével és 50. cikkének (5) bekezdésével, valamint a 2007/533/IB határozat 59. cikkének (3) bekezdésével és 66. cikkének (5) bekezdésével összhangban a Schengeni Információs Rendszer második generációjának (SIS II) értékeléséről, COM(2016) 880 final, Brüsszel, 2016. december 21.

tenyérnyomatokat fognak használni, amint az technikailag lehetségessé válik. A biometrikus tulajdonságokra vonatkozó új szabályok különös kockázatot jelentenek az egyének jogaira nézve. A Bizottság határozataira vonatkozóan megfogalmazott véleményében[869] az európai adatvédelmi biztos megjegyezte, hogy a biometrikus adatok rendkívül különleges adatnak minősülnek, és bevezetésük egy ilyen nagyméretű adatbázisba, mint a SIS rendszer, a szükségesség megállapítására irányuló bizonyíték alapú értékelésen kell, hogy alapuljon. Másképp fogalmazva, igazolni kell, hogy valóban szükséges az új tulajdonságok kezelése. Az európai adatvédelmi biztos továbbá úgy vélte, hogy szükséges tovább pontosítani azt, hogy milyen típusú adatok szerepelhetnek a DNS-profilban. Mivel a DNS-profil tartalmazhat különleges adatokat (a legnyilvánvalóbb példa erre az egészségügyi problémákat feltáró adatok), a SIS-ban tárolt DNS-profiloknak a következőket kellene tartalmazniuk: „csak azt a minimális információt, amely feltétlenül szükséges az eltűnt személyek azonosításához, és nem tartalmazhatnak kifejezetten egészségügyi információkat, faji eredetre vonatkozó vagy egyéb különleges adatokat."[870] A javaslatok ugyanakkor további garanciákat biztosítanak az adatok gyűjtésének és további kezelésének a feltétlenül szükséges és a feladatok ellátásához szükséges mértékűre korlátozásához, és a hozzáférést azon személyekre korlátozzák, akik esetében a személyes adatok kezelése a feladatuk ellátásához szükséges.[871] A javaslatok ezenkívül felhatalmazzák az eu-LISA-t, hogy rendszeres időközönként készítsen az adatminőségre vonatkozó jelentéseket a tagállamok számára, hogy rendszeresen ellenőrizzék a riasztásokat az adatminőség biztosítása érdekében.[872]

869 Európai adatvédelmi biztos (2017), Az európai adatvédelmi biztos véleménye a Schengeni Információs Rendszer új jogalapjáról, 7/2017. sz. vélemény, 2017. május 2.

870 *Uo.*, 22. pont

871 Európai Bizottság (2016), A büntetőügyekben folytatott rendőrségi és igazságügyi együttműködés terén a Schengeni Információs Rendszer (SIS) létrehozásáról, működéséről és használatáról, valamint az 515/2014/EU rendelet módosításáról, továbbá az 1986/2006/EK rendelet, a 2007/533/IB tanácsi határozat és a 2010/261/EU bizottsági határozat hatályon kívül helyezéséről szóló európai parlamenti és tanácsi rendeletre vonatkozó javaslat, COM(2016) 883 final, Brüsszel, 2016. december 21.

872 *Uo.*, 15. o.

A Vízuminformációs Rendszer

A szintén az eu-LISA által üzemeltetett Vízuminformációs Rendszert (VIS) a közös uniós vízumpolitika végrehajtásának támogatására fejlesztették ki.[873] A VIS lehetővé teszi a schengeni államok számára, hogy egy, a schengeni államok nem uniós országokban található konzulátusai az összes schengeni állam külső határátkelőhelyeivel összekötő központosított rendszeren keresztül kicseréljék a vízumkérelmekre vonatkozó adatokat. A VIS a schengeni térségben való rövid távú tartózkodásra vagy a schengeni térségen való átutazásra jogosító vízumok iránti kérelmek adatait dolgozza fel. A VIS lehetővé teszi, hogy a határőrizeti hatóságok biometrikus tulajdonságok, nevezetesen ujjlenyomatok segítségével ellenőrizzék, hogy a vízumot bemutató személy annak jogos tulajdonosa-e, továbbá azonosítsák a hamis dokumentumokkal rendelkező vagy dokumentumokkal egyáltalán nem rendelkező személyeket.

A vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről szóló 767/2008/EK európai parlamenti és a tanácsi rendelet (VIS-rendelet) a személyes adatok továbbítására vonatkozó feltételeket és eljárásokat szabályozza rövid távú tartózkodásra jogosító vízumkérelmek tekintetében. Felügyeli továbbá a kérelmekkel kapcsolatban hozott határozatokat, beleértve a vízum törlésére, visszavonására vagy meghosszabbítására vonatkozó határozatokat.[874] A VIS-rendelet többnyire a kérelmezőre, a kérelmező vízumára, fényképeire, ujjlenyomataira, korábbi kérelmekkel való kapcsolatokra utaló adatokkal, illetve a kísérő személy kérelmével, illetve személyek meghívására vonatkozó adatokkal foglalkozik.[875] Adatok bevitele, módosítása vagy törlése céljából kizárólag a vízumhatóságok férhetnek hozzá a VIS-hez, míg adategyeztetés céljából a vízumhatóságokon kívül a külső határátkelőhelyeken végzett ellenőrzésekre, az idegenrendészeti ellenőrzésre hatáskörrel rendelkező, valamint a menekültügyi hatóságok is hozzáférhetnek a rendszerhez.

873 Az Európai Unió Tanácsa (2004), A Tanács 2004/512/EK határozata (2004. június 8.) a Vízuminformációs Rendszer létrehozásáról (VIS), HL L 213., 2004.6.15.; Az Európai Parlament és a Tanács 767/2008/EK rendelete (2008. július 9.) a vízuminformációs rendszerről (VIS) és a rövid távú tartózkodásra jogosító vízumokra vonatkozó adatok tagállamok közötti cseréjéről (VIS-rendelet), HL L 218., 2008.8.13.; Az Európai Unió Tanácsa (2008), A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről, HL L 218., 2008.8.13.

874 VIS-rendelet, 1. cikk.

875 *Uo.*, 5. cikk.

Bizonyos körülmények között – súlyos terrorista cselekmény vagy bűncselekmény megelőzése, felderítése vagy kivizsgálása céljából – az illetékes nemzeti rendőri hatóságok és az Europol is hozzáférést kérhetnek a VIS-be bevitt adatokhoz.[876] Mivel a VIS-t a közös vízumpolitika végrehajtását támogató eszköznek szánták, a 3.2. fejezetben tárgyalt célhoz kötöttség elve, amely előírja, hogy a személyes adatok kezelése kizárólag meghatározott, egyértelmű és törvényes célokból történhet, és a személyes adatok kezelésük célja szempontjából megfelelőek, relevánsak és nem túlzott mértékűek legyenek, sérülne, ha a VIS-t bűnüldözési eszközzé alakítanák. Ebből az okból a nemzeti bűnüldöző hatóságok és az Europol nem kapott rutinszerű hozzáférést a VIS-adatbázishoz. Hozzáférés csak eseti alapon adható, és azt szigorú garanciáknak kell kísérnie. E hatóságok VIS-hez való hozzáférésére és abba való betekintésére vonatkozó feltételeket és garanciákat a 2008/633/IB tanácsi határozat szabályozza.[877]

A VIS-rendelet továbbá rögzíti az érintettek jogait. Ezek a következők:

- Arra való jog, hogy a felelős tagállam tájékoztassa az érintettet az adott tagállamban a személyes adatok kezeléséért felelős adatkezelő kilétéről és elérhetőségéről, személyes adati VIS-ben történő kezelésének céljairól, azon személyek kategóriáiról, akiknek az adatok továbbíthatók (címzettek), valamint az adatmegőrzési időről. Ezenkívül a vízumkérelmezőket tájékoztatni kell annak tényéről, hogy személyes adataik gyűjtése a VIS alapján kötelező kérelmük kivizsgálásához, míg a tagállamoknak tájékoztatniuk kell az érintetteket azon jogukról is, hogy hozzáférhetnek a róluk tárolt adatokhoz, kérhetik azok helyesbítését vagy törlését, valamint e jogaik gyakorlását lehetővé tevő eljárásokról.[878]

- A VIS-ben rögzített, érintetthez kapcsolódó adatokhoz való hozzáférés joga.[879]

- A pontatlan adatok helyesbítéséhez való jog.[880]

876 Az Európai Unió Tanácsa (2008), A Tanács 2008/633/IB határozata (2008. június 23.) a vízuminformációs rendszerhez (VIS) a tagállamok kijelölt hatóságai, valamint az Europol számára a terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében, betekintés céljából történő hozzáférésről, HL L 218., 2008.8.13.

877 *Uo.*

878 VIS-rendelet, 37. cikk.

879 *Uo.*, 38. cikk (1) bekezdés.

880 *Uo.*, 38. cikk (2) bekezdés.

- A jogszerűtlenül tárolt adatok törléséhez való jog.[881]

A VIS feletti felügyelet biztosítása érdekében létrehozták a VIS felügyeleti koordinációs csoportot. Az európai adatvédelmi biztos és a nemzeti felügyeleti hatóságok képviselőiből áll, akik évente két alkalommal üléseznek. Ez a csoport a 28 uniós tagállam, valamint Izland, Lichtenstein, Norvégia és Svájc képviselőiből áll.

Eurodac

Az Eurodac neve Európai Daktiloszkópiai Rendszert jelent.[882] Az Eurodac a valamely uniós tagállamban menedékjogért folyamodó harmadik országbeli állampolgárok és hontalan személyek ujjlenyomatadatait tartalmazó központi rendszer.[883] A rendszer a 2725/2000 tanácsi rendelet elfogadásával 2003. január óta működik. A rendelet átdolgozott változata 2015 óta hatályos. Célja elsődlegesen az, „ hogy segítse annak eldöntését, hogy mely tagállam felelős megvizsgálni egy a 604/2013/EK rendelet alapján benyújtott menedékjog iránti kérelmet. Az említett rendelet megállapítja egy harmadik országbeli állampolgár vagy egy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételeket és eljárási szabályokat (Dublin III rendelet).[884] Az Eurodac-ban tárolt személyes adatok kizárólag a Dublin III rendelet alkalmazásának megkönnyítése céljából használhatók fel.[885]

881 *Uo.*, 38. cikk (2) bekezdés.

882 Lásd az Európai adatvédelmi biztos weboldalát az Eurodacra vonatkozóan.

883 A Tanács 2725/2000/EK rendelete (2000. december 11.) a dublini egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló Eurodac létrehozásáról, HL L 316., 2000.12.15.; A Tanács 407/2002/EK rendelete (2002. február 28.) a Dublini Egyezmény hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítására irányuló Eurodac létrehozásáról szóló 2725/2000/EK rendelet végrehajtására vonatkozó egyes szabályok megállapításáról, HL L 62., 2002.3.5. (Eurodac-rendelet); Az Európai Parlament és a Tanács 603/2013/EU rendelete (2013. június 26.) a harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet hatékony alkalmazása érdekében az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről, valamint a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség nagyméretű IT-rendszereinek üzemeltetési igazgatását végző ügynökség létrehozásáról szóló 1077/2011/EU rendelet módosításáról, HL L 180., 2013.6.29. (átdolgozott Eurodac-rendelet).

884 Az Európai Parlament és a Tanács 604/2013/EU rendelete (2013. június 26.) egy harmadik országbeli állampolgár vagy egy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról, HL L 180., 2013.6.29. (Dublin III Rendelet).

885 Átdolgozott Eurodac-rendelet, 1. cikk (1) bekezdés.

A nemzeti bűnüldöző hatóságok és az Europol összehasonlíthatják a bűnügyi nyomozásokhoz kapcsolódó ujjlenyomatokat az Eurodac-ban szereplő ujjlenyomatokkal, de kizárólag terrorcselekmények és egyéb súlyos bűncselekmények megelőzése, felderítése és kivizsgálása érdekében. Mivel az Eurodac-ot az EU menekültügyi politikájának végrehajtását támogató eszköznek tervezték, nem pedig bűnüldözési eszköznek, a bűnüldöző hatóságok csak egyedi esetekben, sajátos körülmények között és szigorú feltételek mellett férhetnek hozzá az adatbázishoz.[886] Az adatok további bűnüldözési célból történő felhasználásra a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelv vonatozik, míg az adatoknak a Dublin III rendelet előmozdítására irányuló fő célból történő felhasználására az általános adatvédelmi rendelet az irányadó. Valamely tagállam vagy az Europol által az átdolgozott Eurodac-rendelet alapján megszerzett személyes adatokat tilos harmadik ország, nemzetközi szervezet vagy az Unióban vagy azon kívül letelepedett magánfél számára továbbítani.[887]

Az Eurodac egy, az eu-LISA által működtetett, az ujjlenyomatok tárolására és összehasonlítására szolgáló központi egységből, valamint a tagállamok és a központi adatbázis közötti elektronikus adattovábbításokat végző rendszerből áll. A tagállamok leveszik és továbbítják minden olyan, 14. életévét betöltött személy ujjlenyomatát, aki a területükön menedékjogot kér, továbbá minden olyan, 14. életévét betöltött nem uniós állampolgár vagy hontalan személy ujjlenyomatát, akit a külső határok jogellenes átlépése miatt elfogtak. A tagállamok a területükön engedély nélkül tartózkodó nem uniós állampolgárok vagy hontalan személyek ujjlenyomatait is levehetik és továbbíthatják.

Bár a tagállamok betekinthetnek az Eurodac-ba, és kérhetik annak ujjlenyomatadatokkal való összehasonlítását, kizárólag az adatokat gyűjtő tagállam jogosult módosítani, kiegészíteni vagy törölni a központi rendszerbe általa továbbított adatokat.[888] Az adatvédelem ellenőrzése és az adatbiztonság biztosítása érdekében az eu-LISA nyilvántartást vezet minden adatkezelési tevékenységről.[889] A nemzeti felügyeleti hatóságok nyújtanak segítséget és tanácsot az érintetteknek jogaik gyakorlásával kapcsolatban.[890] Az ujjlenyomatadatok gyűjtése és továbbítása a nemzeti bíróságok

886 *Uo.*, 1. cikk (2) bekezdés.

887 *Uo.*, 35. cikk.

888 *Uo.*, 27. cikk.

889 *Uo.*, 28. cikk.

890 *Uo.*, 29. cikk.

általi bírósági felülvizsgálat alá tartozik.[891] Az uniós intézmények adatvédelmi rendelete[892] és az európai adatvédelmi biztos által gyakorolt felügyelet vonatkozik a központi rendszerben végzett adatkezelési tevékenységekre, amelyeket az Eurodac vonatkozásában az eu-LISA irányít.[893] Ha egy személy a jogszerűtlen adatkezelés vagy az Eurodac-rendelettel össze nem egyeztethető cselekmény következtében kárt szenved, az érintett személy kártérítésre jogosult az elszenvedett kárért felelős tagállamtól.[894] Hangsúlyozni kell azonban, hogy a menedékkérők különösen veszélyeztetett személyek csoportját képezik, akik gyakran hosszú és kockázatos utat vállalnak. Veszélyeztetettségük és menedékjog iránti kérelmük elbírálása alatti bizonytalan helyzetük miatt a gyakorlatban nehéznek bizonyulhat jogaik, beleértve a kártérítéshez való jogok gyakorlása.

Ahhoz, hogy az Eurodac-ot bűnüldözési célra használhassák, a tagállamoknak ki kell jelölniük azt a hatóságot, amelyik jogosult lesz hozzáférést kérni, valamint azt a hatóságot, amelyik ellenőrzi, hogy az összehasonlítás iránti kérelem jogszerű.[895] A nemzeti hatóságok és az Europol Eurodac-ban tárolt ujjlenyomatadatokhoz való hozzáférésére nagyon szigorú feltételek vonatkoznak. A megkereső hatóságnak egy indokolt elektronikus kérelmet kell benyújtania, de csak azután, hogy összehasonlította az adatokat az egyéb elérhető rendszerekben, például a nemzeti ujjlenyomat-adatbázisokban és a VIS-ben található adatokkal. Ahhoz, hogy az összehasonlítás arányos legyen, kell, hogy legyen egy kényszerítő közbiztonsági érdek. Az összehasonlításnak valóban szükségesnek kell lennie, kapcsolódnia kell egy konkrét ügyhöz és megalapozottan feltételezhetőnek kell lennie, hogy az összehasonlítás érdemben hozzájárul a szóban forgó bűncselekmények megelőzéséhez, felderítéséhez vagy kivizsgálásához, különösen akkor, ha alapos a gyanúja annak, hogy egy terrorcselekmény vagy más súlyos bűncselekmény gyanúsítottja, elkövetője vagy áldozata az Eurodac-rendszer szerinti ujjlenyomatgyűjtés alá tartozó valamely kategóriába tartozik. Az összehasonlítás kizárólag ujjlenyomatadatok alapján végezhető el. Az Europolnak szintén be kell szereznie az ujjlenyomatot gyűjtő tagállam engedélyét.

891 *Uo.*, 29. cikk.

892 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

893 Átdolgozott Eurodac-rendelet, 31. cikk.

894 *Uo.*, 37. cikk.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies Tallinn University of Technology*, 5. évf., 2. sz. , 108–129. o.

Az Eurodac-ban tárolt, menedékkérőkre vonatkozó személyes adatokat az ujjlenyomatvétel napjától számított 10 évig őrzik meg, kivéve, ha az érintett valamelyik uniós tagállamban állampolgárságot szerez. Ebben az esetben az adatokat azonnal törölni kell. A külső határok jogellenes átlépése miatt elfogott külföldi állampolgárokra vonatkozó adatokat 18 hónapig tárolják. Ezeket az adatokat azonnal törölni kell, ha az érintett tartózkodási engedélyt kap, elhagyja az EU területét, vagy uniós tagállamban állampolgárságot szerez. Azon személyek adatai, akik menedékjogot kaptak, további három évig elérhetők lesznek összehasonlítás céljából a terrorcselekmények és egyéb súlyos bűncselekmények megelőzésének, felderítésének és kivizsgálásának összefüggésében.

Az uniós tagállamokon kívül – nemzetközi megállapodások alapján – Izland, Norvégia, Liechtenstein és Svájc is alkalmazza az Eurodac-ot.

Az Eurodac felügyeletének biztosítására létrehozták a felügyeleti koordinációs csoportot. Az európai adatvédelmi biztos és a nemzeti felügyeleti hatóságok képviselőiből áll, akik évente két alkalommal üléseznek. Ez a csoport a 28 uniós tagállam, valamint Izland, Lichtenstein, Norvégia és Svájc képviselőiből áll.[896]

Kilátások

2016 májusában a közös európai menekültügyi rendszer (CEAS) működésének javítását célzó reform részeként a Bizottság javaslatot adott ki az Eurodac-rendelet ismételt átdolgozására.[897] A javasolt átdolgozás fontos, mivel az jelentősen kibővíti az eredeti Eurodac adatbázis terjedelmét. Az Eurodac létrehozásának eredeti célja a közös európai menekültügyi rendszer támogatása volt ujjlenyomat alapú bizonyítékok szolgáltatásával annak megállapítására, hogy melyik tagállam felelős az EU-ban benyújtott menedékjog iránti kérelem megvizsgálásáért. A javasolt átdolgozás kiterjeszti az adatbázis hatáskörét, hogy megkönnyítse a szabálytalan bevándorlók visszaküldését.[898] A nemzeti hatóságok betekinthetnek majd az adatbázisba abból a célból, hogy azonosítsák azokat a harmadik országbeli állampolgárokat, akik

896 Lásd az európai adatvédelmi biztos weboldalát az Eurodacra vonatkozóan.

897 Európai Bizottság, Javaslat [A harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet] hatékony alkalmazása érdekében a jogellenesen tartózkodó harmadik országbeli állampolgár vagy hontalan személy azonosítása céljából, az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről szóló európai parlamenti és tanácsi rendeletre (átdolgozás), COM(2016) 272 final, 2016. május 4.

898 Lásd a javaslat indokolását, 3. oldal.

szabálytalanul tartózkodnak az EU-ban, vagy akik szabálytalanul léptek be az EU-ba annak érdekében, hogy bizonyítékot gyűjtsenek, amellyel segítik a tagállamokat e személyek visszaküldésében. Ezenkívül a jelenleg érvényben lévő jogi szabályozás csak az ujjlenyomatok gyűjtését és tárolását írja elő, a javaslat pedig bevezeti az egyének arcképének[899] a gyűjtését is, amely egy másik típusú biometrikus adat. A javaslat továbbá csökkentené azt az életkort, amelytől a gyermekektől biometrikus adat gyűjthető – ez a jelenlegi 14 év helyett hat év lenne[900], ami a 2013-as rendelet szerinti alsó korhatár. A javaslat kiterjesztett alkalmazási köre azt jelenti, hogy az adatbázisba esetleg bekerülő egyének magánélethez és adatvédelemhez fűződő jogaiba való több beavatkozást fog eredményezni. E beavatkozás ellensúlyozására a javaslat és az Európai Parlament LIBE bizottsága[901] által javasolt módosítások igyekeznek szigorítani az adatvédelmi követelményeket. A kézikönyv megszövegezése idején folyamatban volt a javaslat megvitatása az Európai Parlament és a Tanács előtt.

EUROSUR

Az európai határőrizeti rendszert (Eurosur)[902] a schengeni külső határok ellenőrzésének – a szabálytalan bevándorlás és a határokon átnyúló bűnözés felderítése, megelőzése és az ellene való küzdelem útján történő – megerősítésére hozták létre. Fokozza az információcserét és az operatív együttműködést a nemzeti koordinációs központok és a Frontex között, mely utóbbi az integrált határigazgatás új

899 Európai Bizottság, Javaslat [A harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet] hatékony alkalmazása érdekében a jogellenesen tartózkodó harmadik országbeli állampolgár vagy hontalan személy azonosítása céljából, az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről szóló európai parlamenti és tanácsi rendeletre (átdolgozás), COM(2016) 272 final, 2016. május 4., 2. cikk (1) bekezdés.

900 *Uo.*, 2. cikk (2) bekezdés.

901 Európai Parlament, *Jelentés [A harmadik országbeli állampolgár vagy hontalan személy által a tagállamok egyikében benyújtott nemzetközi védelem iránti kérelem megvizsgálásáért felelős tagállam meghatározására vonatkozó feltételek és eljárási szabályok megállapításáról szóló 604/2013/EU rendelet] hatékony alkalmazása érdekében a jogellenesen tartózkodó harmadik országbeli állampolgár vagy hontalan személy azonosítása céljából, az ujjlenyomatok összehasonlítását szolgáló Eurodac létrehozásáról, továbbá a tagállamok bűnüldöző hatóságai és az Europol által az Eurodac-adatokkal való, bűnüldözési célú összehasonlítások kérelmezéséről szóló európai parlamenti és tanácsi rendeletre irányuló javaslatról (átdolgozás),* PE 597.620v03-00, 2017. június 8.

902 Az Európai Parlament és a Tanács 1052/2013/EU rendelete (2013. október 22.) az európai határőrizeti rendszer (EUROSUR) létrehozásáról, HL L 295., 2013.11.6.

koncepciójának kidolgozásáért és alkalmazásáért felelős uniós ügynökség.[903] Általános célkitűzései a következők:

- az EU-ba észrevétlenül bejutó szabálytalan bevándorlók számának csökkentése;
- a szabálytalan bevándorlókat érintő tengeri halálesetek számának csökkentése, azaz több emberi élet megmentése a tengeren;
- az EU egésze belső biztonságának növelése a határokon átnyúló bűnözés megelőzéséhez való hozzájárulás révén.[904]

Az Eurosur 2013. december 2-án kezdte meg működését a külső határokkal rendelkező összes tagállamban, a többi tagállamban pedig 2014. december 1-től. A rendelet a tagállamok szárazföldi és tengeri külső határainak, valamint légi határainak őrzésére vonatkozik. Csak nagyon korlátozott mértékben cserél és kezel személyes adatokat, mivel a tagállamok és a Frontex csak a hajóazonosító számok cseréjére jogosultak. Az Eurosur operatív információkat cserél, mint például az őrjáratok és incidensek helye, és főszabályként a kicserélt információk nem tartalmazhatnak személyes adatokat.[905] Kivételes esetekben, amennyiben az Eurosur keretében kerül sor személyes adatok cseréjre, a rendelet rögzíti, hogy az általános uniós adatvédelmi jogi keretet kell alkalmazni.[906]

Az Eurosur tehát biztosítja az adatvédelemhez való jogot, mégpedig azzal, hogy kimondja, a személyes adatok cseréjére a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvben megállapított kritériumokat és garanciákat kell alkalmazni.[907]

---

903 Az Európai Parlament és a Tanács (EU) 2016/1624 rendelete (2016. szeptember 14.) az Európai Határ- és Parti Őrségről és az (EU) 2016/399 európai parlamenti és tanácsi rendelet módosításáról, valamint a 863/2007/EK európai parlamenti és tanácsi rendelet, a 2007/2004/EK tanácsi rendelet és a 2005/267/EK tanácsi határozat hatályon kívül helyezéséről, HL L 251., 2016.9.16.

904 Lásd még: Európai Bizottság (2008), A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának: Az európai határőrizeti rendszer (Eurosur) kialakításának vizsgálata, COM(2008) 68 végleges, Brüsszel, 2008. február 13.; Európai Bizottság (2011), A „Javaslat európai parlamenti és tanácsi rendeletre az európai határőrizeti rendszer (Eurosur) létrehozásáról" című dokumentumot kísérő hatásvizsgálat, bizottsági szolgálati munkadokumentum, SEC(2011) 1536 final, Brüsszel, 2011. december 12., 18. o.

905 Európai Bizottság, *EUROSUR: A schengeni térség külső határainak védelme – a migránsok életének védelme. Az EUROSUR dióhéjban*, 2013. november 29.

906 1052/2013 rendelet, (13) premabulumbekezdés és 13. cikk.

907 *Uo.*, (13) preambulumbekezdés és 13 cikk.

Váminformációs rendszer

Egy másik, uniós szinten létrehozott információs rendszer a váminformációs rendszer (VIR).[908] A belső piac kialakítása során az EU területén belül mozgó árukra vonatkozó ellenőrzéseket és formalitásokat teljesen eltörölték, ami megnövelte a csalás kockázatát. Ezt a veszélyt a tagállamok vámigazgatási szervei közötti fokozott együttműködéssel ellensúlyozták. A VIR célja, hogy elősegítse a tagállamok számára a nemzeti és uniós vám- és mezőgazdasági jogszabályok súlyos megsértésének megelőzését, felderítését és üldözését. A VIR-t különböző jogalapok alapján elfogadott két jogi aktus hozta létre: Az 515/97/EK tanácsi rendelet a különböző nemzeti közigazgatási hatóságok közötti, a vámunió és a közös mezőgazdasági politika keretében a csalás leküzdése terén megvalósuló együttműködéssel foglalkozik, míg a 2009/917/IB tanácsi határozat célja segíteni a vámjogszabályok súlyos megsértésének megelőzését, kivizsgálását és eljárás alá vonását. Ez azt jelenti, hogy a VIR nem pusztán a bűnüldözéssel foglalkozik.

A VIR nyersanyagokkal, szállítóeszközökkel, vállalkozásokkal, személyekkel, valamint a visszatartott, lefoglalt vagy elkobozott árukkal és készpénzzel kapcsolatos személyes adatokat tartalmaz. Világosan meghatározza a kezelt adatok kategóriáit, és tartalmazza az érintett személyek neveit, állampolgárságát, nemét, születési idejét és helyét, az adatok rendszerbe bevitelének okát, valamint a szállítóeszköz rendszámát.[909] Az említett információk kizárólag az alábbi célokból használhatók fel: megfigyelés és jelentéstétel, célzott megfigyelés, illetve stratégiai vagy operatív elemzés olyan személyre vonatkozóan, aki vámügyi jogszabályok megsértésével gyanúsítható.

A VIR-hez a nemzeti vám-, adó-, mezőgazdasági, közegészségügyi és rendőri hatóságok, valamint az Europol és az Eurojust rendelkezik hozzáférési jogosultsággal.

A személyes adatok kezelése során be kell tartani az 515/97 rendelet és a 20009/917/IB tanácsi határozat által létrehozott különös szabályokat, valamint az általános adatvédelmi rendelet, a Korszerűsített 108. Egyezmény és a Rendőrségi

908 Az Európai Unió Tanácsa (1995), A Tanács jogi aktusa (1995. július 26.) az informatika vámügyi alkalmazásáról szóló egyezmény létrehozásáról, HL C 316., 1995.11.27., amelyet módosított: A Tanács 515/97/EK rendelete (1997. március 13.) a tagállamok közigazgatási hatóságai közötti kölcsönös segítségnyújtásról, valamint a vám- és mezőgazdasági jogszabályok helyes alkalmazásának biztosítása érdekében e hatóságok és a Bizottság együttműködéséről; A Tanács 2009/917/IB határozata (2009. november 30.) az információs technológia vámügyi alkalmazásáról, HL L 323., 2009.12.10. (VIR-határozat).

909 Lásd: VIR-határozat, 24., 25. és 28. cikk.

ajánlás rendelkezéseit. Az európai adatvédelmi biztos felelős a VIR 45/2001/EK rendeletnek való megfelelőségének felügyeletéért. Évente legalább egyszer ülést hív össze az összes VIR-rel kapcsolatos felügyeleti kérdésekben hatáskörrel rendelkező nemzeti adatvédelmi felügyeleti hatóság részvételével.

Az uniós információs rendszerek közötti interoperabilitás

Migrációkezelés, az EU küldő határainak integrált határigazgatása és a terrorizmus, valamint a határokon átnyúló bűnözés elleni küzdelem komoly kihívást jelent, és egyre összetettebb feladattá válik a globalizált világban. Az elmúlt években az EU egy olyan új átfogó megközelítésen dolgozott a biztonság biztosítása és fenntartása terén, amely nem csorbítja az EU értékeit és az alapvető szabadságokat. E törekvések során kulcsfontosságú a nemzeti bűnüldözési hatóságok, a tagállamok és az érintett uniós ügynökségek közötti hatékony információcsere.[910] A meglévő uniós határigazgatási információs és belső biztonsági rendszereknek megvannak a saját célkitűzései, intézményi felépítése, érintetti és felhasználói köre. Az EU azon dolgozott, hogy megoldást találjon a különböző információs rendszerek (így a SIS II, VIS és az Eurodac) között fragmentálódott uniós adatkezelés működési hiányosságaira az interoperabilitás lehetőségeinek feltárásával.[911] A fő célkitűzés annak biztosítása, hogy az illetékes rendészeti, vám és igazságszolgáltatási hatóság szisztematikusan rendelkezzen a feladatai ellátásához szükséges információkkal, miközben megmarad az egyensúly a magánélethez, adatvédelemhez és egyéb alapvető jogok tiszteletben tartásához való joggal.

910 Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek, COM(2016) 205 final, Brüsszel, 2016. április 6.; Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek, az Európai Tanácsnak és a Tanácsnak: Fokozott biztonság a mobilitás korában: a terrorizmus elleni küzdelemmel kapcsolatos információcsere javítása és a külső határok megerősítése, COM(2016) 602 final, Brüsszel, 2016. szeptember 14.; Európai Bizottság (2016), A Schengeni Információs Rendszernek a jogellenesen tartózkodó harmadik országbeli állampolgárok visszatérésére való felhasználásáról szóló európai parlamenti és tanácsi rendeletre irányuló javaslat. Lásd még a Bizottság közleményét az Európai Parlamentnek és a Tanácsnak: A hatékony és valódi biztonsági unió megvalósításáról szóló hetedik eredményjelentés, COM(2017) 261 final, Brüsszel, 2017. május 16.

911 Az Európai Unió Tanácsa (2005), Hágai program: a szabadság, a biztonság és a jog érvényesülésének erősítése az Európai Unióban, HL C 53., 2005.3.3.; Európai Bizottság (2010), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A szabadságon, a biztonságon és a jog érvényesülésén alapuló térségben folytatott információkezelés áttekintése, COM(2010) 385 végleges; Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek, COM(2016) 205 final, Brüsszel, 2016. április 6.; Európai Bizottság (2016), A Bizottság határozata (2016. június 17.) az információs rendszerekkel és interoperabilitással foglalkozó magas szintű szakértői csoport létrehozásáról, HL C 257., 2016.7.15.

Az interoperabilitás „az információs rendszereknek az adatcserére és az információk megosztásának lehetővé tételére vonatkozó képessége”.[912] Ez a csere nem csorbíthatja a feltétlenül szükséges mértékű hozzáférésre és felhasználásra vonatkozó, az általános adatvédelmi rendeletben, a rendészeti és büntető igazságszolgáltatási szervekre vonatkozó adatvédelmi irányelvben, az EU Alapjogi Chartájában és valamennyi egyéb vonatkozó jogszabályban garantált szabályokat. Az adatkezelés egyetlen integrált megoldása sem érintheti a célhoz kötöttség, a beépített adatvédelem vagy az alapértelmezett adatvédelem elvét.[913]

A három fő informatikai rendszer – a SIS II, VIS és Eurodac – funkcionalitásainak fejlesztésén túl a Bizottság javaslatot tett egy negyedik központosított határigazgatási rendszer létrehozására, amely a harmadik országbeli állampolgárokkal foglalkozna: ez a határregisztrációs rendszer (EES),[914] amely várhatóan 2020-ra valósul meg.[915] A Bizottság továbbá javaslatot adott ki egy Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról,[916] amely a vízum nélkül az EU-ba utazó személyekről gyűjt információt, hogy lehetővé tegye az illegális migráció előzetes megakadályozását és az előzetes biztonsági ellenőrzéseket.

912 Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek, COM(2016) 205 final, 2016. április 6., 14. o.

913 *Uo.*, 4–5. oldal.

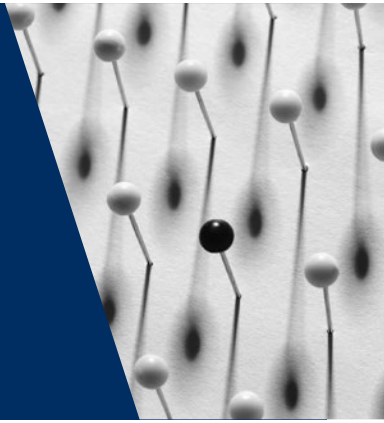
914 Európai Bizottság (2016), Javaslat egy európai parlamenti és tanácsi rendeletre – A tagállamok külső határait átlépő harmadik országbeli állampolgárok belépésére és kilépésére, valamint beléptetésének megtagadására vonatkozó adatok rögzítésére szolgáló határregisztrációs rendszer (EES) létrehozásáról és az EES-hez való bűnüldözési célú hozzáférés feltételeinek meghatározásáról, valamint a Schengeni Megállapodás végrehajtásáról szóló egyezmény, a 767/2008/EK rendelet és az 1077/2011/EU rendelet módosításáról, COM(2016) 194 final, Brüsszel, 2016. április 6.

915 Európai Bizottság (2016), A Bizottság közleménye az Európai Parlamentnek és a Tanácsnak: A határigazgatás és a biztonság erősítését szolgáló, szilárd és intelligens információs rendszerek, COM(2016) 205 final, 2016. április 6., 5. o.

916 Európai Bizottság (2016), Javaslat európai parlamenti és tanácsi rendeletre az Európai Utasinformációs és Engedélyezési Rendszer (ETIAS) létrehozásáról, valamint az (EU) 515/2014 rendelet, az (EU) 2016/399 rendelet, az (EU) 2016/794 rendelet és az (EU) 2016/1624 rendelet módosításáról, COM(2016) 731 final, 2016. november 16.

9

Különleges adattípusok és a rájuk vonatkozó adatvédelmi szabályok



EU	Tárgyalt kérdések	Európa Tanács
Általános adatvédelmi rendelet Elektronikus hírközlési adatvédelmi irányelv	**Elektronikus közlések**	Korszerűsített 108. Egyezmény Távközlési szolgáltatásokra vonatkozó ajánlás
Általános adatvédelmi rendelet, 88. cikk	**Foglalkoztatási jogviszony**	Korszerűsített 108. Egyezmény Foglalkoztatásra vonatkozó ajánlás EJEB, *Copland kontra Egyesült Királyság*, 62617/00. sz. ügy, 2007
Általános adatvédelmi rendelet, 9. cikk (2) bekezdés h) és i) pont	**Orvosi adatok**	Korszerűsített 108. Egyezmény Az orvosi adatokra vonatkozó ajánlás EJEB, *Z kontra Finnország*, 22009/93. sz. ügy, 1997
A klinikai vizsgálatokról szóló rendelet	**Klinikai vizsgálatok**	
Általános adatvédelmi rendelet, 6. cikk (4) bekezdés és 89. cikk	**Statisztikai adatok**	Korszerűsített 108. Egyezmény A statisztikai adatokra vonatkozó ajánlás

EU	Tárgyalt kérdések	Európa Tanács
223/2009/EK rendelet az európai statisztikákról EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008	**Hivatalos statisztikák**	Korszerűsített 108. Egyezmény A statisztikai adatokra vonatkozó ajánlás
2014/65/EU irányelv a pénzügyi eszközök piacairól 648/2012/EU rendelet a tőzsdén kívüli származtatott ügyletekről, a központi szerződő felekről és a kereskedési adattárakról 1060/2009/EK rendelet a hitelminősítő intézetekről 2007/64/EK irányelv a belső piaci pénzforgalmi szolgáltatásokról	**Pénzügyi adatok**	Korszerűsített 108. Egyezmény 90 (19). számú, a kifizetésekre és más kapcsolódó műveletekre vonatkozó ajánlás EJEB, *Michaud kontra Franciaország*, 12323/11. sz. ügy, 2012

Számos esetben speciális jogi aktusokat fogadtak el európai szinten, amelyek a Korszerűsített 108. Egyezményben vagy az általános adatvédelmi rendeletben foglalt általános szabályokat alkalmazzák részletesebben – konkrét helyzetekre.

9.1 Elektronikus közlések

Főbb pontok

- Az Európa Tanács 1995-ös ajánlása a távközlés területén – különös tekintettel a telefonszolgáltatásra – irányadó speciális adatvédelmi szabályokat tartalmaz.
- Az európai szintű kommunikációs szolgáltatásokhoz kapcsolódó személyesadat-kezelést az elektronikus hírközlési adatvédelmi irányelv szabályozza.
- Az elektronikus kommunikáció titkossága nemcsak a kommunikáció tartalmára vonatkozik, hanem a metaadatokra is, köztük arra az információra, hogy ki kivel beszélt, mikor és mennyi ideig, valamint a helymeghatározási adatokra, pl. arra, hogy honnan közölték az adatokat.

A távközlési hálózatok fokozottan sérthetik a felhasználók magánszféráját, mivel erőteljesebb technikai lehetőséget nyújtanak az e hálózatokon zajló beszélgetésekbe való belehallgatásra, illetve e beszélgetések megfigyelésére. Következésképpen speciális adatvédelmi rendelkezések bevezetését tartották szükségesnek

annak érdekében, hogy kezeljék azokat a kockázatokat, amelyeknek a távközlési szolgáltatásokat igénybe vevők ki vannak téve.

1995-ben az Európa Tanács ajánlást adott ki a távközlés területén az adatvédelemről, különös tekintettel a telefonszolgáltatásra.[917] Ezen ajánlás szerint a személyes adatok távközléssel összefüggésben történő gyűjtését és kezelését a következőkre kell korlátozni: a felhasználó bekötése a hálózatba, az adott távközlési szolgáltatás elérhetővé tétele, számlázás, ellenőrzés, a technikai szempontból optimális működés biztosítása, valamint a hálózat és szolgáltatás fejlesztése.

Különleges figyelmet szenteltek a távközlési hálózatok közvetlen üzletszerzési célú (direkt marketing) üzenetek küldésére való használatának. Főszabályként direkt marketing üzenet olyan előfizetőhöz nem irányítható, aki kifejezetten kizárta az ilyen üzenetek vételét. Előre felvett, hirdetési célú üzenetek továbbításához automatikus hívásokat lebonyolító eszközök kizárólag akkor használhatók, ha az előfizető ehhez kifejezetten hozzájárult. Az ezen a területen érvényes részletes szabályokat a nemzeti jog állapítja meg.

Az **uniós jogi keretrendszerben** az első 1997-es kísérletet követően 2002-ben fogadták el, majd 2009-ben módosították az adatvédelemről és az elektronikus hírközlésről szóló irányelvet. Ezzel a jogalkotó célja az volt, hogy a távközlési ágazatra vonatkozóan kiegészítsék és testre szabják az adatvédelmi irányelv rendelkezéseit.[918]

Az elektronikus hírközlési adatvédelmi irányelv alkalmazása a nyilvános elektronikus hírközlő hálózatokon nyújtott hírközlési szolgáltatásokra korlátozódik.

Az elektronikus hírközlési adatvédelmi irányelv a kommunikáció során keletkező adatok három fő kategóriáját különbözteti meg:

---

917 Európa Tanács, Miniszteri Bizottság (1995), Rec (95)4. sz. ajánlás a tagállamok részére a távközlési szolgáltatások területén a személyes adatok védelméről, különös tekintettel a telefonszolgáltatásra, 1995. február 7.

918 Az Európai Parlament és a Tanács 2002/58/EK irányelve (2002. július 12.) az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről (Elektronikus hírközlési adatvédelmi irányelv), HL L 201., 2002.7.31.; módosította az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról, HL L 337., 2009.12.18.

- a kommunikáció során küldött üzenetek tartalmát alkotó adatok; ezek az adatok szigorúan titkosak;

- a kommunikáció létrehozásához és fenntartásához szükséges adatok, az ún. metaadatok vagy az irányelvben használt kifejezés szerint „forgalmi adatok", mint pl. a kommunikációs partnerekre, a kommunikáció időpontjára és időtartamára vonatkozó információk;

- a metaadatokon belül léteznek a kifejezetten a kommunikációs eszköz helyének meghatározására vonatkozó ún. helymeghatározó adatok; ezek az adatok egyidejűleg a kommunikációs eszközök felhasználóinak helyéről is adatokat szolgáltatnak, különös tekintettel a mobil kommunikációs eszközök felhasználóira.

A forgalmi adatokat a szolgáltató kizárólag a számlázás és a műszaki szolgáltatásnyújtás céljára használhatja fel. Az érintett hozzájárulásával azonban ezen adatok más, értéknövelt szolgáltatásokat kínáló adatkezelők számára is felfedhetők, mint pl. tájékoztatás a felhasználó helyéhez képest a legközelebbi metróállomásról vagy gyógyszertárról, vagy a felhasználó helye szerinti időjárás-előrejelzésről.

Az elektronikus hírközlési adatvédelmi irányelv 15. cikke szerint az elektronikus hálózatokon történő kommunikációra vonatkozó adatokhoz való egyéb hozzáféréseknek, köztük a bűncselekmény kivizsgálása céljából történő hozzáférésnek, meg kell felelniük az EJEE 8. cikkének (2) bekezdésében rögzített és az EU Alapjogi Chartájának 8. és 52. cikkében megerősített, az adatvédelemhez való jog igazolható sérelmére vonatkozó követelményeknek. Ebbe beltartozhat a bűncselekmények nyomozása céljából történő hozzáférés is.

Az elektronikus hírközlési adatvédelmi irányelv 2009-et követő módosításai[919] a következőket vezették be:

- A direkt marketing céljából küldött e-mailekre vonatkozó korlátozásokat a rövid szöveges üzenet szolgáltatásokra (SMS), a multimédiás üzenetküldő szolgáltatásokra (MMS) és más hasonló típusú alkalmazásokra is kiterjesztették; marketing

919 Az Európai Parlament és a Tanács 2009/136/EK irányelve (2009. november 25.) az egyetemes szolgáltatásról, valamint az elektronikus hírközlő hálózatokhoz és elektronikus hírközlési szolgáltatásokhoz kapcsolódó felhasználói jogokról szóló 2002/22/EK irányelv, az elektronikus hírközlési ágazatban a személyes adatok kezeléséről, feldolgozásáról és a magánélet védelméről szóló 2002/58/EK irányelv és a fogyasztóvédelmi jogszabályok alkalmazásáért felelős nemzeti hatóságok közötti együttműködésről szóló 2006/2004/EK rendelet módosításáról, HL L 337., 2009.12.18.

célú e-mailek küldése tilos, kivéve, ha ahhoz a címzett előzetes hozzájárulását beszerezték. Ilyen hozzájárulás nélkül csak korábbi ügyfeleknek szabad marketing célú e-mailt küldeni, ha megadták e-mail-címüket, és nem emelnek kifogást.

- Arra kötelezték a tagállamokat, hogy a nem kívánt közlésekre vonatkozó tilalom megszegésének esetére biztosítsanak bírósági jogorvoslati lehetőséget.[920]

- A számítógép tulajdonosának hozzájárulása nélkül immár nem engedélyezett a sütik beállítása, a számítógép-tulajdonos cselekvéseit nyomon követő és rögzítő szoftver. A nemzeti jognak részletesebben is szabályoznia kell, hogyan kell kifejezni és megszerezni a hozzájárulást ahhoz, hogy a védelem megfelelő legyen.[921]

Amennyiben adatvédelmi incidens – jogosulatlan hozzáférés, adatvesztés vagy adatmegsemmisülés – történik, azonnal tájékoztatni kell erről az illetékes felügyeleti hatóságot. Az előfizetőket is tájékoztatni kell, hogy az adatvédelmi incidens következtében káruk keletkezhet.[922]

Az adatmegőrzési irányelv[923] kötelezte a hírközlési szolgáltatókat a metaadatok megőrzésére. Ezt az irányelvet azonban az EUB érvénytelenítette (részletesebben lásd a 8.3 szakaszban).

Kilátások

2017 januárjában az Európai Bizottság egy a régi elektronikus hírközlési adatvédelmi irányelvet felváltó új elektronikus hírközlési adatvédelmi irányelvre irányuló javaslatot fogadott el. A cél továbbra is „természetes és jogi személyek alapvető jogainak és szabadságainak, különösen a magánélet és a magáncélú kommunikáció tiszteletben tartásához való jogainak, továbbá a személyes adatok kezelése tekintetében

920 Lásd a módosított irányelv 13. cikkét.

921 Lásd *uo.* az 5. cikket; lásd még a 29. cikk szerinti munkacsoport 04/2012. sz. véleményét a sütikhez való hozzájárulás alóli mentességről (2012), WP 194, Brüsszel, 2012. június 7.

922 Lásd még a 29. cikk szerinti munkacsoport 01/2011 sz. munkadokumentumát a személyes adatok megsértésére vonatkozó, jelenleg hatályos európai uniós keretről és a jövőbeli szakpolitikai fejleményekkel kapcsolatos ajánlásokról, WP 184, Brüsszel, 2011. április 5.

923 Az Európai Parlament és a Tanács 2006/24/EK irányelve (2006. március 15.) a nyilvánosan elérhető elektronikus hírközlési szolgáltatások nyújtása, illetve a nyilvános hírközlő hálózatok szolgáltatása keretében előállított vagy feldolgozott adatok megőrzéséről és a 2002/58/EK irányelv módosításáról, HL L 105., 2006.4.13.

a természetes személyeknek a védelme". Ugyanakkor az új javaslat célja biztosítani az elektronikus hírközlési adatok és szolgáltatások Unión belüli szabad áramlását.[924] Míg az általános adatvédelmi rendelet elsősorban az EU Alapjogi Chartájának 8. cikkét veszi alapul, addig a javasolt rendelet igyekszik a Charta 7. cikkét beépíteni a másodlagos uniós jogba.

A rendelet a korábbi irányelv rendelkezéseit az új technológiákhoz és az új piaci realitáshoz igazítja, és egy átfogó, következes keretrendszert hoz létre az általános adatvédelmi rendelettel. Ebben az értelemben az elektronikus hírközlési adatvédelmi rendelet az általános adatvédelmi rendelet *lex specialis-a* lenne, amely a rendeletet a személyes adatnak minősülő elektronikus hírközlési adatokhoz igazítja. Az új rendelet kiterjed az „elektronikus hírközlési adatok" kezelésére, beleértve az elektronikus hírközlés nem feltétlenül személyes adatnak minősülő tartalmát és metaadatait. Területi hatálya az EU-ra korlátozódik, beleértve azt is, amikor az EU-ban gyűjtött adatokat az EU-n kívül kezelik, és kiterjed a hálózatsemleges online hírközlési szolgáltatásokra, vagyis azokra a szolgáltatókra, akik a tartalmat, szolgáltatásokat vagy alkalmazásokat az interneten keresztül, egy hálózatüzemeltető vagy internetszolgáltató (ISP) közvetlen bevonása nélkül nyújtják. Ilyen szolgáltatók például a Skype (hang és video hívások), WhatsApp (üzenetküldés), Google (keresés), Spotify (zene) vagy Netflix (video tartalom). Az általános adatvédelmi rendelet jogalkalmazási mechanizmusai vonatkoznának az új rendeletre is.

Az elektronikus hírközlési adatvédelmi rendeletet várhatóan 2018. május 25. előtt elfogadják, vagyis még azelőtt, hogy az általános adatvédelmi rendelet mind a 28 tagállamban hatályba lépne. Ez azonban függ mind az Európai Parlament, mind pedig a Tanács egyetértésétől.[925]

924 Javaslat – Az Európai Parlament és a Tanács rendelete az elektronikus hírközlés során a magánélet tiszteletben tartásáról és a személyes adatok védelméről, valamint a 2002/58/EK irányelv hatályon kívül helyezéséről (elektronikus hírközlési adatvédelmi rendelet), COM(2017) 10 final, 2017/0003 (COD).

925 Bővebb információért lásd: Európai Bizottság (2017), „A Bizottság a magánélet és a személyes adatok magas fokú védelmét javasolja az elektronikus hírközlés területén, és naprakésszé teszi az uniós intézményekre vonatkozó adatvédelmi szabályokat", sajtóközlemény, 2017. január 10.

9.2 A foglalkoztatási jogviszonnyal kapcsolatos adatok

Főbb pontok

- A foglalkoztatási jogviszonyban fennálló adatvédelemre vonatkozó speciális szabályokat az Európa Tanács foglalkoztatási adatokra vonatkozó ajánlása részletezi.
- Az általános adatvédelmi rendelet a foglalkoztatási jogviszonyokat csak a különleges adatok feldolgozásával összefüggésben említi.
- Figyelemmel arra, hogy nincs gazdasági egyensúly a munkáltató és a munkavállalók között, a hozzájárulás – mint a munkavállalói adatok feldolgozásának jogalapja – önkéntessége, s így érvényessége kérdéses lehet. A hozzájárulás megadásának körülményeit alaposan meg kell vizsgálni.

A foglalkoztatással összefüggésében végzett adatkezelés a személyes adatok védelmére vonatkozó általános uniós szabályozás alá tartozik. Egy rendelet[926] azonban kifejezetten a személyes adatoknak az uniós intézmények általi kezelésével foglalkozik (többek között) a foglalkoztatással összefüggésben. Az általános adatvédelmi rendeletben a munkaviszonyt kifejezetten a 9. cikk (2) bekezdése említi, amely kimondja, hogy a személyes adatok kezelésére akkor kerülhet sor, ha az adatkezelő vagy az érintett a munkaviszonnyal összefüggésben kötelezettséget teljesít, vagy speciális jogokat gyakorol.

Az általános adatvédelmi rendelet alapján a munkavállaló számára lehetővé kell tenni, hogy egyértelműen fel tudja ismerni azokat az adatokat, amelyek kezeléséhez/tárolásához szabad akaratából járul hozzá, valamint azokat a célokat, amelyek miatt az adatait tárolják. A munkavállalókat még a hozzájárulás megadása előtt tájékoztatni kell jogaikról, valamint az adatok megőrzési idejéről. Amennyiben egy olyan adatvédelmi incidens történik, amely valószínűsíthetően magas kockázattal jár a természetes személyek jogaira és szabadságaira nézve, a munkáltatónak erről tájékoztatnia kell a munkavállalót. A rendelet 88. cikke megengedi, hogy a tagállamok részletesebb szabályokat állapítsanak meg a munkavállalók személyes adatainak és szabadságainak védelmére a munkaviszonnyal összefüggésben.

926 Az Európai Parlament és a Tanács 45/2001/EK rendelete (2000. december 18.) a személyes adatok közösségi intézmények és szervek által történő feldolgozása tekintetében az egyének védelméről, valamint az ilyen adatok szabad áramlásáról, HL L 8., 2001.1.12.

Példa: A *Worten* ügyben[927] a munkaidő-nyilvántartás tartalmazta a személyes adatnak minősülő napi munkaidőt és pihenőidőket. A nemzeti jog előírhatja, hogy a munkáltató bocsássa a munkaidő-nyilvántartást a munkafeltételeket ellenőrző nemzeti hatóságok rendelkezésére. Ez lehetővé tenné az azonnali hozzáférést a vonatkozó személyes adatokhoz. A személyes adatokhoz való hozzáférés azonban szükséges a nemzeti hatóságnak a munkaidőre vonatkozó szabályozás alkalmazására irányuló ellenőrzési feladatának teljesítéséhez.[928]

Ami az **Európa Tanácsot** illeti, a foglalkoztatási adatokra vonatkozó ajánlást 1989-ben adták ki és 2015-ben vizsgálták felül.[929] Az ajánlás kiterjed a személyes adatok munkaviszonnyal összefüggő kezelésére a magán- és állami szektorban egyaránt. Az adatkezelésnek meg kell felelnie bizonyos elveknek és korlátozásoknak, például az átláthatóság elvének, és a munkahelyi megfigyelő rendszerek telepítése előtt egyeztetni kell a munkavállalók képviselőjével. Az ajánlás azt is kimondja, hogy a munkáltatóknak a munkavállalók internethasználatának megfigyelése helyett inkább megelőző intézkedéseket, például szűrőket kell alkalmazniuk.

A foglalkoztatással összefüggő személyes adatok kezeléséhez kapcsolódó leggyakoribb adatvédelmi problémákról szóló felmérés a 29. cikk szerinti munkacsoport munkadokumentumában található.[930] A munkacsoport elemezte a hozzájárulás, mint a foglalkoztatási jogviszonnyal kapcsolatos adatok kezelése jogalapjának jelentőségét.[931] Megállapította, hogy mivel nincs egyensúly a hozzájárulást kérő munkáltató és a hozzájárulást megadó munkavállaló között, ez gyakran kételyeket vet fel azzal kapcsolatban, hogy a hozzájárulást önténtesen adták-e meg vagy sem. Ezért a foglalkoztatással összefüggő hozzájárulás érvényességének értékelése során gondosan meg kell vizsgálni azon körülményeket, amelyek közepette az adatkezelés jogalapjaként a hozzájárulásra támaszkodnak.

927 EUB, *Worten – Equipamentos para o Lar SA kontra Autoridade para as Condições de Trabalho (ACT)*, C-342/12. sz. ügy, 2013. május 30., 19. pont.

928 *Uo.*, 43. pont.

929 Európa Tanács, Miniszteri Bizottság (2015), Rec(2015)5. sz. ajánlás a tagállamoknak a személyes adatok foglalkoztatással összefüggő kezeléséről, 2015. április.

930 29. cikk szerinti munkacsoport (2017), *2/2017. sz. vélemény a munkahelyi adatkezelésről*, WP 249, Brüsszel, 2017. június 8.

931 29. cikk szerinti munkacsoport (2005), *Munkadokumentum a 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről*, WP 114, 1995. október 24., Brüsszel, 2005. november 25.

A tipikus mai munkakörnyezetben az egyik szokásos adatvédelmi probléma a munkavállalók munkahelyi elektronikus kommunikációja figyelemmel kísérésének törvényes mértéke. Gyakori állítás, hogy ez a probléma könnyen megoldható azzal, ha megtiltják a munkahelyen lévő kommunikációs eszközök magáncélú használatát. Egy ilyen általános tiltás azonban aránytalan és irreális lehet. Az EJEB *Copland kontra Egyesült Királyság* és *Bărbulescu kontra Románia* ügyekben hozott ítéletei különösen érdekesek ebben az összefüggésben.

Példa: A *Copland kontra Egyesült Királyság* ügyben[932] titokban nyomon követték egy szakkollégiumi munkavállaló telefon-, e-mail- és internethasználatát, hogy megbizonyosodjanak arról, hogy a munkavállaló túlzott mértékben személyes célokra használja a kollégiumi infrastruktúrát. Az EJEB megállapította, hogy a munkahelyről lebonyolított telefonhívásokra is vonatkozik a magánélet és a kapcsolattartás fogalma. Ennélfogva a munkahelyről indított ilyen hívások és e-mailek, valamint a személyes internethasználat nyomon követéséből származó információk is védelemben részesülnek az EJEE 8. cikke alapján. A felperes esetében nem létezett olyan rendelkezés, amely azokat a körülményeket szabályozta volna, amelyek fennállása esetén a munkáltató megfigyelheti a munkavállalók telefon- e-mail- és internethasználatát. A beavatkozás tehát nem felelt meg a jogszabályoknak. A Bíróság arra a következtetésre jutott, hogy megsértették az EJEE 8. cikkét.

Példa: A *Bărbulescu kontra Románia* ügyben[933] a felperest azért bocsátották el, mert munkahelyén munkaidőben a belső szabályzat megszegésével használta az internetet. Munkáltatója megfigyelte levelezését. A jegyzőkönyvek, amelyek tisztán magánjellegű üzeneteket tartalmaztak, a hazai eljárás során készültek. Annak megállapítása során, hogy a 8. cikk alkalmazandó, az EJEB nyitva hagyta annak kérdését, hogy a munkáltató korlátozó előírásából a felperesnek következtetnie kellett volna annak magánélethez való jogokra gyakorolt észszerű vonzataival, azonban úgy vélte, hogy a munkáltató utasításai nem csökkenthetnék nullára a magán közösségi életet a munkahelyen.

932 EJEB, *Copland kontra Egyesült Királyság*, 62617/00. sz. ügy, 2007. április 3.

933 EJEB, *Bărbulescu kontra Románia* [Nagykamara], 61496/08. sz. ügy, 2017. szeptember 5., 121. pont.

Megalapozottságát illetően a szerződő államoknak széles mérlegelési mozgásteret kell biztosítani annak mérlegelésére, hogy szükséges-e azon feltételeket illetően jogi keretrendszert kialakítani, amelyek mellett a munkáltatók szabályozhatják munkavállalóik nem szakmai jellegű, elektronikus vagy egyéb kommunikációját a munkahelyen. Mindazonáltal a hazai hatóságoknak biztosítaniuk kell, hogy a levelezések és egyéb kommunikációk megfigyelésére irányuló intézkedések munkáltató általi bevezetéséhez – az ilyen intézkedések mértékétől és tartamától függetlenül – társuljanak megfelelő és elégséges biztosítékok a visszaéléssel szemben. Arányosság és eljárási garanciák voltak szükségesek az önkényesség ellen, és az EJEB számos olyan tényezőt azonosított, amelyek relevánsak az adott körülmények között. Ezek tartalmazták többek között a munkavállalók munkáltató általi megfigyelésének terjedelmét és a munkavállaló magánéletébe történő beavatkozás mértékét, a munkavállalóra vonatkozó következményeket, valamint azt, hogy biztosítottak-e megfelelő biztosítékokat. Emellett a hazai hatóságoknak biztosítaniuk kellett, hogy azon munkavállaló számára, akinek a közléseit megfigyelték, rendelkezésre álljon egy olyan bíróság előtti jogorvoslat lehetősége, amely hatáskörrel rendelkezik annak – legalábbis lényegében történő – megállapítására, hogy a megfogalmazott kritériumok miként lettek megfigyelve, és hogy a megtámadott intézkedések törvényesek voltak-e.

Ebben az esetben az EJEB megállapította a 8. cikk megsértését, mivel a hazai hatóságok nem biztosították a felperes magánélet és kapcsolattartás tiszteletben tartásához való jogának megfelelő védelmét, és következésképpen nem sikerült tisztességes egyensúlyt teremteniük a szóban forgó érdekek között.

Az Európa Tanács foglalkoztatásra vonatkozó ajánlása szerint a foglalkoztatási célokra gyűjtött személyes adatokat közvetlenül a munkavállalótól kell beszerezni.

A toborzás céljából gyűjtött személyes adatok körét a jelöltek alkalmasságának és karrierlehetőségének értékeléséhez szükséges információkra kell korlátozni.

Az ajánlás kifejezetten említi az egyes munkavállalók teljesítményét vagy lehetőségeit minősítő adatokat. A minősítő adatoknak tisztességes, őszinte értékeléseken kell alapulniuk, és megfogalmazásuk semmiképpen sem lehet sértő. Ezt a tisztességes adatfeldolgozás és az adatok pontosságának elve is megköveteli.

A munkáltató-munkavállaló jogviszonyban az adatvédelmi jog egyik speciális vonatkozása a munkavállalók képviselőinek szerepe. Az ilyen képviselők csak olyan mértékben juthatnak hozzá a munkavállalók személyes adataihoz, amennyire ez a munkavállalók érdekeinek képviseletéhez szükséges, vagy ha ezek az adatok a kollektív szerződésben megállapított kötelezettségek teljesítéséhez vagy felügyeletéhez szükségesek.

Foglalkoztatási célokra gyűjtött különleges adatok feldolgozása kizárólag konkrét esetekben, és csakis a nemzeti jog által előírt biztosítékok mellett történhet. A munkáltatók csak akkor kérdezhetik a munkavállalókat vagy a pályázókat egészségi állapotukról, illetve akkor kérhetnek tőlük orvosi vizsgálatot, ha erre a munkára való alkalmasságuk megállapításához, preventív gyógyszerigényük kielégítéséhez, az érintett vagy más munkavállaló és egyén létfontosságú érdekei védelméhez, vagy szociális ellátások odaítéléséhez van szükség. Egészségügyi adatok az érintett munkavállalón kívüli forrásból nem gyűjthetők, kivéve, ha ehhez megszerezték a munkavállaló kifejezett beleegyező nyilatkozatát, vagy ha az adatgyűjtést nemzeti jogszabály írja elő.

A foglalkoztatásra vonatkozó ajánlás értelmében a munkavállalókat tájékoztatni kell személyes adataik feldolgozásának céljáról, a gyűjtött személyes adatok típusáról, azon jogalanyokról, akikkel az adatokat rendszeresen közlik, valamint e közlések céljáról és jogalapjáról. Az elektronikus közlésekhez csak biztonságra vagy egyéb jogszerű okra hivatkozva lehet hozzáférni a munkahelyen, és a hozzáférés csak azután megengedett, hogy a munkavállalókat tájékoztatták arról, hogy a munkáltató hozzáférhet az ilyen jellegű kommunikációhoz.

A munkavállalóknak hozzáférési joggal kell rendelkezniük a foglalkoztatási adataikhoz, továbbá a helyesbítés vagy törlés jogával is rendelkezniük kell. Minősítő adatok feldolgozása esetén a munkavállalóknak a minősítés vitatására is jogosultnak kell lenniük. E jogok azonban – belső vizsgálat céljára – ideiglenesen korlátozhatók. Ha egy munkavállalótól megtagadják a foglalkoztatáshoz kapcsolódó személyes adataihoz való hozzáférést, ezen adatok helyesbítését vagy törlését, nemzeti jogszabálynak kell rendelkeznie a megfelelő eljárásról, amelynek keretében az elutasító határozat vitatható.

9.3 Egészségügyi adatok

Legfontosabb pont

- Az egészségügyi adatok érzékeny adatok, ezért speciális védelmet élveznek.

Az érintett egészségi állapotára vonatkozó személyes adatok az általános adatvédelmi rendelet 9. cikkének (1) bekezdése és a Korszerűsített 108. Egyezmény 6. cikke értelmében különleges adatnak minősülnek. Ennek megfelelően az orvosi adatok a nem különleges adatoknál szigorúbb adatvédelmi rendszer alá tartoznak. Az általános adatvédelmi rendelet tiltja az „egészségügyi személyes adatok" („az érintett egészségi állapotára vonatkozó olyan adatok, amelyek információt hordoznak az érintett múltbeli, jelenlegi vagy jövőbeli testi vagy pszichikai egészségi állapotáról")[934], valamint a genetikai és biometrikus adatok kezelését, kivéve, ha az a 9. cikk (2) bekezdése értelmében megengedett. Mindkét típusú adat szerepel a „különleges adatkategóriák" listáján.[935]

Példa: A *Z kontra Finnország* ügyben[936] a felperes volt férje, aki HIV-fertőzött, több szexuális bűncselekményt követett el. Elítélték emberölésért azon az alapon, hogy szándékosan tette ki áldozatait a HIV-fertőzés kockázatának. A nemzeti bíróság az ítélet teljes egészét és az ügy dokumentumait 10 évre titkosította annak ellenére, hogy a felperes hosszabb titkosítási időszakot kért. Ezeket a kérelmeket a fellebbviteli bíróság elutasította, és ítélete a felperes és volt férje teljes nevét is tartalmazta. Az EJEB megállapította, hogy a beavatkozás nem minősül egy demokratikus társadalomban szükségesnek, mert az orvosi adatok védelme a magánélet és a családi élet tiszteletben tartásához való jog gyakorlása szempontjából alapvető fontosságú, különösen, ha HIV-fertőzésre vonatkozó információkról van szó – tekintetbe véve, hogy számos társadalomban ehhez az állapothoz megbélyegzés kapcsolódik. Ezért a Bíróság arra a következtetésre

934 Általános adatvédelmi rendelet, (35) preambulumbekezdés.

935 *Uo.*, 2. cikk.

936 EJEB, *Z kontra Finnország*, 22009/93. sz. ügy, 1997. február 25., 94. és 112. pont; lásd még: EJEB, *M.S. kontra Svédország*, 20837/92. sz. ügy, 1997. augusztus 27.; EJEB, *L.L. kontra Franciaország*, 7508/02. sz. ügy, 2006. október 10.; EJEB, *I. kontra Finnország*, 20511/03. sz. ügy, 2008. július 17.; EJEB, *K.H. és társai kontra Szlovákia*, 32881/04. sz. ügy, 2009. április 28.; EJEB, *Szuluk kontra Egyesült Királyság*, 36936/05. sz. ügy, 2009. június 2.

jutott, hogy az, hogy a fellebbviteli bíróság ítéletében mindössze tíz évvel az ítélet kihirdetését követően megadja a hozzáférést a felperes személyazonosságához és egészségügyi állapotához, sérti az EJEE 8. cikkét.

Az **uniós jog értelmében** az általános adatvédelmi rendelet 9. cikke (2) bekezdésének h) pontja engedélyezi orvosi adatok feldolgozását, amennyiben az megelőző egészségügyi, orvosi diagnosztikai célból, gondozás vagy feldolgozás alkalmazása vagy egészségügyi szolgáltatások igazgatása céljából szükséges. A feldolgozás azonban kizárólag akkor engedélyezhető, ha egészségügyi szakember végzi szakmai titoktartási kötelezettség mellett, vagy más személy végzi, akit ezzel egyenértékű kötelezettség terhel.

Az **Európa Tanács joga értelmében** az 1997-es, orvosi adatokra vonatkozó ajánlás részletesebben is alkalmazza az egészségügyi területen végzett adatfeldolgozásra a 108. Egyezményben foglalt elveket.[937] A tervezett szabályok összhangban állnak az általános adatvédelmi rendeletnek az orvosi adatok törvényes célokra való feldolgozásával, az egészségügyi adatokat felhasználó személyek szükséges szakmai titoktartási kötelezettségével, valamint az érintettek átláthatósághoz, hozzáféréshez, helyesbítéshez és törléshez való jogával kapcsolatos rendelkezéseivel. Ezenkívül az egészségügyi szakemberek által törvényesen feldolgozott orvosi adatok bűnüldöző hatóságok részére is továbbíthatók, amennyiben „megfelelő biztosítékok" állnak rendelkezésre „az EJEE 8. cikkében garantált [...] magánélet tiszteletben tartásához való joggal össze nem egyeztethető közlések megakadályozására".[938] A nemzeti jogot továbbá „kellő pontossággal kell megfogalmazni és annak megfelelő jogi védelmet kell nyújtania az önkényességgel szemben".[939]

Az orvosi adatokra vonatkozó ajánlás a születendő gyermekek és korlátozottan cselekvőképes vagy cselekvőképtelen személyek orvosi adataira, valamint a genetikai adatok feldolgozására vonatkozóan speciális rendelkezéseket is tartalmaz. A tudományos kutatást kifejezetten elismerik az adatok szükségesnél hosszabb ideig való megőrzésének indokául, bár ehhez általában anonimizálás szükséges. Az orvosi adatokra vonatkozó ajánlás 12. cikke részletes szabályokat javasol olyan helyzetekre, amikor a kutatóknak személyes adatokra van szükségük, és az anonimizált adatok nem elegendőek.

937 Európa Tanács, Miniszteri Bizottság (1997), Rec(97)5. sz. ajánlás a tagállamok részére az orvosi adatok védelméről, 1997. február 13. Megjegyezzük, hogy ez az ajánlás jelenleg felülvizsgálat alatt áll.

938 EJEB, *Avilkina és társai kontra Oroszország*, 1585/09. sz. ügy, 2013. június 6., 53. pont. Lásd még: EJEB, *Biriuk kontra Litvánia*, 23373/03. sz. ügy, 2008. november 25.

939 EJEB, *L.H. kontra Lettország*, 52019/07. sz. ügy, 2014. április 29., 59. pont.

Az álnéven kezelés megfelelő lehet a tudományos igények kielégítésére, ugyanakkor az érintett betegek érdekeit is megvédi. Az adatvédelemmel összefüggésben az adatok álnéven való kezelésének koncepcióját a 2.1.1 szakaszban részletesebben is kifejtjük.

Az Európa Tanácsnak a genetikai vizsgálatokból származó adatok kezelésére vonatkozó 2016-os ajánlása is alkalmazandó az egészségügyi területen végzett adatkezelésre.[940] Ez az ajánlás óriási jelentőségű az E-egészségügy (eHealth) szempontjából, ahol az IKT-t az egészségügyi ellátás megkönnyítésére használják. Erre példa a beteg apasági vizsgálata eredményének egyik egészségügyi szolgáltatótól a másikhoz való elküldése. Az ajánlás célja, hogy védje azon személyek jogait, akiknek a személyes adatait biztosítási célból kezelik az illető egészségével, testi épségével, korával vagy halálával összefüggő kockázatok elleni biztosítás céljából. A biztosítóknak indokolniuk kell az egészségi állapottal kapcsolatos adatok kezelését, és annak arányosnak kell lennie a figyelembe vett kockázat jellegével és fontosságával. Az adatok ilyen jellegű kezelése függ az érintett hozzájárulásától. A biztosítóknak garanciákat kell biztosítaniuk az egészségi állapottal kapcsolatos adatok tárolásához.

A klinikai vizsgálatok, amelyek új gyógyszerek betegekre gyakorolt hatását vizsgálják dokumentált kutatási környezetben, komoly adatvédelmi vonzatokkal járnak. Az emberi felhasználásra szánt gyógyszereken végzett klinikai vizsgálatokat az emberi felhasználásra szánt gyógyszerek klinikai vizsgálatairól, valamint a 2001/20/EK irányelv hatályon kívül helyezéséről szóló, 2014. április 16-i 536/2014/EU európai parlamenti és a tanácsi rendelet (a klinikai vizsgálatokról szóló rendelet) szabályozza.[941] A klinikai vizsgálatokról szóló rendelet fő elemei a következők:

- egyszerűsített kérelmezési eljárás az uniós portálon keresztül;[942]
- a klinikai vizsgálatok iránti kérelmek elbírálásának határideje;[943]

940 Európai Tanács, Miniszteri Bizottság (2016), Rec(2016)8. sz. ajánlás a tagállamok részére az egészségi állapottal kapcsolatos személyes adatok biztosítási célból történő kezeléséről, beleértve a genetikai vizsgálatok eredményéből származó adatokat is, 2016. október 26.

941 Az Európai Parlament és a Tanács 536/2014/EU rendelete (2014. április 16.) az emberi felhasználásra szánt gyógyszerek klinikai vizsgálatairól és a 2001/20/EK irányelv hatályon kívül helyezéséről (a klinikai vizsgálatokról szóló rendelet), HL L 158., 2014.5.27.

942 A klinikai vizsgálatokról szóló rendelet, 5. cikk (1) bekezdés.

943 *Uo.*, 5. cikk (2)–(5) bekezdés.

- az elbírálás részét képező, a tagállam jogszabályaival (és az érintett időtartamot meghatározó uniós jogszabályokkal) összhangban felállított etikai bizottság;[944] és

- fokozott átláthatóság a klinikai vizsgálatokat és eredményeiket illetően.[945]

Az általános adatvédelmi rendelet kiköti, hogy klinikai vizsgálatok során végzett tudományos kutatásban való részvételhez történő hozzájárulás tekintetében az 536/2014/EU rendeletet kell alkalmazni.[946]

A személyes adatok egészségügyi ágazatban való kezelését illetően számos jogszabályi és egyéb kezdeményezés van uniós szinten függőben.[947]

Elektronikus egészségügyi nyilvántartások

Az elektronikus egészségügyi nyilvántartás „az elektronikus formában tárolt, egy adott személy múltbeli és pillanatnyi fizikai és mentális egészségi állapotára vonatkozó olyan átfogó egészségügyi nyilvántartás vagy ahhoz hasonló dokumentáció, amely lehetővé teszi, hogy orvosi kezelés vagy egyéb, azzal szorosan összefüggő cél érdekében ezekhez az adatokhoz könnyen hozzá lehessen férni".[948] Az elektronikus egészségügyi nyilvántartás a betegek kórtörténetének elektronikus változata, és tartalmazhat az érintett egyénekre vonatkozó klinikai adatokat, például múltbeli kórtörténetre, problémákra és állapotokra, gyógyszerelésekre és kezelésekre vonatkozó adatokat, továbbá laboreredményeket és jelentéseket. Ezekhez az elektronikus állományokhoz, amelyek a teljes nyilvántartástól a kivonatokig vagy összefoglalókig terjedhetnek, hozzáférhetnek a háziorvosok, gyógyszerészek és egyéb egészségügyi szakemberek. Az „eEgészségügy" elgondolása szintén ezeket az egészségügyi nyilvántartásokat érinti.

944 *Uo.*, 2. cikk (2) bekezdés 11. pont.

945 *Uo.*, 9. cikk (1) bekezdés és (67) preambulumbekezdés.

946 Általános adatvédelmi rendelet, (156) és (161) preambulumbekezdés.

947 Európai adatvédelmi biztos (2013), Az európai adatvédelmi biztos véleménye az „E-egészségügyi cselekvési terv 2012–2020 – innovatív egészségügyi ellátás a 21. században" című bizottsági közleményről, Brüsszel, 2013. március 27.

948 A Bizottság ajánlása (2008. július 2.) az elektronikus egészségügyi nyilvántartó rendszerek határokon átnyúló átjárhatóságáról, 3(c) pont.

Példa: A. biztosítást kötött a B. biztosítótársasággal. Az utóbbi A-tól bekér néhány egészségi állapottal, például folyamatos egészségügyi problémával vagy betegségekkel kapcsolatos adatot. A biztosítónak A. egészségi állapotával kapcsolatos adatait az egyéb adatoktól elkülönítve kell tárolnia. A biztosítónak az egészségi állapottal kapcsolatos adatokat az egyéb személyes adatoktól is elkülönítve kell tárolnia. Ez azt jelenti, hogy csak A. ügyének kezelőjének lesz hozzáférése az A. egészségi állapotával kapcsolatos adatokhoz.

Mindazonáltal az elektronikus egészségügyi dokumentumok felvetnek néhány adatvédelmi kérdést, például az azokhoz való hozzáférést, megfelelő tárolásukat, és az érintett általi hozzáférést illetően.

Az elektronikus egészségügyi nyilvántartásokon kívül 2014. április 10-én az Európai Bizottság közzétett egy zöld könyvet a mobil egészségügyre (m-egészségügy) vonatkozóan, amelyben megállapítja, hogy az m-egészségügy egy olyan fejlődő és gyorsan növekedő terület, amely magában rejti az egészségügy átalakításának, hatékonysága növelésének és minősége javításának lehetőségét. A kifejezés mobil eszközök, például mobiltelefonok, betegfigyelő eszközök, digitális személyi asszisztens és más vezeték nélküli eszközök, illetve alkalmazások (jólléti alkalmazások) által támogatott, és orvosi készülékekhez vagy érzékelőkhöz csatlakoztatható orvosi és közegészségügyi szolgáltatásra utal.[949] A dokumentum részletezi, hogy az m-egészségügy fejlődése milyen kockázatokkal jár a személyes adatok védelméhez való jogra nézve, és rendelkezik arról, hogy figyelemmel az egészségügyi adatok különleges jellegére, a biztonsági kockázatok mérséklése érdekében a fejlesztésnek konkrét és megfelelő garanciákat kell nyújtaniuk, mint például a betegek adatainak titkosítása, továbbá megfelelő hitelesítési mechanizmusokat. A személyes adatok védelmére, az érintett tájékoztatására, valamint az adatbiztonságra vonatkozó szabályok betartása, továbbá a személyes adatok jogszerű feldolgozásának elve alapvetően fontos az m-egészségügyi megoldások iránti bizalom megalapozásához.[950] Ebből a célból az ágazat összeállított egy magatartási kódexet, amely az érdekeltek széles körének – ideértve az adatvédelem terén jártas képviselőket, az ön- és társszabályozás, IKT és egészségügy képviselőit – meglátásain alapul.[951] A kézikönyv megszövegezésének idején a magatartási kódex tervezetét

949 Európai Bizottság (2014), Zöld könyv a mobil egészségügyről („m-egészségügyről"), COM(2014) 219 final, Brüsszel, 2014. április 10.

950 *Uo.*, 8. o.

951 Adatvédelmi magatartási kódex a mobil egészségügyi alkalmazásokra vonatkozóan, 2016. június 7.

észrevételezésre benyújtották a 29. cikk szerinti munkacsoportnak, és annak hivatalos jóváhagyására vár.

9.4 Kutatási és statisztikai célú adatkezelés

Főbb pontok

- A statisztikai, tudományos vagy történelmi kutatási célokra gyűjtött adatok semmilyen más célra nem használhatók fel.
- A bármilyen célból jogszerűen gyűjtött adatok statisztikai, tudományos vagy történelmi kutatási célokra tovább felhasználhatók, feltéve, hogy biztosítottak a megfelelő garanciák. Ebből a célból az adatok harmadik feleknek történő továbbítása előtti anonimizálással vagy álnevesítéssel biztosíthatók ezek a garanciák.

Az **uniós jog** akkor engedi meg az adatok statisztikai, tudományos vagy történelmi kutatási célokból való kezelését, ha az érintett jogait és szabadságait illetően megfelelő garanciák vannak érvényben. Ez lehet az adatok álnevesítése is.[952] Az uniós vagy a nemzeti jog biztosíthat bizonyos eltéréseket az érintettek jogaitól, ha e jogok valószínűsíthetően lehetetlenné teszik vagy súlyosan hátráltatják a kutatás jogszerű céljainak elérését.[953] Az eltérés alkalmazható az érintett hozzáférési jogára, helyesbítési jogára, az adatkezelés korlátozásához való jogára és a tiltakozási jogra.

Noha az adatkezelő által bármilyen célra jogszerűen gyűjtött adatokat az adatkezelő saját statisztikai, tudományos vagy történelmi kutatási célból ismét felhasználhatja, az adatot anonimizálni kell, vagy például az adott esettől függően álnevesíteni kell, mielőtt azokat harmadik félnek továbbítja statisztikai, tudományos vagy történelmi kutatási célból, kivéve, ha az érintett hozzájárult ehhez, vagy arról nemzeti jogszabály kifejezetten rendelkezik. Az álnevesített adatok – az anonimizált adatokkal ellentétben – továbbra is az általános adatvédelmi rendelet hatálya alá tartoznak.[954]

A rendelet így tehát különleges bánásmódban részesíti a kutatást az általános adatvédelmi szabályokat illetően a tudományos kutatás korlátozásának elkerülése, és az európai kutatási térség elérését szolgáló célkitűzés teljesítése érdekében az EUMSZ 179. cikkben foglaltaknak megfelelően. Rendelkezik arról, hogy

952 Általános adatvédelmi rendelet, 89. cikk (1) bekezdés.

953 *Uo.*, 89. cikk (2) bekezdés.

954 *Uo.*, (26) preambulumbekezdés.

a személyes adatok kezelését tudományos kutatási célokból tág körűen kell értelmezni, oly módon, hogy az magában foglalja többek között a technológiafejlesztési és demonstrációs tevékenységeket, az alapkutatást, az alkalmazott kutatást, és a magánfinanszírozású kutatást. Felismeri továbbá a nyilvántartásokból származó adatok kutatási célú összevetésének jelentőségét és azt, hogy az adatgyűjtés időpontjában nehéz lehet meghatározni a személyes adatok tudományos kutatási célú kezelésének további célját.[955] Ebből az okból a rendelet lehetővé teszi az adatok e célból történő kezelését az érintett hozzájárulása nélkül, feltéve, hogy megfelelő biztosítékok vannak érvényben.

Az adatok statisztikai célokra való felhasználásának fontos példája a nemzeti és uniós statisztikai hivatalok által a hivatalos statisztikákról szóló nemzeti és uniós jogszabályok alapján készített hivatalos statisztikák. E jogszabályok szerint a polgárok és a vállalkozások általában kötelesek adatokat közölni az érintett statisztikai hatóságokkal. A statisztikai hivatalokban dolgozó tisztviselőkre speciális szakmai titoktartási kötelezettségek vonatkoznak, amelyeket megfelelően be kell tartani, mivel a polgároknak a statisztikai hatóságok részére történő kötelező adatszolgáltatásba vetett bizalma szempontjából alapvető fontosságúak.[956]

Az európai statisztikákról szóló 223/2009/EK rendelet (európai statisztikákról szóló rendelet) a hivatalos statisztikákkal összefüggő alapvető adatvédelmi szabályokat tartalmazza, ezért a nemzeti szintű hivatalos statisztikákra vonatkozó rendelkezések tekintetében is relevánsnak tekinthető.[957] A rendelet fenntartja azt az elvet, hogy a hivatalos statisztikai tevékenységhez kellően egyértelmű jogalap szükséges.[958]

955 *Uo.*, (33), (157) és (159) preambulumbekezdés.

956 *Uo.*, 90. cikk.

957 Az Európai Parlament és a Tanács 223/2009/EK rendelete (2009. március 11.) az európai statisztikákról és a titoktartási kötelezettség hatálya alá tartozó statisztikai adatoknak az Európai Közösségek Statisztikai Hivatala részére történő továbbításáról szóló 1101/2008/EK, Euratom európai parlamenti és tanácsi rendelet, a közösségi statisztikákról szóló 322/97/EK tanácsi rendelet és az Európai Közösségek statisztikai programbizottságának létrehozásáról szóló 89/382/EGK, Euratom tanácsi határozat hatályon kívül helyezéséről, HL L 87., 2009.3.31., amelyet módosított az Európai Parlament és a Tanács (EU) 2015/759 rendelete (2015. április 29.) az európai statisztikákról szóló 223/2009/EK rendelet módosításáról, HL L 123., 2015.5.19.

958 Ezt az elvet az Eurostat gyakorlati kódexe részletesebben is kifejti, amely az európai statisztikákról szóló rendelet 11. cikkével összhangban etikai iránymutatást ad a hivatalos statisztikák elkészítésének módjára vonatkozóan, a személyes adatok körültekintő használatát is beleértve.

Példa: A *Huber kontra Németországi Szövetségi Köztársaság* ügyben[959] egy Németországba költözött osztrák üzletember panaszában arra hivatkozott, hogy külföldiek személyes adatainak gyűjtése és tárolása egy központi nyilvántartásban (AZR) – statisztikai célokból is – a német hatóságok által sérti az adatvédelmi irányelv szerinti jogait. Figyelemmel arra, hogy a 95/46 irányelvnek az volt a szándéka, hogy valamennyi tagállamban azonos védelmi szintet biztosítson, az EUB megállapította, hogy a magas védelmi szint EU-ban történő biztosítása érdekében a 7. cikk e pontjában foglalt szükségesség fogalma nem lehet eltérő tartalmú az egyes tagállamokban. Ez tehát egy önálló közösségi jogi fogalom az uniós jogban, és oly módon kell értelmezni, hogy az maradéktalanul megfeleljen a 95/46 irányelv célkitűzésének. Az EUB, miután megállapította, hogy statisztikai célból kizárólag anonim információk kérhetők, azt az ítéletet hozta, hogy a német nyilvántartás nem összeegyeztethető a 7. cikk e) pontjában foglalt szükségességi követelménnyel.

Az **Európa Tanács** jogának összefüggésében az adatok további kezelése tudományos vagy történelmi kutatási, valamint statisztikai célból megengedett, amennyiben az közérdekből történik, és megfelelő garanciák vannak érvényben.[960] Az érintettek jogai a statisztikai célból történő adatkezelés vonatkozásában korlátozhatók is, feltéve, hogy az érintettek jogai és szabadságai megsértésének kockázata nem áll felismerhetően fenn.[961]

Az 1997-ben kiadott, statisztikai adatokra vonatkozó ajánlás a köz- és magánszektorban végzett statisztikai tevékenységgel foglalkozik.[962]

A statisztikai célokra adatkezelő által gyűjtött adatok semmilyen más célra nem használhatók fel. A nem statisztikai célból gyűjtött adatok további statisztikai célokra felhasználhatók. A statisztikai adatokra vonatkozó ajánlás még az adatok harmadik felekkel való közlését is megengedi, feltéve, hogy ez kizárólag statisztikai célokra történik. Ilyen esetben a feleknek meg kell állapodniuk, és írásban rögzíteniük kell a statisztikai célú további törvényes felhasználás mértékét. Mivel ez nem

959 EUB, *Heinz Huber kontra Bundesrepublik Deutschland* [nagytanács], C-524/06. sz. ügy, 2008. december 16., lásd különösen a 68. pontot.

960 Korszerűsített 108. Egyezmény, 5. cikk (4) bekezdés b) pont.

961 *Uo.*, 11. cikk (2) bekezdés.

962 Európa Tanács, Miniszteri Bizottság (1997), Rec(97)18. sz. ajánlás a tagállamok részére statisztikai célokra gyűjtött és feldolgozott személyes adatok védelméről, 1997. szeptember 30.

helyettesítheti az érintett hozzájárulását – amennyiben szükség van arra –, feltételezhető, hogy a személyes adatokkal való visszaélés kockázatainak minimalizálása érdekében nemzeti jogszabályban előírt megfelelő garanciákra – például az adatok továbbítás előtti anonimizálására vagy álnevesítésére irányuló kötelezettségre – van szükség.

A hivatásszerűen statisztikai kutatással foglalkozó szakembereket a nemzeti jog szerint speciális szakmai titoktartási kötelezettségnek kell terhelnie, ami a hivatalos statisztikák esetében szokásos. A titoktartásnak a kérdezőkre és a személyes adatok egyéb kezelőire is ki kell terjednie, ha az érintettektől vagy más személyektől való adatgyűjtés a munkaköri kötelezettségük.

Ha a személyes adatok felhasználásával készített statisztikai felmérést nem jogszabály engedélyezi, ahhoz, hogy a felmérés törvényes legyen, az érintetteknek hozzá kellene járulniuk adataik felhasználásához, vagy legalább lehetőséget kellene biztosítani számukra a tiltakozásra. Ha statisztikai célokra kérdezők gyűjtenek személyes adatokat, egyértelműen tájékoztatni kell őket arról, hogy a nemzeti jog értelmében az adatok közlése kötelező-e vagy sem.

Ha a statisztikai felmérés anonim adatokkal nem végezhető el, és szükség van személyes adatokra, az e célra gyűjtött adatokat a lehető leghamarabb anonimizálni kell. A statisztikai felmérés eredményei alapján az érintettek nem lehetnek azonosíthatók, kivéve, ha ez egyértelműen semmiféle kockázatot nem jelentene.

A statisztikai elemzés lezárását követően a felhasznált személyes adatokat törölni vagy anonimizálni kell. Ilyen esetekben a statisztikai adatokra vonatkozó ajánlás azt tanácsolja, hogy az azonosító adatokat más személyes adatoktól elkülönítve kell tárolni. Ez azt jelenti például, hogy vagy a titkosítási kulcsot, vagy az azonosító szinonimákat tartalmazó listát az egyéb adatoktól elkülönítve kell tárolni.

9.5 Pénzügyi adatok

Főbb pontok

- Bár a pénzügyi adatok nem a Korszerűsített 108. Egyezmény vagy az általános adatvédelmi rendelet értelmében vett különleges adatok, kezelésük – a pontosság és az adatbiztonság szavatolása érdekében – különleges garanciákat igényel.

- Az elektronikus pénzforgalmi rendszerek esetében a rendszerbe eleve beépített – beépített és alapértelmezett – adatvédelem szükséges.
- Ezen a területen speciális adatvédelmi problémák merülnek fel a megfelelő hitelesítési mechanizmusok meglétének igényéből fakadóan.

Példa: A *Michaud kontra Franciaország* ügyben[963] a felperes, egy francia ügyvéd, vitatta a francia jog alapján fennálló azon kötelezettségét, hogy be kell jelentenie ügyfelei lehetséges pénzmosási tevékenységével kapcsolatos gyanúját. Az EJEB megállapította, hogy az ügyvédek arra való kötelezése, hogy jelentsenek olyan információkat a közigazgatási hatóságoknak egy másik személyről, amelyek hivatalos információcsere során kerültek a birtokukba, beavatkozásnak minősül az ügyvéd – az EJEE 8. cikke alapján fennálló – kapcsolattartási jogának és magánéletének tiszteletben tartásához való jogába, mivel e fogalomba a szakmai vagy üzleti jellegű tevékenységek is beletartoznak. A beavatkozás azonban megfelelt a jogszabályoknak, és törvényes célt szolgált – nevezetesen zavargás vagy bűncselekmény megelőzését. Mivel az ügyvédek csupán igen korlátozott körülmények fennállása esetén voltak kötelesek a gyanú bejelentésére, az EJEB megállapította, hogy ez a kötelezettség arányos. Arra a következtetésre jutott, hogy Franciaország nem sértette meg az Egyezmény 8. cikkét.

Példa: Az *M.N. és társai kontra San Marino* ügyben[964] a felperes, egy olasz állampolgár, vagyonkezelői szerződést kötött egy nyomozás alá vont társasággal. Ez azt jelentette, hogy a társaságnál átkutatták és lefoglalták a(z) (elektronikus) dokumentumok másolatait. A felperes panaszt nyújtott be a San Marinó-i bíróságon, azt állítva, hogy nem volt köze a feltételezett bűncselekményekhez. A bíróság azonban a panaszát elfogadhatatlannak minősítette, mivel ő nem minősült „érdekelt félnek". Az EJEB megállapította, hogy a felperes jelentős hátrányt szenvedett a bírósági védelem tekintetében egy „érdekelt félhez" képest, noha adatai továbbra is a kutatási és lefoglalási műveletek tárgyát képezték. Így tehát a Bíróság megállapította a 8. cikk megsértését.

963 EJEB, *Michaud kontra Franciaország*, 12323/11. sz. ügy, 2012. december 6. Lásd még: EJEB, *Niemietz kontra Németország*, 13710/88. sz. ügy, 1992. december 16., 29. pont; EJEB, *Halford kontra Egyesült Királyság*, 20605/92. sz. ügy, 1997. június 25., 42. pont.

964 EJEB, *M.N. és társai kontra San Marino*, 28005/12. sz. ügy, 2015. július 7.

Példa: A *G.S.B. kontra Svájc* ügyben[965] a felperes bankszámlaadatait az USA és Svájc közötti közigazgatási együttműködési megállapodás alapján megküldték az USA adóhatóságának. Az EJEB megállapította, hogy a szóban forgó adattovábbítás nem sértette az EJEE 8. cikkét, mivel a felperes jogaiba való beavatkozást törvény írta elő, törvényes célt szolgált és a szóban forgó közérdekkel arányos volt.

A 108. Egyezményben meghatározott általános adatvédelmi keretnek a pénzforgalommal összefüggésben történő alkalmazását az **Európa Tanács** 1990-es, (90)19. sz. ajánlásában dolgozták ki.[966] Ez az ajánlás a kifizetésekkel – különösen a bankkártyás fizetésekkel – összefüggésben pontosítja a törvényes adatgyűjtés és -felhasználás terjedelmét. Részletes ajánlásokat is megfogalmaz a belföldi jogalkotók számára a fizetési adatok harmadik felekkel való közlésének szabályaira, az adatok megőrzésének időbeli korlátaira, az átláthatóságra, az adatbiztonságra és az országhatárokat átlépő adatáramlásra, valamint a felügyeletre és a jogorvoslatokra vonatkozóan. Az Európa Tanács kidolgozott egy véleményt az adóügyi adatok továbbítására vonatkozóan is,[967] amely ajánlásokat fogalmaz meg, és rámutat arra, hogy mely kérdéseket kell figyelembe venni adóügyi adatok továbbításakor.

Az EJEB megengedi a pénzügyi adatok – különösen az egyén bankszámla adatainak – továbbítását az EJEE 8. cikke alapján, ha azt törvény írja elő, törvényes célt szolgál és a szóban forgó közérdekkel arányos.[968]

Az **uniós jog** szerint a személyesadat-kezeléssel járó elektronikus fizetési rendszereknek be kell tartaniuk az általános adatvédelmi rendelet előírásait. Ezért ezeknek a rendszereknek biztosítaniuk kell a beépített és alapértelmezett adatvédelmet. A beépített adatvédelem kötelezi az adatkezelőt, hogy megfelelő technikai és szervezési intézkedéseket léptessen érvénybe az adatvédelmi elvek végrehajtása érdekében. Az alapértelmezett adatvédelem azt jelenti, hogy az adatkezelőnek biztosítania kell, hogy alapértelmezés szerint csak azokat a személyes adatokat kezeljék, amelyek szükségesek egy adott cél eléréséhez (lásd a 4.4 szakaszt). A pénzügyi adatokat illetően az EUB megállapította, hogy a továbbított adóügyi adatok

965 EJEB, *G.S.B. kontra Svájc*, 28601/11. sz. ügy, 2015. december 22.

966 Európa Tanács, Miniszteri Bizottság (1990), (90)19. sz. ajánlás a fizetéshez és más kapcsolódó műveletekhez használt személyes adatok védelméről, 1990. szeptember 13.

967 Európa Tanács, 108. Egyezmény konzultatív bizottsága (2014), Vélemény az adóügyi adatok közigazgatási és adóügyi célból történő automatikus államközi továbbítását szolgáló mechanizmusok adatvédelmi vonzatairól, 2014. június 4.

968 EJEB, *G.S.B. kontra Svájc*, 28601/11. sz. ügy, 2015. december 22.

személyes adatoknak minősülnek.[969] A 29. cikk szerinti munkacsoport erre vonatkozóan iránymutatást adott ki a tagállamoknak, amely tartalmazza az adatvédelmi szabályoknak való megfelelés biztosításának kritériumait az adózás célját szolgáló személyes adatok automatizált cseréjekor.[970] Emellett számos jogi eszközt léptettek életbe a pénzügyi piacok és a hitelintézetek és befektetési vállalkozások tevékenységeinek szabályozása érdekében.[971] Más jogi aktusok a bennfentes kereskedelem és a piaci manipuláció elleni küzdelemhez nyújtanak segítséget.[972] A következő fő területek vannak hatással az adatvédelemre:

- a pénzügyi tranzakciókra vonatkozó nyilvántartások megőrzése;
- személyes adatok harmadik országokba történő továbbítása;
- telefonbeszélgetés vagy elektronikus kommunikáció felvétele, beleértve az illetékes hatóságok azon jogkörét, hogy telefon- és adatforgalmi nyilvántartásokat kérjenek;
- személyes információk közlése, a szankciók közzétételét is beleértve;
- az illetékes hatóságok felügyeleti és nyomozati hatásköre, a helyszíni szemlét és a dokumentumok lefoglalása céljából magánterületre való belépést is beleértve;
- jogsértések bejelentésére vonatkozó mechanizmusok, azaz visszaélés-jelentési rendszerek; és

969 EUB, *Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai*, C-201/14. sz. ügy, 2015. október 1., 29. pont.

970 29. cikk szerinti munkacsoport (2015), *Közlemény az adózás célját szolgáló személyes adatok államok közötti automatizált cseréjéről*, 14/EN WP 230.

971 Az Európai Parlament és a Tanács 2014/65/EU irányelve (2014. május 15.) a pénzügyi eszközök piacairól, valamint a 2002/92/EK irányelv és a 2011/61/EU irányelv módosításáról EGT-vonatkozású szöveg; Az Európai Parlament és a Tanács 600/2014/EU rendelete (2014. május 15.) a pénzügyi eszközök piacairól és a 648/2012/EU rendelet módosításáról, HL L 173., 2014.6.12.; Az Európai Parlament és a Tanács 2013/36/EU irányelve (2013. június 26.) a hitelintézetek tevékenységéhez való hozzáférésről és a hitelintézetek és befektetési vállalkozások prudenciális felügyeletéről, a 2002/87/EK irányelv módosításáról, a 2006/48/EK és a 2006/49/EK irányelv hatályon kívül helyezéséről, HL L 176., 2013.6.27.

972 Az Európai Parlament és a Tanács 596/2014/EU rendelete (2014. április 16.) a piaci visszaélésekről (piaci visszaélésekről szóló rendelet), valamint a 2003/6/EK európai parlamenti és tanácsi irányelv és a 2003/124/EK, a 2003/125/EK és a 2004/72/EK bizottsági irányelv hatályon kívül helyezéséről, HL L 173., 2014.6.12.

- együttműködés az illetékes tagállami hatóságok és az Európai Értékpapírpiaci Hatóság (ESMA) között.

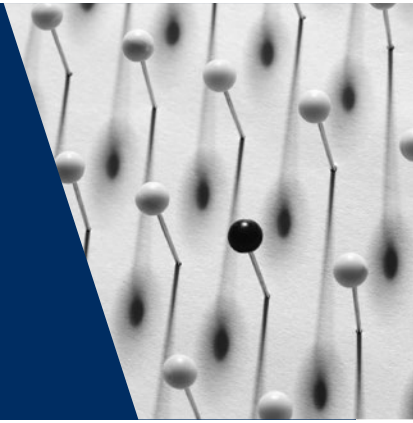
E területek más kérdéseivel külön is foglalkoznak, például az érintettek pénzügyi helyzetére vonatkozó adatok gyűjtésével[973] vagy a banki átutalásokon keresztül történő, országhatárokat átlépő fizetés kérdésével, amelyek elkerülhetetlenül személyes adatok áramlásához vezetnek.[974]

973 Az Európai Parlament és a Tanács 1060/2009/EK rendelete (2009. szeptember 16.) a hitelminősítő intézetekről, HL L 302., 2009.11.17., amelyet a közelmúltban módosított az Európai Parlament és a Tanács 2014/51/EU irányelve (2014. április 16.) a 2003/71/EK és a 2009/138/EK irányelvnek, valamint az 1060/2009/EK, az 1094/2010/EU és az 1095/2010/EU rendeletnek az európai felügyeleti hatóság (Európai Biztosítás- és Foglalkoztatóinyugdíj-hatóság) és az európai felügyeleti hatóság (Európai Értékpapírpiaci Hatóság) hatásköre tekintetében történő módosításáról, HL L 153., 2014.5.22.; Az Európai Parlament és a Tanács 462/2013/EU rendelete (2013. május 21.) a hitelminősítő intézetekről szóló 1060/2009/EK rendelet módosításáról, HL L146., 2013.5.31.

974 Az Európai Parlament és a Tanács 2007/64/EK irányelve (2007. november 13.) a belső piaci pénzforgalmi szolgáltatásokról és a 97/7/EK, a 2002/65/EK, a 2005/60/EK és a 2006/48/EK irányelv módosításáról és a 97/5/EK irányelv hatályon kívül helyezéséről, HL L 319., 2007.12.5., amelyet módosított az Európai Parlament és a Tanács 2009/111/EK irányelve (2009. szeptember 16.) a 2006/48/EK, a 2006/49/EK és a 2007/64/EK irányelvnek a központi hitelintézetek kapcsolt bankjai, egyes szavatolótőke-elemek, nagykockázat-vállalások, felügyeleti szabályok és válságkezelés tekintetében történő módosításáról, HL L 302., 2009.11.17.

10

A személyes adatok védelmének modern kori kihívásai



A digitális korszakot vagy az információs technológia korszakát a számítógépek, az internet és a digitális technológiák széles körben elterjedt használata jellemzi. Ez magában foglalja hatalmas mennyiségű adatok – köztük személyes adatok – gyűjtését és kezelését. A személyes adatok gyűjtése és kezelése egy globalizált gazdaságban azt jelenti, hogy egyre növekszik a határokon átnyúló adatáramlások száma. Az ilyen adatkezelés jelentős és látható előnyökkel járhat a mindennapi életünkre: a keresőmotorok megkönnyítik a hozzáférést jelentős mennyiségű információhoz és tudáshoz, a közösségi hálózati szolgáltatások lehetővé teszik, hogy az emberek világszerte tudjanak kommunikálni egymással, kifejezzék véleményüket és mobilizálják a szociális, környezeti és politikai indíttatású támogatásokat, miközben a vállalatok és a fogyasztók profitálnak a gazdaságot fellendítő hatékony és eredményes marketing technikákból. A technológia és az adatkezelés az állami hatóságok elengedhetetlen eszköze a bűncselekmények és terrorizmus elleni küzdelemben. Hasonlóan a nagy adathalmazok – hatalmas mennyiségű adatok gyűjtése, tárolása és elemzése a trendek azonosításához és a viselkedés előrejelzéséhez – jelentős értéket képviselnek a társadalom számára, amely fokozza a termelékenységet, a közszféra teljesítményét és a társadalmi részvételt ".[975]

Számos haszna ellenére a digitális korszak kihívásokat is jelent az adatvédelem szempontjából, mivel hatalmas mennyiségű személyes adat gyűjtése és kezelése valósul meg egyre összetettebb és átláthatatlanabb módon. A technológiai haladás olyan folyamatosan növekvő méretű adathalmazok kialakulásához vezetett, amelyek könnyen összevethetők és tovább elemezhetők, mintázatok és összefüggések

975 Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, T-PD(2017)01, Strasbourg, 2017. január 23.

feltárása érdekében, vagy olyan algoritmusok alapján történő döntések elfogadására, amelyek soha nem látott mértékű betekintést nyújtanak az emberi viselkedésbe vagy a magánéletbe.[976]

Az új technológiák erőteljesek, és különösen veszélyesek lehetnek, ha rossz kezekbe kerülnek. Az ezen technológiákat hasznosító és tömeges megfigyelést végző állami hatóságok jól példázzák, hogy e technológiák milyen komoly hatást képesek gyakorolni az egyén jogaira. 2013-ban Edward Snowden kiszivárogtatásai a titkosszolgálatok által néhány államban végzett nagymértékű internetes és telefonos megfigyelési programokkal kapcsolatosan, komoly aggodalmat keltett a megfigyelési tevékenységek magánéletre, demokratikus kormányzásra és a véleménynyilvánítás szabadságára jelentett veszélyeit illetően. A tömeges megfigyelést és a személyes adatok globalizált tárolását és kezelését, valamint az adatokhoz való tömeges hozzáférést lehetővé tevő technológiák ellentétesek lehetnek a magánélethez való jog lényegével.[977] Ráadásul ezek negatív hatást gyakorolhatnak a politikai kultúrára, a demokráciára, kreativitásra és innovációra.[978] Annak puszta ténye, hogy az állam folyamatosan nyomon követheti és elemezheti a polgárok viselkedését és tevékenységeit, elbátortalaníthatja őket attól, hogy kifejezzék véleményüket bizonyos kérdésekben, és gyanakvást, illetve óvatosságot eredményezhet.[979] Ez a kihívás arra sarkallt számos közjogi hatóságot, kutatóközpontot és civil társadalmi szervezetet, hogy elemezzék az új technológiák társadalomra gyakorolt hatásait. 2015-ben az európai adatvédelmi biztos számos kezdeményezést indított, amelyek célja a nagy adathalmazok és a dolgok internetének etikára gyakorolt hatásának vizsgálata. Nevezetesen létrehozott egy Etikai Tanácsadó Testületet, amelynek célja „nyílt és tájékozott párbeszéd kezdeményezése a digitális etikáról, amely lehetővé teszi az EU számára, hogy egyszerre biztosítsa a technológia előnyeit a társadalom

976 Európai Parlament (2017), Jelentés a nagy adathalmazok alapjogi vonatkozásairól: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés (P8_TA-PROV(2017)0076, Strasbourg, 2017. március 14.

977 Lásd: ENSZ Közgyűlés, *Különmegbízotti jelentés az emberi jogok és alapvető szabadságok előmozdításáról és védelméről a terrorizmus elleni küzdelemben*, Ben Emmerson, A/69/397, 2014. szeptember 23., 59. pont. Lásd még: EJEB, *Tájékoztató a tömeges megfigyelésről*, 2017. július.

978 Európai adatvédelmi biztos (2015), Válasz az óriásméretű adathalmazok jelentette kihívásokra, 7/2015. sz. vélemény, Brüsszel, 2015. november 19.

979 Lásd konkrétan: EUB, *Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai,* valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8., 37. pont.

és a gazdaság számára és megerősítse az egyének jogait és szabadságait, különösen a magánélethez és az adatvédelemhez fűződő jogaikat."[980]

A személyesadat-kezelés a vállalatok kezében is ütős eszköz. Manapság részletes információkat képes feltárni egy személy egészségügyi állapotával vagy pénzügyi helyzetével kapcsolatban, és ezeket az információkat a vállalatok arra használják fel, hogy fontos döntéseket hozzanak az egyének számára, például megállapítsák a rájuk vonatkozó biztosítási díjat vagy a hitelképességüket. Az adatkezelési technikák is hatással lehetnek a demokratikus folyamatokra, amikor azokat a politikusok vagy vállalatok a választások befolyásolására használják – például a szavazói kommunikáció „mikrocélzásán" keresztül. Másképp fogalmazva, míg az adatvédelmet kezdetben az egyén jogaiba való közjogi hatóságok általi indokolatlan beavatkozás elleni védelemhez való jognak tekintették, a modern korban e tekintetben már a magánszereplők is veszélyt jelentenek. Ez kérdéseket vet fel a technológiának és a prediktív elemzésnek az egyének mindennapi életét befolyásoló döntésekben való használatával kapcsolatban, és megerősíti az arra irányuló igényt, hogy minden személyesadat-kezelési tevékenység tiszteletben tartsa az alapvető jogokkal szembeni követelményeket.

Az adatvédelem szorosan összefügg a technológiai, társadalmi és politikai változásokkal, ezért lehetetlen volna összeállítani a jövőbeli kihívások egy átfogó listáját. Ez a fejezet a nagy adathalmazokat, az internetes közösségi hálózatokat és az EU digitális egységes piacát érintő válogatott területekkel foglalkozik. Ez adatvédelmi szempontból nem jelenti e területek kimerítő vizsgálatát, helyette viszont kiemeli az új vagy átdolgozott emberi tevékenységek és az adatvédelem közötti lehetséges interakciók sokaságát.

980 Európai adatvédelmi biztos, 2015. december 3-i határozat az adatvédelem etikai vonatkozásait vizsgáló külső tanácsadó testület (Etikai Tanácsadó Testület) létrehozásáról, 2015. december 3., (5) preambulumbekezdés.

10.1 Nagy adathalmazok, algoritmusok és mesterséges intelligencia

Főbb pontok

- Az IKT ágazatban zajló forradalmi innováció egy újfajta életet alakít ki, ahol a társadalmi kapcsolatok, az üzleti, magán- és közszolgáltatások digitálisan kölcsönösen kapcsolódnak egymáshoz, és ezáltal egyre növekvő mennyiségű adatot hoznak létre, amelyek nagy része személyes adat.
- A kormányok, vállalkozások és polgárok egyre inkább adatok által vezérelt gazdaságban működnek, amelyben maguk az adatok válnak értékes eszközzé.
- A nagy adathalmazok fogalma magára az adatokra és azok elemzésére is utal.
- A nagyadathalmaz-analitika révén kezelt személyes adatok az EU és az Európa Tanács szabályozása alá tartozik.
- Az adatvédelmi szabályok alóli eltérések jogokra és olyan speciális helyzetekre korlátozódnak, amelyekben a jog érvényre juttatása valószínűsíthetően lehetetlen lenne, vagy az adatkezelők részéről aránytalan erőfeszítéseket igényelne.
- A teljes mértékben automatizált döntéshozatal általában tilos, kivéve néhány speciális esetet.
- A jogok érvényesítésének biztosításához elengedhetetlen az egyének tudatossága, és hogy képesek legyenek irányítani.

Egyre digitalizáltabb világunkban minden tevékenység digitális nyomot hagy, amely gyűjthető, kezelhető és értékelhető vagy elemezhető. Az új információs és kommunikációs technológiákkal egyre több adatot gyűjtenek és rögzítenek.[981] Egészen a közelmúltig egyetlen technológia sem volt képes arra, hogy elemezze és kiértékelje a tömeges adatokat, vagy hogy hasznos következeteseket vonjon le belőle. Az adatok egyszerűen túl nagyszámúak voltak ahhoz, hogy értékelni lehessen őket, túl összetettek, rosszul strukturáltak és gyorsan változóak ahhoz, hogy trendeket vagy szokásokat lehessen azonosítani belőlük.

981 Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, „Úton a prosperáló adatközpontú gazdaság felé”, COM(2014) 442 final, Brüsszel, 2014. július 2.

10.1.1 A nagy adathalmazok, algoritmusok és mesterséges intelligencia meghatározása

Nagy adathalmazok

A „nagy adathalmazok" (vagy óriási méretű adathalmazok) egy a kontextustól függően számos fogalomra használt felkapott kifejezés. Általánosságban magában foglalja „a növekvő technológiai képességet új és prediktív ismeretek gyűjtésére, kezelésére és kivonatolására nagy mennyiségű, nagy sebességű és változatos adatokból".[982] A nagy adathalmazok fogalma ezért magára az adatokra és azok elemzésére egyaránt utal.

Az adatok **forrásai** különböző típusúak, és magukban foglalják az embereket és személyes adataikat, gépeket vagy érzékelőket, éghajlati információkat, műholdas felvételeket, digitális képeket és videókat, vagy a GPS jeleket. Az adatokat és információkat nagy mértékben azonban személyes adatok képezik, ami lehet név, fénykép, e-mail cím, banki adatok, GPS nyomkövető adatok, posztok a közösségi hálózati weboldalakon, orvosi információk vagy egy számítógép IP-címe.[983]

A nagy adathalmazok kifejezés utal a tömeges adatok és rendelkezésre álló információk **kezelésére,** elemzésére és kiértékelésére is, pl. annak érdekében, hogy hasznos információkhoz jussanak a nagyadathalmaz-elemzéshez. Ez azt jelenti, hogy a gyűjtött adatok és információk felhasználhatók az eredetileg tervezettől eltérő célokra, pl. statisztikai trendekhez, vagy sokkal testreszabottabb szolgáltatásokhoz, mint például a reklámozás. Valójában ott, ahol már léteznek a nagy adathalmazokat gyűjtő, kezelő és kiértékelő technológiák, ott bármilyen információ egyesíthető és újraértékelhető: a pénzügyi tranzakciók, hitelképesség, orvosi kezelések, magánjellegű fogyasztás, szakmai tevékenység, követés és megtett utak, internethasználat, elektronikus kártyák és telefonok, videó vagy kommunikáció megfigyelése. A nagy adathalmazok elemzése az adatoknak egy új mennyiségi dimenzióját

982 Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméről, tekintettel a személyes adatoknak a nagy adathalmazok világában való kezelésére, 2017. január 23., 2. o; Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának, „Úton a prosperáló adatközpontú gazdaság felé", COM(2014) 442 final, Brüsszel, 2014. július 2., 4. o.; Nemzetközi Távközlési Unió (2015), Y.3600. sz. ajánlás, Óriási méretű adathalmazok – A felhőalapú számítástechnika követelményei és képességei.

983 Az Európai Bizottság tájékoztatója, Az uniós adatvédelmi reform és a nagy adathalmazok; Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, 2017. január 23., 2. o.

hívja életre, egy olyat, amely kiértékelhető, és valós időben felhasználható, hogy a fogyasztóknak személyre szabott szolgáltatást lehessen nyújtani.

Algoritmus és mesterséges intelligencia

A mesterséges intelligencia az „intelligens ügynökként" viselkedő robotokra utal. Intelligens ügynökként bizonyos eszközök szoftver támogatásával képesek érzékelni környezetüket, és algoritmusok szerint cselekedni. A mesterséges intelligencia kifejezést akkor használják, amikor a gépek utánozzák a „kognitív" funkciókat – például a tanulást és problémamegoldást – amelyeket normás esetben természetes személyeknek tulajdonítunk.[984] A döntéshozatal utánzásához a modern technológiák és szoftverek algoritmusokat használnak, amelyeket a készülékek „automatikus döntéshozatalra" használnak. A algoritmus a legjobban úgy jellemezhető, mint egy lépésről lépésre történő számítás, adatkezelés, kiértékelés és automatizált indoklás és döntéshozatal.

A nagyadathalmaz-analitikához hasonlóan az általa létrehozott automatizált döntéshozatalhoz nagy mennyiségű adat összeállítása és kezelése szükséges. Ezek az adatok magából az eszközből származnak (fékek fűtése, üzemanyag, stb.) vagy a környezetből. A profilalkotás például egy olyan folyamat, amely az automatizált döntéshozatalra támaszkodik előre meghatározott sémák vagy tényezők alapján.

Példa: A profilalkotás és a célzott reklám

A profilalkotás nagy adathalmazokon alapul, és ennek során olyan mintázatokat keresnek, amelyek tükrözik „egy személyiségtípus jellemvonásait" – például, amikor az online kereskedők „ez is tetszhet" termékeket ajánlanak a korábban a kosárba helyezett termékekről gyűjtött információk alapján. Minél több az adat, annál világosabb a kép. Az okostelefon például egy erőteljes kérdőív, amelyet az egyének minden egyes használattal kitöltenek, tudatosan és tudattalanul.

A modern pszichográfia – a személyiségek tanulmányozásával foglalkozó tudomány – az OCEAN-módszert használja, amely alapján meghatározza, hogy milyen típusú személyiséggel van dolga. A „Nagy öt" személyiségdimenziók

984 Stuart Russel és Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, 27., 32–58, 968-972. o.; Stuart Russel és Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, 2. o.

a következő területeket érintik: nyitotság (Openness) (mennyire nyitott a személy az újdonságra), lelkiismeretesség (Conscientiousness) (mennyire maximalista a személy), extraverzió (Extraversion) (mennyire társaságkedvelő a személy), együttműködés (Agreeableness) (mennyire együttműködő a személy) és neurocitás (Neuroticism) (mennyire sérülékeny a személy). Ezen információk adják meg a szóban forgó egyén profilját, szükségleteit és félelmeit, viselkedésének módját stb. Ezután ezeket a személyre vonatkozó egyéb információkkal egészítik ki a rendelkezésre álló forrásokból, adatkereskedőktől, közösségi hálózatokról (beleérte a posztokra és a posztolt fotókra kapott „tetszik" -ek számát), az online hallgatott zenéket, vagy a GPS és nyomkövetési adatokat is beleértve.

A nagyadathalmaz-elemzési technikákkal létrehozott profilok tömegét hasonló mintázatok azonosítása és a személyiségcsoportok értelmezése érdekében később összevetik. Az egyes személyiségek viselkedésére és magatartására vonatkozó információk ezért invertáltak. A nagy adathalmazokhoz való hozzáféréssel és azok használatával a személyiségteszt megfordult, a viselkedésre és magatartásra vonatkozó információkat már arra használják, hogy jellemezzék az egyén személyiségét. A közösségi hálózatok „tetszik" információinak, a nyomkövetési adatoknak és a meghallgatott zenéknek vagy megnézett filmeknek a kombinációjával világos képet lehet kapni egy egyén személyiségéről, ami lehetővé teszi a vállalkozások számára, hogy személyre szabott reklámokat és/vagy információkat közöljenek az adatott személy „személyiségének" megfelelően. Ráadásul ezek az információk valós időben kezelhetők.[985]

10.1.2 A nagy adathalmazok előnyeinek és kockázatának mérlegelése

A modern adatkezelési technikák hatalmas adatmennyiségek kezelésére alkalmasak; képesek gyorsan importálni új adatokat, valós idejű adatkezelést végezni a rövid válaszidők szempontjából (még összetett kérések esetén is), több vagy egyidejű kérésekre válaszolni, és különböző típusú információkat (fotókat, szövegeket vagy számokat) elemezni. Ezek a technológiai újítások lehetővé teszik a hatalmas

985 Az adatkezelési technikák és az új szoftverek kiértékelik az arra vonatkozó információkat, hogy egy személy mit szeret, mit néz meg az online vásárlások során, vagy mit tesz az online bevásárló kosarába valós időben, és javasolhatnak számára olyan „termékeket", amelyek a gyűjtött információk alapján érdekelhetik.

tömegű adatok és információk valós idejű strukturálását, kezelését és kiértékelését.[986] A rendelkezésre álló és elemzett adatok mennyiségének exponenciális növekedésével mára lehetővé vált olyan eredmények elérése, amely kisebb mértékű elemzéssel lehetetlen lett volna. A nagy adathalmazok segítették új üzletágak kialakulását, amelyekben új szolgáltatások jelenhetnek meg a vállalkozások és fogyasztók számára egyaránt. Az uniós polgárok személyes adatainak értéke 2020-ig várhatóan évente közel 1000 milliárd euróval fog növekedni.[987] Ezért a nagy adathalmazok új **lehetőségeket** kínálhatnak a tömeges adatok új társadalmi, gazdasági vagy tudományos betekintés céljából történő kiértékelése eredményeképp, ami egyaránt az egyének, a vállalkozások és a kormányzatok hasznára válhat.[988]

A nagyadathalmaz-analitika mintázatokat képes kimutatni a különböző források és adathalmazok között, ami hasznos információkkal szolgál például a tudomány és orvoslás terén. Ez történik például az egészségügyben, az élelmiszerbiztonság, az intelligens szállítórendszerek, energiahatékonyság és várostervezés terén. Ezzel a valós idejű adatelemzéssel javíthatók az alkalmazott rendszerek. A kutatás terén új ismeretekre lehet szert tenni a nagy mennyiségű adatok és statisztikai kiértékelések összekapcsolásával különösen olyan tudományágakban, amelyekben a nagy mennyiségű adatokat eddig csak manuálisan értékelték. A rendelkezésre álló információtömeggel végzett összehasonlítások alapján az egyes betegekre szabott új kezeléseket lehet kidolgozni. A vállalkozások remélik, hogy a nagy adathalmazok elemzése versenyelőnyhöz juttatja majd őket, és lehetővé teszi számukra, hogy megtakarításokat képezzenek és új üzleti területeket hozzanak létre a közvetlen és személyre szabott ügyfélszolgálaton keresztül. A kormányzati szervek azt remélik,

986 A nagy adathalmazok: kezelésére képes szoftverek fejlesztése még mindig korai szakaszban van. Mindazonáltal a közelmúltban elemzőprogramokat fejlesztettek ki különösen a tömeges adatok és információk valós idejű elemzésére az egyének tevékenységéhez kapcsolódóan. A nagy adathalmazok strukturált módon történő elemzésének és kezelésének a lehetősége megteremtette a profilalkotás és a célzott reklám új módját. Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Úton a prosperáló adatközpontú gazdaság felé, COM(2014) 442 final, Brüsszel, 2014. július 2.; Az Európai Bizottság tájékoztatója, Az uniós adatvédelmi reform és a nagy adathalmazok; Európa Tanács, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, 2017. január 23., 2. o.

987 Az Európai Bizottság tájékoztatója, Az uniós adatvédelmi reform és a nagy adathalmazok.

988 Az adatvédelmi és a magánélet védelmével foglalkozó biztosok nemzetközi konferenciája (2014), Állásfoglalás a nagy adathalmazokra vonatkozóan; lásd továbbá: Európai Bizottság, A Bizottság közleménye az Európai Parlamentnek, a Tanácsnak, az Európai Gazdasági és Szociális Bizottságnak és a Régiók Bizottságának – Úton a prosperáló adatközpontú gazdaság felé, COM(2014) 442 final, Brüsszel, 2014. július 2., 2. o.; Az Európai Bizottság tájékoztatója, Az uniós adatvédelmi reform és a nagy adathalmazok; Európa Tanács, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, 2017. január 23., 1. o.

hogy javulásokat tudnak majd elérni a bűnügyi igazságszolgáltatás terén. A Bizottságnak az európai digitális egységes piaci stratégiáról szóló közleménye felismeri az adatközpontú technológiákban, szolgáltatásokban és a nagy adathalmazokban rejlő azon lehetőségeket, hogy katalizálják a gazdasági növekedést, innovációt és digitalizációt az EU-ban.[989]

A nagy adathalmazok ugyanakkor **kockázatokat** is hordoznak, amelyek jellemzően a kezelt adatok tulajdonságaiból, angol elnevezésük alapján a „három V-ből" fakadnak: volume (mennyiség), velocity (sebesség) és variety (sokféleség). A mennyiség a kezelt adatok mennyiségére utal, a sokféleség az adatok típusának számosságára és sokféleségére, míg a sebesség az adatkezelés sebességét jelzi. Az adatvédelemmel kapcsolatos speciális megfontolások ugyanis akkor merülnek fel, amikor a nagyadathalmaz-analitikát nagyméretű adatállományokon alkalmazzák új és prediktív ismeretek kinyerésére az egyénekre és/vagy csoportokra vonatkozó döntéshozatal céljából.[990] A nagy adathalmazok adatvédelemre és magánéletre jelentett kockázataival kiemelten foglalkoznak az európai adatvédelmi biztos és a 29. cikk szerinti munkacsoport véleményei, az Európai Parlament állásfoglalásai, valamint az Európa Tanács politikai dokumentumai.[991]

A kockázatok közé tartozik például a nagy adathalmazok helytelen kezelése az információtömeghez hozzáféréssel rendelkezők által az egyének vagy maghatározott társadalmi csoportok manipulálásán, megkülönböztetésén vagy elnyomásán keresztül.[992] Amikor az egyéni viselkedésre vonatkozóan tömeges személyes adatokat gyűjtenek, kezelnek és értékelnek, azok hasznosítása az alapvető jogok és szabadságok magánélethez való jogon túlmutató mértékű komoly megsértését eredményezheti. Lehetetlen megmérni, hogy pontosan milyen mértékben befolyásolja

989 Az Európai Parlament 2017. március 14-i állásfoglalása a nagy adathalmazok alapjogi vonatkozásairól: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés (2016/2225(INI)).

990 Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, 2017. január 23., 2. o.

991 Lásd például: Európai adatvédelmi biztos (2015), Válasz az óriás méretű adathalmazok jelentette kihívásokra, 7/2015. sz. vélemény, 2015. november 19.; Európai adatvédelmi biztos (2016), Az alapjogok következetes érvényesítése a nagy adathalmazok korában, 8/2016. sz. vélemény, 2016. szeptember 23.; Európai Parlament (2016), Jelentés a nagy adathalmazok alapjogi vonatkozásairól: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés, P8_TA(2017)0076, Strasbourg, 2017. március 14.; Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, T-PD(2017)01, Strasbourg, 2017. január 23.

992 Az adatvédelmi és a magánélet védelmével foglalkozó biztosok nemzetközi konferenciája (2014), Állásfoglalás a nagy adathalmazokra vonatkozóan.

ez a magánéletet és a személyes adatokat. Az Európai Parlament megállapította, hogy hiányzik egy olyan módszer, amellyel el lehetne végezni a nagy adathalmazok teljes hatásának bizonyítékokon alapuló értékelését, azonban léteznek arra utaló bizonyítékok, hogy a nagyadathalmaz-analitika jelentős horizontális hatást képes gyakorolni a köz- és magánszektorra egyaránt.[993]

Az általános adatvédelmi rendelet tartalmaz rendelkezéseket arra vonatkozóan, hogy az egyénnek joga van mentesülni az automatizált döntéshozatal alól, ideértve a profilalkotást is.[994] Adatvédelmi kérdés akkor merül fel, amikor a tiltakozási jog gyakorlásához emberi beavatkozás szükséges, ami lehetővé teszi az érintett számára, hogy álláspontját kifejezze, és a döntéssel szemben kifogást nyújtson be.[995] Ez kihívásokat eredményezhet a személyes adatok megfelelő szintű védelmének biztosítása terén, ha például emberi beavatkozás nem lehetséges, vagy amikor az algoritmusok túl összetettek, és az érintett adatok mennyisége túl nagy ahhoz, hogy az egyének számára bizonyos döntéseket megindokoljanak, és/vagy beszerezzék előzetes hozzájárulásukat. A mesterséges intelligencia és automatizált döntéshozatal használatára jó példa a jelzáloghitel-kérelmek, illetve toborzási folyamatok során történő alkalmazásának közelmúltbeli fejleményei. A kérelmeket elutasítják, ha a kérelmező nem felel meg előre meghatározott paramétereknek vagy tényezőknek.

10.1.3 Adatvédelmet érintő kérdések

Az adatvédelem szempontjából a legfontosabb kérdések egyrészt a kezelt személyes adatok mennyisége és változatossága, másrészt pedig a kezelés és annak eredménye. Az összetett algoritmusok és szoftverek bevezetése annak érdekében, hogy a tömeges adatokat döntéshozatali forrássá alakítsák át, különösen az egyéneket és a csoportokat érinti, nevezetesen a profilalkotás vagy címkézés esetében, és végső soron számos adatvédelmi kérdést vet fel.[996]

993 Az Európai Parlament 2017. március 14-i állásfoglalása a nagy adathalmazok alapjogi vonatkozásairól: magánélet, adatvédelem, megkülönböztetésmentesség, biztonság és bűnüldözés (2016/2225(INI)).

994 Általános adatvédelmi rendelet, 22. cikk.

995 *Uo.*, 22. cikk (3) bekezdés.

996 Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, 2017. január 23., 2. o.

Az adatkezelő és adatfeldolgozók azonosítása, és ezek felelőssége

A nagy adathalmazok és a mesterséges intelligencia számos kérdést vet fel az adatfeldolgozók azonosítása, és ezek felelőssége vonatkozásában: ilyen nagy mennyiségű adat gyűjtésekor és kezelésekor ki az adatok tulajdonosa? Amikor az adatokat intelligens gépek és szoftverek kezelik, akkor ki minősül adatkezelőnek? A kezelésben résztvevő szereplőket pontosan milyen felelősség terheli? Milyen célból használhatják fel a nagy adathalmazokat?

A felelősség kérdése a mesterséges intelligencia összefüggésében egyre nagyobb kihívást jelent, amikor a mesterséges intelligencia a saját maga által kifejlesztett adatkezelésre alapozva hoz döntéseket. Az általános adatvédelmi rendelet biztosítja a jogi keretet az adatkezelők és adatfeldolgozók felelősségéhez. A személyes adatok jogszerűtlen kezelése felveti az adatkezelő és adatfeldolgozó felelősségét.[997] A mesterséges intelligencia és az automatizált döntéshozatal kérdéseket vet fel azzal kapcsolatban, hogy ki a felelős az érintettek magánéletét érintő szabályszegésekért, amikor a kezelt adatok összetettsége és mennyisége biztonsággal nem állapítható meg. Amikor a mesterséges intelligenciát és algoritmusokat termékeknek tekintjük, kérdések merülnek fel a személyes felelősség, amelyet az általános adatvédelmi rendelet szabályoz, illetve a termékfelelősség között, amelyet viszont a rendelet nem szabályoz.[998] Ehhez kellenének felelősségre vonatkozó szabályok, amelyek áthidalnák a személyes felelősség és a robotika, valamint mesterséges intelligencia – beleértve például az automatizált döntéshozatalt – termékfelelősség közötti hézagot.[999]

Az adatvédelmi elvekre gyakorolt hatás

A nagy adathalmazok fent ismertetett jellege, elemzése és felhasználása kihívás elé állítja az európai adatvédelmi szabályozás néhány tradicionális alapelvének alkalmazását.[1000] Ezek a kihívások többnyire a jogszerűség, az adattakarékosság, a célhoz kötöttség és az átláthatóság elvével kapcsolatosak.

997 Általános adatvédelmi rendelet, 77–79. és 82. cikk.

998 Európai Parlament, Európai polgári jog szabályai a robotika terén, Belpolitikai Főigazgatóság, (2016. október), 14. o.

999 Roberto Viola beszéde a robotikára vonatozó európai jogról az Európai Parlamentben a média szemináriumon (SPEECH 16/02/2017); az Európai Parlament bejelentése a Bizottságnak a robotika és mesterséges intelligencia polgári jogi felelősségére vonatkozó javaslatra irányuló kérésére.

1000 Európa Tanács, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében az óriási méretű adathalmazok világában, T-PD(2017)01, Strasbourg, 2017. január 23.

Az adattakarékosság elve megköveteli, hogy a személyes adatok megfelelőek, relevánsak legyenek és az adatkezelési cél teljesítéséhez szükségesre korlátozódjanak. A nagy adathalmazok üzleti modellje azonban az adattakarékosság antitézise lehet, mivel ehhez minél több adatra van szükség, ráadásul gyakran meghatározatlan célokból.

Ugyanez vonatkozik a célhoz kötöttség elvére, amely előírja, hogy az adatokat konkrét célokból kell kezelni, és nem használhatók fel az adatgyűjtés eredeti céljától eltérő célra, kivéve, ha az ilyen adatkezelés jogszerű indokon alapul, vagy az érintett hozzájárulásán(lásd a 4.1.1 szakasz).

Végezetül pedig a nagy adathalmazok próbára teszik az adatok pontosságának elvét is, mivel a nagy adathalmaz alkalmazások rendszerint különféle forrásokból gyűjtenek adatokat annak lehetősége nélkül, hogy ellenőrizhessék és/vagy fenntartsák a gyűjtött adatok pontosságát.[1001]

Sajátos szabályok és jogok

A főszabály továbbra is az, hogy a nagyadathalmaz-analitikával kezelt személyes adatok az adatvédelmi szabályozás hatálya alá tartozik. Az **Unió és az Európa Tanács joga** azonban sajátos szabályokat és eltéréseket biztosít a speciális esetekre az algoritmusos összetett adatkezelés vonatkozásában.

Az Európa Tanács jogában a Korszerűsített 108. Egyezmény új jogokat biztosít az adatalanyoknak, hogy hatékonyabban ellenőrizhessék személyes adataik kezelését a big data korában. Ennek tipikus példái a Korszerűsített 108. Egyezmény 9. cikk (1) bekezdés a), c) és d) pontjai, amelyek értelmében az érintett jogosult arra, hogy ne terjedjen ki rá az olyan kizárólag automatizált adatkezelésen alapuló döntés, amely őt jelentős mértékben érintené, anélkül, hogy a véleményét figyelembe vették volna; hogy kérelemre tájékoztatást kapjon az adatkezelés indokairól amikor az adatkezelés eredményeképpen hozott döntés rá nézve hatással jár, valamint, hogy tiltakozzon az adatkezelés ellen. A Korszerűsített 108. Egyezmény más rendelkezései különösen a transzparenciára és további kötelezettségekre vonatkozó előírások a Korszerűsített 108. Egyezmény által létrehozott, a digitális kihívásokkal szembeni védelmi mechanizmusok kiegészítő elemei.

1001 Európai adatvédelmi biztos (2016), Az alapjogok következetes érvényesítése a nagy adathalmazok korában, 8/2016. sz. vélemény, 2016. szeptember 23., 8. o.

Az EU jogban az általános adatvédelmi rendelet 23. cikkében felsorolt esetek mellett valamennyi személyesadat-kezelési tevékenység tekintetében biztosítani kell az **átláthatóságot**. Különösen fontos ez az internetes szolgáltatásokkal és egyéb összetett automatizált adatkezeléssel, például az algoritmusok döntéshozatalra való használatával kapcsolatban. Itt az adatfeldolgozó rendszerek tulajdonságainak lehetővé kell tenniük, hogy az érintettek valóban megtudják, mi történik az adataikkal. A tisztességes és átlátható adatkezelés biztosítása érdekében az általános adatvédelmi rendelet előírja, hogy az adatkezelő tájékoztassa az érintettet az automatizált döntéshozatal – beleértve a profilalkotást is – során alkalmazott logikára vonatkozóan.[1002] Az Európa Tanács Miniszteri Bizottsága „A véleménynyilvánítás szabadságához és a magánélethez való jog védelme és előmozdítása a hálózatsemlegesség tekintetében" című ajánlásában azt mondta ki, hogy az internetszolgáltatók „biztosítsanak a felhasználók számára egyértelmű, teljes körű és nyilvánosan hozzáférhető információt a felhasználók tartalomhoz való hozzáférését és terjesztését, az alkalmazásokat és szolgáltatásokat érintő forgalomkezelési gyakorlatukra vonatkozóan".[1003] Az illetékes hatóságok által az internetes forgalomkezelési gyakorlatokra vonatkozóan összeállított jelentéseket valamennyi tagállamban nyílt és átlátható módon kell elkészíteni és a nyilvánosság számára ingyenesen kellene rendelkezésre bocsátani.[1004]

Az adatkezelő köteles **tájékoztatni** az érintetteket **–** akkor is, amikor az adatokat tőlük, és akkor is, amikor nem tőlük gyűjti – nem csak a gyűjtött adatokra és a tervezett adatkezelésre vonatkozó konkrét információkra vonatkozóan (lásd a 6.1.1 szakaszt), hanem adott esetben az automatizált döntéshozatal tényére és „az alkalmazott logikára" vonatkozóan is,[1005] továbbá az ilyen adatkezelés céljairól, és arról, hogy az érintettre nézve milyen várható következményekkel jár. Az általános adatvédelmi rendelet azt is pontosítja (kizárólag azokban az esetekben, amikor a személyes adatokat nem az érintettől szerzik be), hogy az adatkezelő nem köteles tájékoztatni az érintettet, amennyiben „a szóban forgó információk rendelkezésre bocsátása lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényelne".[1006] A 29. cikk szerinti munkacsoport az *Iránymutatás a 2016/679 rendelet alkalmazásában történő automatizált egyedi döntéshozatalhoz és*

1002 Általános adatvédelmi rendelet, 13. cikk (2) bekezdés f) pont.

1003 Európa Tanács, Miniszteri Bizottság (2016), CM/Rec(2016)1. sz. ajánlás: a véleménynyilvánítás szabadságához és a magánélethez való jog védelme és előmozdítása a hálózatsemlegesség tekintetében, 2016. január 13., 5.1. pont.

1004 *Uo.*, 5.2. pont.

1005 Általános adatvédelmi rendelet, 13. cikk (2) bekezdés f) pont és 14. cikk (2) bekezdés g) pont.

1006 *Uo.*, 14. cikk (5) bekezdés b) pont.

a profilalkotáshoz című véleményében ugyanakkor hangsúlyozta, hogy az adatkezelés összetettsége önmagában nem zárhatja ki, hogy az adatkezelő világos magyarázatot nyújtson az érintett számára a célokra és az adatkezelés során használt analitikára vonatkozóan.[1007]

Az érintettek joga, hogy **hozzáférjenek** személyes adataikhoz, **helyesbítsék** és **töröljék** azokat, továbbá hogy **korlátozzák** az adatkezelést, nem tartalmaz hasonló mentességet. Az adatkezelő azon kötelezettsége azonban, hogy tájékoztassa az érintettet a személyes adatait érintő helyesbítésről vagy törlésről (lásd a 6.1.4 szakaszt) szintén feloldható, amennyiben „ez lehetetlennek bizonyul, vagy aránytalanul nagy erőfeszítést igényel".[1008]

Az érintettek az általános adatvédelmi rendelet 21. cikke alapján (lásd a 6.1.6 szakaszt) jogosultak tiltakozni személyes adataik kezelése ellen, ideértve a nagyadathalmaz-analitikát is. Bár az adatkezelők mentesülhetnek e kötelezettség alól, ha elsőbbséget élvező jogos érdekeket igazolnak, nem élvezik ugyanezt a mentességet az adatok közvetlen üzletszerzés céljából történő kezelése esetén.

E jogoktól való speciális eltéréseket is alkalmazhatnak az adatkezelők, amennyiben a személyes adatok kezelése a közérdekű archiválás céljából, tudományos és történelmi kutatási célból vagy statisztikai célból történik.[1009]

A **profilalkotással és automatizált döntéshozatallal kapcsolatban** az általános adatvédelmi rendelet speciális szabályokat vezetett be: A 22. cikk (1) bekezdése kiköti, hogy az érintett „jogosult arra, hogy ne terjedjen ki rá az olyan, kizárólag automatizált adatkezelésen alapuló döntés hatálya, amely rá nézve joghatással járna". A 29. cikk szerinti munkacsoport irányelvében kiemelte, hogy ez a cikk a teljes mértékben automatizált döntéshozatal általános tilalmát jelenti.[1010] Az adatkezelők kizárólag három konkrét esetben mentesülhetnek e tilalom alól, mégpedig, ha a döntés: 1) az érintett és az adatkezelő közötti szerződés megkötése vagy teljesítése érdekében szükséges, 2) uniós vagy tagállami jog teszi lehetővé, vagy 3) kifejezett hozzájáruláson alapul.[1011]

1007 29. cikk szerinti munkacsoport, *Iránymutatás a 2016/679 rendelet alkalmazásában történő automatizált egyedi döntéshozatalhoz és a profilalkotáshoz*, WP 251, 2017. október 3., 14 o.

1008 Általános adatvédelmi rendelet, 19 cikk.

1009 *Uo.*, 89. cikk (2) és (3) bekezdés

1010 29. cikk szerinti munkacsoport, *Iránymutatás a 2016/679 rendelet alkalmazásában történő automatizált egyedi döntéshozatalhoz és a profilalkotáshoz*, WP 251, 2017. október 3., 9 o.

1011 Általános adatvédelmi rendelet, 22. cikk (2) bekezdés.

Egyedi kontroll

A nagyadathalmaz-analitika összetettsége és az azt körülvevő átláthatóság hiánya szükségessé teszi a személyes adatok egyedi kontrolljának újragondolását. Azt az adott társadalmi és technológiai környezethez kellene igazítani, figyelembe véve az ismeretek hiányát az egyének részéről. Ezért a nagy adathalmazokkal kapcsolatos adatvédelemnek az adatok felhasználása feletti tágabb értelemben vett kontrollt kellene alkalmaznia, amely szerint az egyedi kontroll az adatok felhasználásához kapcsolódó kockázatokra vonatkozó hatásvizsgálatok összetettebb folyamatává válna.[1012]

Az, hogy mennyire jó egy nagyadathalmaz-alkalmazás attól függ, hogy az mennyire jól tudja előre jelezni a tesztegyének (vagy fogyasztók) vágyait vagy viselkedéseit. A jelenlegi nagyadathalmaz-analitikán alapuló prediktív modelleket folyamatosan finomítják. A közelmúlt fejlesztései közé tartozik nem csak az adatoknak a személyiségek kategorizálására (vagyis viselkedés és magatartás) történő használata, hanem a viselkedések elemzése is hangminták, valamint annak elemzése révén, hogy az üzeneteket milyen gyorsan gépelik be, vagy akár a testhőmérséklet elemzése alapján. Mindezen információk valós időben használhatók a nagy adathalmazok kiértékeléséből levont ismeretekkel összevetve, például a hitelképesség értékelésére egy banki képviselővel folytatott megbeszélés során. Az értékelés nem a hitelért folyamodó egyén érdemei alapján történik, hanem inkább az elemzésből kapott viselkedési jellemzők, valamint a nagy adathalmazok kiértékelésével kapott információk alapján, vagyis a jelölt erőteljes vagy hízelgő hangú beszédje, testbeszéde vagy testhőmérséklete alapján.

A profilalkotás és a célzott reklám nem feltétlenül jelent problémát, ha az egyének **tisztában** vannak azzal, hogy személyre szabott hirdetések célpontjai. A profilalkotás akkor válik problémává, ha az egyének manipulálására használják, vagyis arra, hogy pl. politikai kampány céljából egy bizonyos személyiségű egyéneket vagy csoportokat találjanak. A bizonytalan szavazók csoportját például meg lehet szólítani az ő „személyiségükre" és magatartásukra szabott politikai hirdetésekkel. Egy másik probléma lehet az ilyen profilalkotás arra való használata, hogy bizonyos egyénektől megtagadják az árukhoz vagy szolgáltatásokhoz való hozzáférést. Egy garancia, amely védelmet tud nyújtani a nagy adathalmazokkal való visszaélésekkel szemben

1012 Európa Tanács, a 108. Egyezmény konzultatív bizottsága, Iránymutatás az egyének védelméhez a személyes adatok kezelése tekintetében a big data világában, T-PD(2017)01, Strasbourg, 2017. január 23.

a személyes adatok álnevesítése (lásd a 2.1.1 szakaszt).[1013] Azok az esetek, ahol a személyes adatok valóban anonimizálva vannak, vagyis ahol az információ nem hagy az érintetthez vezető nyomokat maga után, nem tartoznak az általános adatvédelmi rendelet hatálya alá. Az érintettek és egyének hozzájárulása a nagy adathalmazok kezelése során szintén kihívást jelent az adatvédelmi törvény számára. Ez kiterjed azon hozzájárulásra, hogy az érintett személyre szabott reklámok és profilalkotás alanya legyen, ami „ügyfél-élmény" szempontjából indokolható lehet, valamint a személyes adattömegek felhasználására az információalapú, analitikai eszközök finomítása és kifejlesztése érdekében. A nagy adathalmazokkal kapcsolatos tudatosság vagy a tudatosság hiánya számos kérdést vet fel azzal kapcsolatban, hogy az érintettek miként gyakorolhatják jogaikat, figyelemmel arra, hogy a nagy adathalmazok kezelése álnevesített és algoritmusok tárgyát képező anonimizált adatokra egyaránt támaszkodhat. Míg az álnevesített adatok az általános adatvédelmi rendelet hatálya alá tartoznak, a rendelet nem vonatkozik az anonimizált adatokra. Az egyedi kontroll és a tudatosság a személyes adatok feldolgozásával kapcsolatban döntő fontosságú a nagyadathalmaz-analitikában: enélkül az egyéneknek nem lesz világos elképzelésük az adatkezelő személyéről, és ez megakadályozza, hogy hatékonyan gyakorolhassák jogaikat.

10.2 Web 2.0 és web 3.0: közösségi hálózatok és a dolgok internete

Főbb pontok

- A közösségi hálózatépítő szolgáltatások online kommunikációs platformok, amelyek lehetővé teszik, hogy az egyén hasonló gondolkodású felhasználók hálózatához csatlakozzon, vagy ilyen hálózatot létrehozzon.
- A dolgok internete a tárgyak internethez való csatlakozását és a tárgyak egymás közötti összekapcsolódását jelenti.
- Az érintettek hozzájárulása az adatkezelők által a közösségi hálózatokon végzett jogszerű adatkezelés leggyakoribb jogalapja.
- A közösségi hálózatok felhasználóit általában védi az „otthoni tevékenységre vonatkozó mentesítés", ez az eltérés azonban speciális összefüggésekben feloldható.

1013 *Uo.*, 2. o.

- A közösségi hálózatok szolgáltatóit nem védi az „otthoni tevékenységre vonatkozó mentesítés”.
- A beépített és alapértelmezett adatvédelem döntő fontosságú az adatbiztonság biztosításához ezen a területen.

10.2.1 A web 2.0 és a web 3.0 meghatározása

Közösségi hálózatépítő szolgáltatások

Az internetet eleinte úgy képzelték el, hogy az a számítógépek egymással való összekapcsolására és üzenetek küldésére szolgáló hálózat korlátozott adatcsere lehetőségével, amely a weboldalakat pusztán azért kínálja, hogy az egyének passzívan megtekintsék azok tartalmát.[1014] A web 2.0 korszakban az internet egy olyan fórummá alakult, ahol a felhasználók egymással kapcsolatba lépnek, együttműködnek és tartalmat hoznak létre. Ezt a korszakot a közösségi hálózatépítő szolgáltatások figyelemre méltó sikere és széles körű használata jellemzi, amely már emberek milliói számára a mindennapok elengedhetetlen részét képezi.

A közösségi hálózatépítő szolgáltatások vagy a „közösségi média” tág értelemben úgy definiálható, mint „online kommunikációs platformok, amelyek lehetővé teszik az egyén számára, hogy hasonló gondolkodású felhasználók hálózatához csatlakozzon, vagy ilyen hálózatot létrehozzon”.[1015] Ahhoz, hogy egy hálózathoz csatlakozzanak vagy hálózatot hozzanak létre, az egyéneket felkérik, hogy adják meg személyes adataikat és hozzák létre profiljukat. A közösségi hálózatépítő szolgáltatások lehetővé teszik, hogy a felhasználók digitális „tartalmat” hozzanak létre a fényképektől és a videóktól egészen az újságokra mutató linkekig és saját nézeteiket kifejező személyes posztokig. Ezeken az online kommunikációs platformokon keresztül a felhasználók számos más felhasználóval kapcsolatba léphetnek és kommunikálhatnak. Fontos, hogy a népszerű közösségi hálózatépítő szolgáltatások nem kérnek regisztrációs díjat. A felhasználók számára előírt csatlakozási díj helyett a közösségi hálózatépítő szolgáltatók árbevételének többsége inkább célzott reklámokból származik. A hirdetők komolyan profitálnak a naponta ezeken az oldalakon közzétett személyes adatokból. A felhasználók korának, nemének, tartózkodási helyének és érdeklődési körének birtokában hirdetéseikkel a „megfelelő” emberekhez jutnak el.

1014 Európai Bizottság (2016), *A dolgok internetének fejlesztése Európában*, SWD(2016) 110 final.

1015 29. cikk szerinti munkacsoport (2009), *5/2009. sz. vélemény az internetes ismeretségi hálózatokról*, WP 163, 2009. június 12., 4. o.

Az Európa Tanács Miniszteri Bizottsága elfogadta a személyes adatok közösségi hálózatépítő szolgáltatásokkal kapcsolatos védelméről szóló ajánlását,[1016] amely kifejezett rendelkezéseket tartalmaz az adatvédelemről, és amelyet 2018-ban egy másik ajánlás egészített ki az internetes közvetítők szerepéről és felelősségéről.[1017]

Példa: Nóra nagyon boldog, mert párja megkérte a kezét. A jó hírt szeretné megosztani barátaival és családjával, ezért úgy dönt, hogy egy érzelmes posztot ír egy közösségi oldalon, ahol hangot ad örömének, és kapcsolati állapotát „eljegyzettre" állítja. A következő napokban, amikor Nóra belép a fiókjába, esküvői ruhákat és virágüzleteket hirdető reklámokat lát. Hogy ennek mi az oka?

Amikor egy hirdetést hoztak létre a Facebookon, az esküvői ruhákkal és virágokkal foglalkozó vállalatok kiválasztottak néhány paramétert, hogy eljussanak a Nórához hasonló emberekhez. Amikor Nóra profilja azt jelzi, hogy nő, eljegyzett, Párizsban él, a hirdetéseket feladó esküvőiruha- és virágüzletekhez közel, azonnal látni fogja ezek hirdetését.

A dolgok internete

A dolgok internete képviseli az internet fejlődésének következő állomását, a web 3.0 korszakát. A dolgok internetével a készülékek összekapcsolhatók, és az interneten keresztül kapcsolatba tudnak lépni más készülékekkel. Ez lehetővé teszi, hogy a tárgyak és emberek egymással összekapcsolódjanak kommunikációs hálózatokon keresztül, hogy állapotukról és/vagy az őket körülvevő környezetről beszámoljanak.[1018] A dolgok internete és az összekapcsolt készülékek már valósággá váltak, és – az intelligens készülékek megalkotásával és továbbfejlesztésével – a következő néhány évben várhatóan jelentősen növekedni fognak, ami intelligens városok, intelligens otthonok és intelligens üzletek kialakulásához fog vezetni.

1016 Európa Tanács, Miniszteri Bizottság (2012), CM/Rec(2012)4. sz. ajánlás a tagállamoknak a személyes adatok közösségi hálózatépítő szolgáltatásokkal kapcsolatos védelméről, 2012. április 4.

1017 Európa Tanács, Miniszteri Bizottság (2018), CM/Rec(2018)2. sz. ajánlás a tagállamoknak az internetes közvetítők szerepéről és felelősségéről, 2018. március 7.

1018 Európai Bizottság, bizottsági szolgálati munkadokumentum, *A dolgok internetének fejlesztése Európában*, SWD(2016) 110, 2016. április 19.

Példa: A dolgok internete különösen előnyös lehet az egészségügyben. A vállalatok már megalkották azokat a készülékeket, érzékelőket és alkalmazásokat, amelyek lehetővé teszik a beteg egészségének figyelemmel kísérését. Hordható riasztógomb és a lakásban elhelyezett vezeték nélküli szenzorok használatával lehetővé válik az egyedül élő idősek napi rutinjának figyelemmel kísérése, és riasztó jelzések generálása, ha a napi ütemtervükhöz képest súlyos zavarokat észlelnek. Az idősek például széles körben használják az esést észlelő érzékelőket. Ezek az érzékelők pontosan tudják észlelni az eséseket, és értesítik az egyén orvosát és/vagy családját az esésről.

Példa: Barcelona az intelligens városok egyik legismertebb példája. 2012. óta használ a város innovatív technológiákat abból a célból, hogy létrehozzon egy intelligens tömegközlekedési, hulladékgazdálkodási, parkolási és közvilágítási rendszert. A hulladékgazdálkodás fejlesztése érdekében a város például intelligens kukákat használ. Ezek lehetővé teszik a hulladékszintek nyomon követését, és ezáltal a hulladékbegyűjtési útvonal optimalizálását. Amikor már majdnem megteltek a kukák, azok a mobil kommunikációs hálózaton keresztül jeleket küldenek, amelyet a rendszer a hulladékgazdálkodó vállalat szoftverére továbbít. A vállalat így megtervezi a legoptimálisabb hulladékbegyűjtési útvonalat, amely során előnyben részesíti azokat a kukákat, amelyeket valóban ki kell üríteni, illetve csak ezek begyűjtését szervezi meg.

10.2.2 A nagy adathalmazok előnyeinek és kockázatának mérlegelése

A közösségi hálózatépítő szolgáltatások elmúlt évtizedben végbement hatalmas bővülése és sikere arra enged következtetni, hogy **hatalmas előnnyel bírnak.** A célzott hirdetés például (a kiemelt példában leírtak szerint) különösen innovatív módja annak, ahogy a vállalatok elérik közönségüket, specifikusabb piacot kínálva számukra. A fogyasztók érdekét is szolgálhatja, ha számukra relevánsabb és érdekesebb reklámokkal találkoznak. Ennél is fontosabb azonban, hogy a közösségi hálózatépítő szolgáltatások és a közösségi média pozitív hatást is gyakorolhat a társadalomra és a változások megvalósítására. Felhatalmazzák a fogyasztókat, hogy kommunikáljanak és kapcsolatba lépjenek egymással, csoportokat és eseményeket szervezzenek az őket érintő témákban.

Hasonlóan a dolgok internete is várhatóan komoly előnyöket fog nyújtani a gazdaság számára, és az uniós stratégia részét képezi egy digitális egységes piac kialakítására irányuló stratégia. Az EU-n belül a becslések szerint 2020-ra hat milliárdra növekszik a dolgok internete kapcsolatainak száma. Az összekapcsolhatóságnak e bővülése várhatóan fontos gazdasági előnyöket fog eredményezni az innovatív szolgáltatások és alkalmazások fejlesztése révén, úgy mint jobb egészségügyet, a fogyasztók szükségleteinek jobb megértését és nagyobb hatékonyságot.

Ugyanakkor figyelemmel a közösségi média felhasználói által generált és a szolgáltatók által később kezelt hatalmas mennyiségű adatra, a közösségi hálózatépítő szolgáltatások bővülése **egyre növekvő aggodalommal** jár a magánélet és személyes adatok védelmének lehetséges módját illetően. A közösségi hálózatépítő szolgáltatások fenyegethetik a magánéletet és a véleménynyilvánítás szabadságát. Az ilyen fenyegetések közé a következők tartozhatnak: „a felhasználók kizárását eredményező folyamatok körüli jogi és eljárási garanciák hiánya; a gyermekek és fiatalkorúak nem megfelelő védelme a káros tartalmakkal vagy viselkedésekkel szemben; mások jogai tiszteletben tartásának hiánya; a magánélet tiszteletben tartását előmozdító alapértelmezett beállítások hiánya; az átláthatóság hiánya a személyes adatok gyűjtésének és kezelésének célját illetően."[1019] Az európai adatvédelmi törvény megpróbált választ adni a közösségi média által életre hívott adatvédelmi kihívásokra. Az olyan elvek, mint a hozzájárulás, beépített és alapértelmezett adatvédelem, valamint az egyének jogai különösen fontosak a közösségi média és a hálózatépítő szolgáltatások összefüggésében.

A dolgok internete összefüggésében a különféle összekapcsolt készülékekkel létrehozott személyes adatok hatalmas mennyisége kockázatot is jelent a magánélet és adatvédelem szempontjából. Bár az átláthatóság az európai adatvédelmi jog fontos elve, az összekapcsolt készülékek számossága miatt nem mindig egyértelmű, hogy ki tud adatokat gyűjteni, és hozzáférni a dolgok internetében használt eszközökről gyűjtött adatokhoz illetve felhasználni azokat.[1020] Az EU és az Európa Tanács joga szerint azonban az átláthatóság elve kötelezettséget keletkeztet az adatkezelő számára, hogy az érintetteket világosan és közérthetően megfogalmazott módon tájékoztassa adataik felhasználásának módjáról. A személyes adataik kezelését érintő kockázatokat, szabályokat, biztosítékokat és jogokat világossá kell tenni az egyének számára. A dolgok internetében használt eszközök, és a kapcsolódó adatkezelési

1019 Európai Bizottság, Rec(2012)4. sz. ajánlás a tagállamok részére az emberi jogok védelméről a közösségépítő hálózatépítő szolgáltatások tekintetében, 2012. április 4.

1020 Európai adatvédelmi biztos (2017), A dolgok internetének megértése.

műveletek és adatok számossága szintén próbára teheti az adatkezeléshez való, világos és megfelelő információk birtokában történő hozzájárulásra vonatkozó követelményt – amennyiben az adatkezelés hozzájáruláson alapul. Az egyének sokszor nincsenek tisztában az ilyen adatkezelés technikai működésével, ennélfogva pedig hozzájárulásuk következményeivel.

Egy másik komoly aggály a biztonság, figyelemmel arra, hogy az összekapcsolt készülékek különösen sérülékenyek a biztonsági kockázatokkal szemben. Az összekapcsolt készülékek változó szintű biztonsággal rendelkeznek. Mivel a standard informatikai infrastruktúrán túl üzemelnek, előfordulhat, hogy hiányzik a megfelelő adatfeldolgozási sebesség és tároló kapacitás ahhoz, hogy biztonsági szoftvert tudjanak tárolni vagy biztonsági technikákat alkalmazzanak, mint pl. adattitkosítás, álnevesítés vagy anonimizálás a felhasználók személyes adatainak védelme érdekében.

Példa: Németországban a szabályozók határoztak arról, hogy betiltják az internetre kötött játékokat, miután komoly aggályok merültek fel a játéknak a gyermekek magánéletének tiszteletben tartására gyakorolt hatását illetően. A szabályozók úgy vélték, hogy egy Cayla nevű, internethez csatlakoztatott baba egy rejtett kémszerkezetet testesít meg. A baba úgy működött, hogy a vele játszó gyermek audio kérdéseit elküldte egy digitális készüléken lévő alkalmazásnak, amely azt szöveggé alakította, és a választ megkereste az interneten. Az alkalmazás ezt követően választ küldött a babának, aki azt elmondta a gyermeknek. A babán keresztül a gyermek, valamint a közelben lévő felnőttek kommunikációját rögzíteni lehetett, és azt az alkalmazásnak lehetett továbbítani. Amennyiben a gyártók nem alkalmaztak megfelelő biztonsági intézkedéseket, a babát bárki használhatta beszélgetések kihallgatására.

10.2.3 Adatvédelmet érintő kérdések

Hozzájárulás

Európában a személyes adatok kezelése csak akkor jogszerű, ha azt megengedi az európai adatvédelmi törvény. A közösségi hálózatépítő szolgáltatók számára az érintettek hozzájárulása általában biztosítja a jogszerű adatkezelés jogalapját. A hozzájárulást szabad akaratból kell megadni, és annak konkrétnak, megfelelő

tájékoztatáson alapulónak és egyértelműnek kell lennie (lásd a 4.1.1 szakaszt).[1021] A „szabad akaratból" lényegében azt jelenti, hogy kell, hogy az érintettnek valódi választása legyen. A hozzájárulás „konkrét" és „megfelelő tájékoztatáson alapul", amennyiben az érthető, egyértelműen és pontosan hivatkozik az adatkezelés teljes hatáskörére, céljára és következményeire. A közösségi média összefüggésében megkérdőjelezhető hogy a hozzájárulás szabad akaratból történik-e, konkrét-e és megfelelő tájékoztatáson alapul-e a közösségi hálózatépítő szolgáltatók által végzett minden típusú adatkezelés tekintetében.

Példa: Ahhoz, hogy egy egyén csatlakozzon és hozzáférjen egy közösségi hálózatépítő szolgáltatáshoz, gyakran el kell fogadnia személyes adatainak különféle kezelését, és ezt gyakran anélkül, hogy megkapná a szükséges tájékoztatásokat vagy alternatív lehetőséget biztosítanának számára. Egy példa erre az, amikor ahhoz, hogy regisztráljon egy közösségi hálózatépítő szolgáltatásra, el kell fogadnia, hogy viselkedésalapú reklámot kapjon. Ahogy azt a 29. cikk szerinti munkacsoport a hozzájárulás fogalommeghatározásáról szóló véleményében megállapítja, „figyelemmel arra a jelentőségre, amelyre néhány közösségi hálózat szert tett, a felhasználók egyes csoportjai (pl. a tinédzserek) beleegyeznek, hogy a viselkedésalapú reklámokat küldjenek a számukra, csak hogy elkerüljék annak kockázatát, hogy kirekesztődjenek a társas érintkezés egyik területéről. Olyan helyzetet kell teremteni a felhasználó számára, hogy önkéntes és kifejezett hozzájárulását adhassa ahhoz, hogy viselkedésalapú reklámokat küldjenek a számára, függetlenül a közösségi hálózatszolgáltatáshoz való hozzáférésétől." [1022]

Az általános adatvédelmi rendelet alapján a 16 éven aluli gyermek személyes adatai elvben nem kezelhetők a gyermek hozzájárulása alapján.[1023] Ha az adatkezeléshez hozzájárulás szükséges, azt a gyermek szülőjének vagy gyámjának kell megadnia. A gyermekek különleges védelmet élveznek amiatt, hogy jellemzően kevésbé vannak tisztában az adatkezelés kockázataival és következményeivel. Ez a közösségi média összefüggésében nagyon fontos, mivel a gyermekek sérülékenyebbek az ilyen médiával járó néhány negatív hatással, például az internetes megfélemlítéssel (cyberbullying), online zaklatással vagy személyazonosság-lopással szemben.

1021 Általános adatvédelmi rendelet, 4. és 7. cikk; Korszerűsített 108. Egyezmény, 5. cikk.

1022 29. cikk szerinti munkacsoport (2011), *15/2011. sz. vélemény a hozzájárulás fogalmáról*, WP 187, Brüsszel, 2011. július 13., 18. o.

1023 Lásd az általános adatvédelmi rendelet 8. cikkét. Az EU tagállamok jogszabályban alacsonyabb korhatárt is előírhatnak, azonban az nem lehet 13 évnél alacsonyabb.

Biztonság, beépített és alapértelmezett adatvédelem

A személyes adatok kezeléséhez szorosan kapcsolódnak biztonsági kockázatok is, figyelemmel a biztonság olyan megsértésének folyamatos lehetőségére, amely a kezelt személyes adatok véletlen vagy jogellenes megsemmisítését, elvesztését, módosítását, jogosulatlan felfedését vagy az azokhoz való jogosulatlan hozzáférést eredményezi. Az uniós adatvédelmi jog alapján az adatkezelők és adatfeldolgozók kötelesek megfelelő technikai és szervezési intézkedéseket végrehajtani az adatkezelési műveletekbe való jogosulatlan beavatkozás megakadályozására. Az európai adatvédelmi szabályok hatálya alá tartozó közösségi hálózatépítő szolgáltatóknak eleget kell tenniük e kötelezettségnek.

A beépített és alapértelmezett adatvédelem elvei előírják az adatkezelők és adatfeldolgozók számára, hogy termékeik kialakítása tartalmazzon biztonsági elemeket, és automatikusan alkalmazzanak megfelelő adatvédelmi beállításokat. Ez azt jelenti, hogy amikor valaki úgy dönt, hogy csatlakozik egy közösségi hálózathoz, a szolgáltató nem teszi a szolgáltatás új felhasználójára vonatkozó összes információt azonnal hozzáférhetővé valamennyi felhasználója számára. A szolgáltatáshoz való csatlakozáskor az alapértelmezett adatvédelmi beállítások szerint az információk csak az egyén kiválasztott kapcsolatai számára lehetnének elérhetők. A hozzáférés kiterjesztése e listán kívüli személyekre csak akkor lehetne lehetséges, miután a felhasználó manuálisan módosította az alapértelmezett adatvédelmi beállításokat. Ennek jelentősége lehet azokban az esetekben is, amikor adatvédelmi incidens történik az érvényben lévő biztonsági intézkedések ellenére. Ilyen esetekben a szolgáltatónak tájékoztatnia kell az érintett felhasználókat, ha az adatvédelmi incidens valószínűsíthetően magas kockázattal jár az érintettek jogaira és szabadságaira nézve.[1024]

A beépített és alapértelmezett adatvédelem különösen fontos a közösségi hálózatépítő szolgáltatások összefüggésében, mivel a jogosulatlan hozzáférés kockázatán túl, amely a legtöbb adatkezelési típust érinti, a személyes adatok közösségi médiában való megosztása további biztonsági kockázatot jelent. Ezek gyakran az egyének ismereteinek hiányából fakadnak arra vonatkozóan, hogy *ki* férhet hozzá adataikhoz és azokat hogyan használhatják fel. A közösségi média elterjedt használatával a személyazonosság-lopások és az áldozatok száma emelkedett.

1024 *Uo.*, 34. cikk.

Példa: A személyazonosság-lopás egy olyan jelenség, amely során egy személy megszerzi egy másik személy (az áldozat) információit, adatait, iratait, és ezeket az információkat felhasználva az áldozatnak adja ki magát, hogy az áldozat nevében árukat és szolgáltatásokat szerezzen meg. Vegyük például Pault, aki egy közösségi média oldalán fiókkal rendelkezik. Paul tanár, és közösségének aktív tagja, nagyon társaság kedvelő, és nem különösebben aggódik a közösségi média fiókjának adatvédelmi beállításai miatt. Rengeteg ismerőse van, néha olyanokat is felvesz, akit személyesen nem ismer. Mivel egy nagy iskolában dolgozik, és nagyon népszerű az iskolai focicsapat edzőjeként, azt gondolja, hogy ezek az emberek nagy valószínűséggel szülők vagy az iskola barátai. Paul e-mail címe és születésnapja megjelenik a közösségi média fiókjában. Ráadásul Paul rendszeresen posztol fotókat a kutyájáról, Tobyról, olyan szöveggel, hogy „Toby és én a reggeli futásunkon". Paulban nem tudatosult, hogy az e-mail-címét és mobil telefonszámát védő egyik legnépszerűbb biztonsági kérdés az, hogy „mi a háziállatod neve". Paul közösségi média fiókjában lévő adatok felhasználásával Nick könnyedén fel tudja törni Paul fiókját.

Egyének jogai

A közösségi hálózatépítő szolgáltatóknak tiszteletben kell tartaniuk az egyének jogait (lásd a 6.1 szakaszt), beleértve a tájékoztatáshoz való jogot az adatkezelés célját illetően, valamint a személyes adatok közvetlen üzletszerzés céljából történő felhasználásának módjáról. Az egyéneknek továbbá biztosítani kell a jogot, hogy hozzáférjenek a közösségi hálózatépítő platformon létrehozott adataikhoz, és azok törlését kérjék. Még ha az egyének hozzá is járultak személyes adataik kezeléséhez és feltöltöttek információkat az internetre, képesnek kell lenniük az „elfeledtetésüket" kérni, ha többé nem kívánják igénybe venni a közösségi hálózat szolgáltatásait. Az adathordozhatósághoz való jog továbbá lehetővé teszi a felhasználó számára, hogy kérje a közösségi hálózatépítő szolgáltatónak megadott személyes adatai másolatát tagolt, széles körben használt, géppel olvasható formátumban, továbbá jogosult arra, hogy ezeket az adatokat egy másik közösségi hálózatépítő szolgáltatónak továbbítsa.[1025]

1025 *Uo.*, 21. cikk.

Adatkezelők

A közösségi médiával összefüggésben gyakran felmerülő és nehéz kérdés, hogy ki az adatkezelő, vagyis, ki az a személy, akinek eleget kell tennie az adatvédelmi szabályokban fogalt kötelezettségeknek és felelősségeknek. Az európai adatvédelmi jog értelmében a közösségi hálózatépítő szolgáltatók tekintendők adatkezelőknek. Ez nyilvánvaló, figyelemmel az „adatkezelő" tág értelemben vett meghatározására, és arra, hogy ezek a szolgáltatók határozzák meg az egyének által megosztott személyes adatok kezelésének célját és módját. Az uniós jog szerint, ha uniós érintetteknek nyújtanak szolgáltatást, az adatkezelők kötelesek eleget tenni az általános adatvédelmi rendelet előírásainak, még akkor is, ha székhelyük nem az EU-ban van.

A közösségi hálózatok felhasználói azért tekinthetők adatkezelőnek? Amennyiben az egyének „kizárólag személyes vagy otthoni tevékenység keretében" kezelnek személyes adatokat, az adatvédelmi szabályokat nem kell alkalmazni. Ez az európai adatvédelmi jogban „otthoni tevékenységre vonatkozó mentesítésként" ismert. Néhány esetben azonban előfordulhat, hogy a közösségi hálózatépítő szolgáltatás felhasználója nem tartozik az otthoni tevékenységre vonatkozó mentesítés hatálya alá.

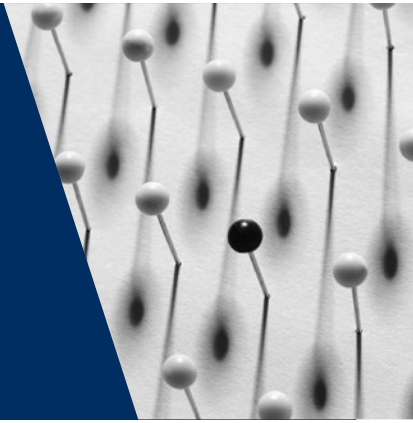
A felhasználók önként osztják meg személyes adataikat az interneten. Az online megosztott adatok azonban gyakran tartalmazzák más egyének személyes adatait is.

Példa: Paul egy nagyon népszerű közösségi hálózatépítő platformon rendelkezik fiókkal. Paul színész szeretne lenni, és fiókját arra használja, hogy a művészet iránti szenvedélyét magyarázó fotókat, videókat és posztokat tegyen közzé. Jövője szempontjából fontos a népszerűség, azért úgy döntött, hogy profilja ne csak a közeli ismerősei, hanem az internet valamennyi felhasználója számára elérhető legyen, függetlenül attól, hogy azok a hálózat tagjai-e. Paul posztolhat barátjával, Sarah-val közös fotókat és videókat Sarah hozzájárulása nélkül? Általános iskolai tanítóként Sarah igyekszik magánéletét távol tartani munkaadójától, diákjaitól és azok szüleitől. Képzeljünk el egy olyan helyzetet, ahol Sarah, aki nem használja a közösségi hálózatokat, egy közös barátjuktól, Nicktől megtudja, hogy egy partin róla és Paulról készült fotót posztoltak az interneten. Ebben az esetben Paul adatkezelése nem tartozik az uniós jog alá, mivel arra érvényes az „otthoni tevékenységre vonatkozó mentesítés".

Ugyanakkor továbbra is döntő fontosságú a felhasználók számára, hogy tisztában legyenek azzal, és figyelembe vegyék, hogy más egyénekre vonatkozó információk feltöltése azok hozzájárulása nélkül sértheti az illetők magánélethez és a személyes adatok védelméhez való jogait. Még azokban az esetekben is, amikor alkalmazható az otthoni tevékenységre vonatkozó mentesítés, például amikor egy felhasználó olyan profillal rendelkezik, amely csak az általa kiválasztott ismerősök számára elérhető, másokra vonatkozó személyes adatok közzététele a felhasználó felelősségét vonhatja maga után. Annak ellenére, hogy az adatvédelmi szabályok nem alkalmazandók az otthoni tevékenységre vonatkozó mentesítés esetén, egyéb nemzeti szabályok, például a rágalmazásra vagy a személyiség megsértésére vonatkozó szabályok felvethetik az illető felelősségét. Végezetül pedig csak a közösségi hálózatépítő szolgáltatások felhasználóit védi az otthoni tevékenységre vonatkozó mentesítés: az ilyen privát adatkezelés eszközét biztosító adatkezelők és adatfeldolgozók az uniós adatvédelmi jog hatálya alá tartoznak.[1026]

Az elektronikus hírközlési adatvédelmi irányelv reformjával a távközlési szolgáltatásokat nyújtókra a jelenlegi jogi keret alapján érvényes adatvédelmi és biztonsági szabályok a gépek közötti kommunikációra és az elektronikus hírközlési szolgáltatásokra is vonatkoznak, beleértve például az „over the top" szolgáltatásokat.

1026 *Uo.*, (18) preambulumbekezdés.



Irodalomjegyzék

1. fejezet

Araceli Mangas, M. (szerk.) (2008), *Carta de los derechos fundamentales de la Unión Europea*, Bilbao, Fundación BBVA.

Berka, W. (2012), *Das Grundrecht auf Datenschutz im Spannungsfeld zwischen Freiheit und Sicherheit*, Bécs, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C., „Four fundamental rights: finding the balance", *International Data Privacy Law*, 6. évf., 3. sz., 195–209. o.

EDRi, *An introduction to data protection*, Brüsszel.

Frowein, J. és Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. és Gellert, G. (2012), „The fundamental right of data protection in the European Union: in search of an uncharted right", *International Review of Law, Computers and Technology*, 26. évf, 1. sz., 73–82. o.

Grabenwarter, C. és Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwange, C. és Nouwt, S. (szerk.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. és Bates, E. (2009), *Law of the European Convention on Human Rights*, Oxford, Oxford University Press.

Hijmans, H. (2016), *The European Union as Guardian of Internet Privacy – the Story of Art 16 TFEU*, Springer.

Hustinx, P. (2016), *EU Data Protection Law: the review of Directive 95/46/EC and the Proposed General Data Protection Regulation.*

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

Kokott, J. és Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, 3. évf, 4. sz., 222–228. o.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, 1. évf., 1. sz., 70–79. o.

Lynskey, O. (2014), „Deconstructing data protection: the 'added-value' of a right to data protection in the EU legal order", *International and Comparative Law Quarterly*, 63. évf., 3. sz., 569–597. o.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oxford, Oxford University Press.

Mayer, J. (2011), *Charta der Grundrechte der Europäischen Union*, Baden-Baden, Nomos.

Mowbray, A. (2012), *Cases, materials, and commentary on the European Convention on Human Rights*, Oxford, Oxford University Press.

Nowak, M., Januszewski, K. és Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. és Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Brüsszel, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, 5. sz., 281–288. o.

Warren, S. és Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* 4. évf., 5. sz., 193–220. o.

White, R. és Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

2. fejezet

Acquisty, A. és Gross R. (2009), „Predicting Social Security numbers from public data", *Proceedings of the National Academy of Science*, 2009. július 7.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

De Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., és Blondel, V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility", *Nature Scientific Reports*, 3. évf, 2013.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Párizs, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

González Fuster, G. (2014), *The Emergence of Personal Data Protection as a Fundamental Right in the EU*, Springer.

Morgan, R. és Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, 57. évf., 6. sz., 1701–1777. o.

Samarati, P. és Sweeney, L. (1998), „Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppressio", Technical Report SRI-CSL-98-04.

Sweeney, L. (2002), „K-Anonymity: A Model for Protecting Privacy", *International Journal of Uncertainty, Fuzziness and Knowledge-based Systems*, 10. évf., 5. sz., 557–570. o.

Tinnefeld, M., Buchner, B. és Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice*.

3–6. fejezet

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr", in: Grabitz, E., Hilf, M. és Nettesheim, M. (szerk.), *Das Recht der Europäischen Union*, IV. kötet, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cádiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. és Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?", *Computer Law & Security Review*, 26. évf., 3. sz., 273–283. o.

Dammann, U. és Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. és Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, 22. évf., 6. sz., 1–5. o.

De Hert, P. és Papakonstantinou, V. (2012), „The proposed data protection Regulation replacing Directive 95/46/EC: A sound system for the protection of individuals", *Computer Law & Security Review*, 28. évf., 2. sz., 130–142. o.

Feretti, Federico (2012), „A European perspective on data processing consent through the re-conceptualization of European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, 20. évf., 2. sz., 473–506. o.

FRA (Az Európai Unió Alapjogi Ügynöksége) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxembourg, az Európai Unió Kiadóhivatala (Kiadóhivatal).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (konferencia-kiadás), Bécs, FRA.

FRA (2011), *Az igazságszolgáltatáshoz való hozzáférés Európában: a kihívások és lehetőségek áttekintése*, Luxembourg, Kiadóhivatal.

Irish Health Information and Quality Authority (2010), *Guidance on Privacy Impact Assessment in Health and Social Care*.

Kierkegaard, S., Waters, N., Greenleaf, G., Bygrave, L. A., Lloyd, I. és Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, 27. évf., 3. sz., 223–231. o.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

7. fejezet

Európai adatvédelmi biztos (2014), *Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies*.

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. és Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oxford, Oxford University Press.

29. cikk szerinti munkacsoport (2005), *Munkadokumentum a 95/46/EK irányelv 26. cikke (1) bekezdésének egységes értelmezéséről*.

8. fejezet

Blasi Casagran, C. (2016), *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, London, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level*, Berlin, Springer.

De Hert, P. és Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, 22. évf., 6. sz., 1–5. o.

Drewer, D. és Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, 13. évf., 3. sz., 381–395. o.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Hága, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxembourg, Kiadóhivatal.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. és Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. és De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, 36. évf., 5. sz., 722–776. o.

Santos Vara, J. (2013), *The role of the European Parliament in the conclusion of the Transatlantic Agreements on the transfer of personal data after Lisbon*, Centre for the Law of EU External Relations (CLEER), a CLEER 2013/2. sz. munkadokumentuma.

9. fejezet

Büllesbach, A., Gijrath, S., Poullet, Y. és Hacon, R. (2010), *Concise European IT law*, Amszterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. és Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. és Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. és De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem", *European Law Review*, 36. évf., 5. sz., 722–776. o.

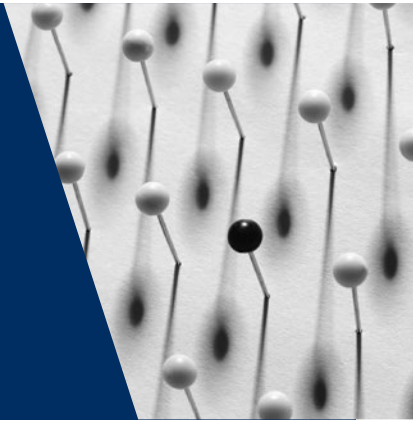
Rosemary, J. és Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

10. fejezet

El Emam, K. és Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, 5. évf., 1. sz., 73–87. o.

Mayer-Schönberger, V. és Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, 3. évf., 2. sz., 67–73. o.

Rubistein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, 3. évf., 2. sz., 74–87. o.



Ítélkezési gyakorlat

Az Emberi Jogok Európai Bíróságának válogatott jogesetei

Személyes adatokhoz való hozzáférés

Gaskin kontra Egyesült Királyság, 10454/83. sz. ügy, 1989. július 7.
Godelli kontra Olaszország, 33783/09. sz. ügy, 2012. szeptember 25.
K.H. és társai kontra Szlovákia, 32881/04. sz. ügy, 2009. április 28.
Leander kontra Svédország, 9248/81. sz. ügy, 1987. március 26.
M.K. kontra Franciaország, 19522/09. sz. ügy, 2013. április 18.
Odièvre kontra Franciaország [Nagykamara], 42326/98. sz. ügy, 2003. február 13.

Az adatvédelem és a véleménynyilvánítás szabadsága és az információhoz való jog közötti egyensúly megteremtése

Axel Springer AG kontra Németország [Nagykamara], 39954/08. sz. ügy, 2012. február 7.
Bohlen kontra Németország, 53495/09. sz. ügy, 2015. február 19.
Couderc és Hachette Filipacchi Associés kontra Franciaország [Nagykamara], 40454/07. sz. ügy, 2015. november 10.
Magyar Helsinki Bizottság kontra Magyarország [Nagykamara], 18030/11. sz. ügy, 2016. november 8.
Müller és társai kontra Svájc, 10737/84. sz. ügy, 1988. május 24.
Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország [Nagykamara], 931/13. sz. ügy, 2017. június 27.

Vereinigung bildender Künstler kontra Ausztria, 68354/01. sz. ügy, 2007. január 25.
Von Hannover kontra Németország (no. 2) [Nagykamara], 40660/08. és 60641/08. sz. ügyek, 2012. február 7.

Az adatvédelem és a vallásszabadság közötti egyensúly megteremtése
Sinan Işık kontra Törökország, 21924/05. sz. ügy, 2010. február 2.

Kihívások az online adatvédelem terén
K.U. kontra Finnország, 2872/02. sz. ügy, 2008. december 2.

Az érintett hozzájárulása
Elberte kontra Lettország, 61243/08. sz. ügy, 2015. január 13.
Sinan Işık kontra Törökország, 21924/05. sz. ügy, 2010. február 2.
Y kontra Törökország, 648/10. sz. ügy, 2015. február 17.

Kapcsolattartás
Amann kontra Svájc [Nagykamara], 27798/95. sz. ügy, 2000. február 16.
Association for European Integration and Human Rights és Ekimdzhiev kontra Bulgária, 62540/00. sz. ügy, 2007. június 28.
Bernh Larsen Holding AS és társai kontra Norvégia, 24117/08. sz. ügy, 2013. március 14.
Cemalettin Canli kontra Törökország, 22427/04. sz. ügy, 2008. november 18.
D.L. kontra Bulgária, 7472/14. sz. ügy, 2016. május 19.
Dalea kontra Franciaország, 964/07. sz. ügy, 2010. február 2.
Gaskin kontra Egyesült Királyság, 10454/83. sz. ügy, 1989. július 7.
Haralambie kontra Románia, 21737/03. sz. ügy, 2009. október 27.
Khelili kontra Svájc, 16188/07. sz. ügy, 2011. október 18.
Leander kontra Svédország, 9248/81. sz. ügy, 1987. március 26.
Malone kontra Egyesült Királyság, 8691/79. sz. ügy, 1984. augusztus 2.
Rotaru kontra Románia [Nagykamara], 28341/95. sz. ügy, 2000. május 4.
S. és Marper kontra Egyesült Királyság [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4.
Shimovolos kontra Oroszország, 30194/09. sz. ügy, 2011. június 21.
Silver és társai kontra Egyesült Királyság, 5947/72., 6205/73., 7052/75., 7061/75., 7107/75., 7113/75. sz. ügyek, 1983. március 25.
The Sunday Times kontra Egyesült Királyság, 6538/74. sz. ügy, 1979. április 26.

Bűnügyi nyilvántartási adatbázisok
Aycaguer kontra Franciaország, 8806/12. sz. ügy, 2017. június 22.
B.B. kontra Franciaország, 5335/06. sz. ügy, 2009. december 17.
Brunet kontra Franciaország, 21010/10. sz. ügy, 2014. szeptember 18.
M.K. kontra Franciaország, 19522/09. sz. ügy, 2013. április 18.
M.M. kontra Egyesült Királyság, 24029/07. sz. ügy, 2012. november 13.

Adatbiztonság
Haralambie kontra Románia, 21737/03. sz. ügy, 2009. október 27.
K.H. és társai kontra Szlovákia, 32881/04. sz. ügy, 2009. április 28.

DNS-adatbázisok
S. és Marper kontra Egyesült Királyság [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4.

GPS-adatok
Uzun kontra Németország, 35623/05. sz. ügy, 2010. szeptember 2.

Egészségügyi adatok
Avilkina és társai kontra Oroszország, 1585/09. sz. ügy, 2013. június 6.
Biriuk kontra Litvánia, 23373/03. sz. ügy, 2008. november 25.
I. kontra Finnország, 20511/03. sz. ügy, 2008. július 17.
L.H. kontra Lettország, 52019/07. sz. ügy, 2014. április 29.
L.L. kontra Franciaország, 7508/02. sz. ügy, 2006. október 10.
M.S. kontra Svédország, 20837/92. sz. ügy, 1997. augusztus 27.
Szuluk kontra Egyesült Királyság, 36936/05. sz. ügy, 2009. június 2.
Y kontra Törökország, 648/10. sz. ügy, 2015. február 17.
Z kontra Finnország, 22009/93. sz. ügy, 1997. február 25.

Személyazonosság
Ciubotaru kontra Moldova, 27138/04. sz. ügy, 2010. április 27.
Godelli kontra Olaszország, 33783/09. sz. ügy, 2012. szeptember 25.
Odièvre kontra Franciaország [Nagykamara], 42326/98. sz. ügy, 2003. február 13.

Szakmai tevékenységgel kapcsolatos információk
G.S.B. kontra Svájc, 28601/11. sz. ügy, 2015. december 22.

M.N. és társai kontra San Marino, 28005/12. sz. ügy, 2015. július 7.
Michaud kontra Franciaország, 12323/11. sz. ügy, 2012. december 6.
Niemietz kontra Németország, 13710/88. sz. ügy, 1992. december 16.

Beszélgetések lehallgatása
Amann kontra Svájc [Nagykamara], 27798/95. sz. ügy, 2000. február 16.
Brito Ferrinho Bexiga Villa-Nova kontra Portugália, 69436/10. sz. ügy, 2015. december 1.
Copland kontra Egyesült Királyság, 62617/00. sz. ügy, 2007. április 3.
Halford kontra Egyesült Királyság, 20605/92. sz. ügy, 1997. június 25.
Iordachi és társai kontra Moldova, 25198/02. sz. ügy, 2009. február 10.
Kopp kontra Svájc, 23224/94. sz. ügy, 1998. március 25.
Liberty és társai kontra Egyesült Királyság, 58243/00. sz. ügy, 2008. július 1.
Malone kontra Egyesült Királyság, 8691/79. sz. ügy, 1984. augusztus 2.
Mustafa Sezgin Tanrıkulu kontra Törökország, 27473/06. sz. ügy, 2017. július 18.
Pruteanu kontra Románia, 30181/05. sz. ügy, 2015. február 3.
Szuluk kontra Egyesült Királyság, 36936/05. sz. ügy, 2009. június 2.

A jogalanyok kötelezettségei
B.B. kontra Franciaország, 5335/06. sz. ügy, 2009. december 17.
I. kontra Finnország, 20511/03. sz. ügy, 2008. július 17.
Mosley kontra Egyesült Királyság, 48009/08. sz. ügy, 2011. május 10.

Személyes adatok
Amann kontra Svájc [Nagykamara], 27798/95. sz. ügy, 2000. február 16.
Bernh Larsen Holding AS és társai kontra Norvégia, 24117/08. sz. ügy, 2013. március 14.
Uzun kontra Németország, 35623/05. sz. ügy, 2010. szeptember 2.

Fényképek
Sciacca kontra Olaszország, 50774/99. sz. ügy, 2005. január 11.
Von Hannover kontra Németország, 59320/00. sz. ügy, 2004. június 24.

Az elfeledtetéshez való jog
Satakunnan Markkinapörssi Oy és Satamedia Oy kontra Finnország [Nagykamara], 931/13. sz. ügy, 2017. június 27.
Segerstedt-Wiberg és társai kontra Svédország, 62332/00. sz. ügy, 2006. június 6.

A tiltakozáshoz való jog
Leander kontra Svédország, 9248/81. sz. ügy, 1987. március 26.
M.S. kontra Svédország, 20837/92. sz. ügy, 1997. augusztus 27.
Mosley kontra Egyesült Királyság, 48009/08. sz. ügy, 2011. május 10.
Rotaru kontra Románia [Nagykamara], 28341/95. sz. ügy, 2000. május 4.
Sinan Işık kontra Törökország, 21924/05. sz. ügy, 2010. február 2.

Az adatok érzékeny kategóriái
Brunet kontra Franciaország, 21010/10. sz. ügy, 2014. szeptember 18.
I. kontra Finnország, 20511/03. sz. ügy, 2008. július 17.
Michaud kontra Franciaország, 12323/11. sz. ügy, 2012. december 6.
S. és Marper kontra Egyesült Királyság [Nagykamara], 30562/04. és 30566/04. sz. ügyek, 2008. december 4.

Felügyelet és az előírások betartatása (a különböző szereplők, köztük a felügyeleti hatóságok szerepe)

I. kontra Finnország, 20511/03. sz. ügy, 2008. július 17.
K.U. kontra Finnország, 2872/02. sz. ügy, 2008. december 2.
Von Hannover kontra Németország, 59320/00. sz. ügy, 2004. június 24.
Von Hannover kontra Németország (no. 2) [Nagykamara], 40660/08. és 60641/08. sz. ügyek, 2012. február 7.

Felügyeleti módszerek
Allan kontra Egyesült Királyság, 48539/99. sz. ügy, 2002. november 5.
Association for European Integration and Human Rights és Ekimdzhiev kontra Bulgária, 62540/00. sz. ügy, 2007. június 28.
Bărbulescu kontra Románia [Nagykamara], 61496/08. sz. ügy, 2017. szeptember 5.
D.L. kontra Bulgária, 7472/14. sz. ügy, 2016. május 19.
Dragojević kontra Horvátország, 68955/11. sz. ügy, 2015. január 15.
Karabeyoğlu kontra Törökország, 30083/10. sz. ügy, 2016. június 7.
Klass és társai kontra Németország, 5029/71. sz. ügy, 1978. szeptember 6.
Roman Zakharov kontra Oroszország [Nagykamara], 47143/06. sz. ügy, 2015. december 4.
Rotaru kontra Románia [Nagykamara], 28341/95. sz. ügy, 2000. május 4.
Szabó és Vissy kontra Magyarország, 37138/14. sz. ügy, 2016. január 12.
Taylor-Sabori kontra Egyesült Királyság, 47114/99. sz. ügy, 2002. október 22.
Uzun kontra Németország, 35623/05. sz. ügy, 2010. szeptember 2.

Versini-Campinchi és Crasnianski kontra Franciaország, 49176/11. sz. ügy, 2016. június 16.
Vetter kontra Franciaország, 59842/00. sz. ügy, 2005. május 31.
Vukota-Bojić kontra Svájc, 61838/10. sz. ügy, 2016. október 18.

Videokamerás megfigyelés
Köpke kontra Németország, 420/07. sz. ügy, 2010. október 5.
Peck kontra Egyesült Királyság, 44647/98. sz. ügy, 2003. január 28.

Hangminták
P.G. és J.H. kontra Egyesült Királyság, 44787/98. sz. ügy, 2001. szeptember 25.
Wisse kontra Franciaország, 71611/01. sz. ügy, 2005. december 20.

Az Európai Unió Bíróságának válogatott jogesetei

Az adatvédelmi irányelvvel kapcsolatos ítélkezési gyakorlat

Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) és Federación de Comercio Electrónico y Marketing Directo (FECEMD) kontra Administración del Estado, C-468/10. és C-469/10. sz. egyesített ügyek, 2011. november 24.

[Az adatvédelmi irányelv 7. cikke f) pontjának – „mások jogszerű érdekei" – megfelelő átültetése a nemzeti jogba]

Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) kontra Netlog NV, C-360/10. sz. ügy, 2012. február 16.

[Közösségihálózat-szolgáltatók azon kötelezettsége, hogy megakadályozzák zeneművek és audiovizuális művek hálózatfelhasználók általi jogellenes használatát]

Bodil Lindqvist elleni büntetőeljárás, C-101/01. sz. ügy, 2003. november 6.

[Személyes adatok különleges kategóriái]

Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce kontra Salvatore Manni, C-398/15. sz. ügy, 2017. március 9.

[A személyes adatok törléséhez való jog; az adatkezelés elleni tiltakozáshoz való jog]

College van burgemeester en wethouders van Rotterdam kontra M.E.E. Rijkeboer, C-553/07. sz. ügy, 2009. május 7.

[Az érintett hozzáférési joga]

Deutsche Telekom AG kontra Bundesrepublik Deutschland, C-543/09. sz. ügy, 2011. május 5.

[Újabb hozzájárulás szükségessége]

Digital Rights Ireland Ltd kontra Minister for Communications, Marine and Natural Resources és társai, valamint *Kärntner Landesregierung és társai* [nagytanács], C-293/12. és C-594/12. sz. egyesített ügyek, 2014. április 8.

[Az elsődleges uniós jog megsértése az adatmegőrzési irányelv által; jogszerű adatkezelés; célhoz kötöttség és korlátozott tárolhatóság]

Európai Bizottság kontra Magyarország [nagytanács], C-288/12. sz. ügy, 2014. április 8.
[A nemzeti adatvédelmi biztos hivatalból való felmentésének jogszerűsége]

Európai Bizottság kontra Németországi Szövetségi Köztársaság [nagytanács], C-518/07. sz. ügy, 2010. március 9.
[Egy nemzeti felügyeleti hatóság függetlensége]

Európai Bizottság kontra Osztrák Köztársaság [nagytanács], C-614/10. sz. ügy, 2012. október 16.
[Egy nemzeti felügyeleti hatóság függetlensége]

František Ryneš kontra Úřad pro ochranu osobních údajů, C-212/13. sz. ügy, 2014. december 11.
[Az „adatkezelés" és az „adatkezelő" fogalma]

Google Spain SL és Google Inc. kontra Agencia Española de Protección de Datos (AEPD) és Mario Costeja González [nagytanács], C-131/12. sz. ügy, 2014. május 13.
[A keresőmotorok üzemeltetőjének kötelezettsége, hogy az érintett kérésére a személyes adatok ne jelenjenek meg a találati eredmények között; az adatvédelmi irányelv alkalmazhatósága; az „adatkezelés" fogalma; az „adatkezelő" jelentése; megfelelő egyensúly megteremtése az adatvédelem és a véleménynyilvánítás szabadsága között; az elfeledtetéshez való jog]

Heinz Huber kontra Bundesrepublik Deutschland [nagytanács], C-524/06. sz. ügy, 2008. december 16.
[Külföldiekre vonatkozó adatok statisztikai nyilvántartásban való tárolásának jogszerűsége]

Institut professionnel des agents immobiliers (IPI) kontra Geoffrey Englebert és társai, C-473/12. sz. ügy, 2013. november 7.
[A személyes adatok kezeléséről történő tájékoztatáshoz való jog]

Maximillian Schrems kontra Data Protection Commissioner [nagytanács], C-362/14. sz. ügy, 2015. október 6.
[A jogszerű adatkezelés elve; alapvető jogok; a biztonságos kikötőről szóló határozat érvénytelenítése; a független felügyeleti hatóságok hatásköre]

Michael Schwarz kontra Stadt Bochum, C-291/12. sz. ügy, 2013. október 17.

[Hivatkozás az előzetes döntéshozatalra; a szabadságon, a biztonságon és a jog érvényesülésén alapuló térség; biometrikus útlevél; ujjlenyomatok; jogalap; arányosság]

Patrick Breyer kontra Bundesrepublik Deutschland, C-582/14. sz. ügy, 2016. október 19.

[A „személyes adat" definíciója; internetprotokoll-címek; adatok tárolása online médiaszolgáltató által; az adatkezelő jogos érdekének figyelembevételét nem engedélyező nemzeti szabályozás]

Peter Nowak kontra Data Protection Commissioner, C-434/16. sz. ügy, Kokott főtanácsnok indítványa, 2017. július 20.

[A „személyes adat" fogalma; hozzáférés a saját vizsgadolgozathoz; javítói megjegyzések]

Pilkington Group Ltd kontra Európai Bizottság, T-462/12. R. sz. ügy, a Törvényszék elnökének végzése, 2013. március 11.

Productores de Música de España (Promusicae) kontra Telefónica de España SAU [nagytanács], C-275/06. sz. ügy, 2008. január 29.

[A „személyes adat" fogalma; internetszolgáltatók azon kötelezettsége, hogy a szellemi tulajdon védelmével foglalkozó szervezetekkel közöljék a KaZaA fájlcserélő program felhasználóinak kilétét]

Rechnungshof kontra Österreichischer Rundfunk és társai, valamint *Christa Neukomm és Joseph Lauermann kontra Österreichischer Rundfunk*, C-465/00., C-138/01. és C-139/01. sz. egyesített ügyek, 2003. május 20.

[A bizonyos kategóriákba tartozó közszférabeli intézmények alkalmazottainak fizetésére vonatkozó személyes adatok közzétételére vonatkozó jogszabályi kötelezettség arányossága]

Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10. sz. ügy, 2011. november 24.

[Információs társadalom; szerzői jog; internet; „peer-to-peer" szoftverek; internetszolgáltatók; elektronikus közléseket szűrő rendszer telepítése a szerzői jogokat sértő fájlmegosztások megakadályozására; a továbbított adatok ellenőrzésére vonatkozó általános kötelezettség hiánya]

Smaranda Bara és társai kontra Casa Națională de Asigurări de Sănătate és társai, C-201/14. sz. ügy, 2015. október 1.

[A személyes adatok kezeléséről történő tájékoztatáshoz való jog]

Tele2 Sverige AB kontra Post- och telestryrelsen és *Secretary of State for the Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016. december 21.

[Az elektronikus közlések titkossága; elektronikus hírközlési szolgáltatók; a forgalmi és a helymeghatározó adatok általános és különbségtétel nélküli megőrzésére vonatkozó kötelezettség; bíróság vagy független közigazgatási szerv előzetes felülvizsgálatának hiánya; az Európai Unió Alapjogi Chartája; az uniós joggal való összeegyeztethetőség]

Tietosuojavaltuutettu kontra Satakunnan Markkinapörssi Oy és Satamedia Oy [nagytanács], C-73/07. sz. ügy, 2008. december 16.

[Az adatvédelmi irányelv 9. cikke értelmében vett „újságírói tevékenység" fogalma]

Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde kontra Rīgas pašvaldības SIA „Rīgas satiksme", C-13/16. sz. ügy, 2017. május 4.

[A jogszerű adatkezelés elve: harmadik fél jogos érdekének érvényesítése]

Volker und Markus Schecke GbR és Hartmut Eifert kontra Land Hessen [nagytanács], C-92/09. és C-93/09. sz. egyesített ügyek, 2010. november 9.

[A „személyes adat" fogalma; az egyes uniós mezőgazdasági alapok kedvezményezettjei személyes adatainak közzétételére vonatkozó jogszabályi kötelezettség arányossága]

Weltimmo s. r. o. kontra Nemzeti Adatvédelmi és Információszabadság Hatóság, C-230/14. sz. ügy, 2015. október 1.

[A nemzeti felügyeleti hatóságok hatásköre]

Worten – Equipamentos para o Lar SA kontra Autoridade para as Condições de Trabalho (ACT), C-342/12. sz. ügy, 2013. május 30.

[A „személyes adat" fogalma; munkaidő-nyilvántartás; az adatminőséghez kapcsolódó elvek, és a jogszerű adatkezelés kritériumai; a munkafeltételek ellenőrzéséért felelős nemzeti hatóság általi hozzáférés; a munkáltató kötelezettsége, hogy rendelkezésre bocsássa a munkaidő-nyilvántartást, azonnali betekintést lehetővé téve]

YS kontra Minister voor Immigratie, Integratie en Asiel és *Minister voor Immigratie, Integratie en Asiel kontra M és S*, C-141/12. és C-372/12. sz. egyesített ügyek, 2014. július 17.

[Az érintett hozzáférési jogának terjedelme; az egyének védelme a személyes adatok kezelése tekintetében; a „személyes adat" fogalma; határozattervezethez kapcsolódó közigazgatási dokumentumban szereplő, tartózkodási engedélyt kérelmezőre vonatkozó adatok és jogi elemzés; az Európai Unió Alapjogi Chartája]

A 2016/681 irányelvvel kapcsolatos ítélkezési gyakorlat

A Bíróság 1/15. sz. véleménye [nagytanács], 2017. július 26.

[Jogalap; Kanada és az Európai Unió közötti megállapodástervezet az utasnyilvántartási adatállomány továbbításáról és kezeléséről; a megállapodástervezet összeegyeztethetősége az EUMSZ 16. cikkel, valamint az Európai Unió Alapjogi Chartájának 7., 8. cikkével és az 52. cikk (1) bekezdésével]

Az uniós intézmények adatvédelmi rendeletével kapcsolatos ítélkezési gyakorlat

ClientEarth, Pesticide Action Network Europe (PAN Europe) kontra Európai Élelmiszerbiztonsági Hatóság (EFSA), Európai Bizottság, C-615/13. P. sz. ügy, 2015. július 16.

[A dokumentumokhoz való hozzáférés]

Európai Bizottság kontra The Bavarian Lager Co. Ltd. [nagytanács], C-28/08. P. sz. ügy, 2010. június 29.

[A dokumentumokhoz való hozzáférés]

A 2002/58/EK irányelvvel kapcsolatos ítélkezési gyakorlat

Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB kontra Perfect Communication Sweden AB, C-461/10. sz. ügy, 2012. április 19.

[Szerzői jog és szomszédos jogok; internetes adatfeldolgozás; kizárólagos jog megsértése; az internetszolgáltató által biztosított IP-címről FTP-szerver segítségével az interneten hozzáférhetővé tett hangoskönyvek; az IP-címet használó személy nevének és címének közlése céljából az internetszolgáltatóhoz intézett meghagyás]

Scarlet Extended SA kontra Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10. sz. ügy, 2011. november 24.

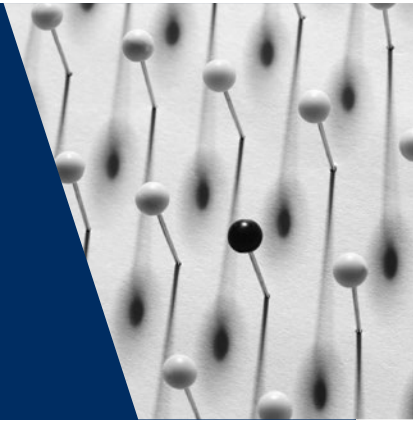
[Információs társadalom; szerzői jog; internet; „peer-to-peer" szoftverek; internetszolgáltatók; elektronikus közléseket szűrő rendszer telepítése a szerzői jogokat sértő fájlmegosztások megakadályozására; a továbbított adatok ellenőrzésére vonatkozó általános kötelezettség hiánya]

Tele2 (Netherlands) BV és társai kontra Autoriteit Consument en Markt (AMC), C-536/15. sz. ügy, 2017. március 15.

[A hátrányos megkülönböztetés tilalmának elve; az előfizetők személyes adatainak a nyilvános tudakozószolgálatok és telefonkönyvek szolgáltatása céljából történő rendelkezésre bocsátása; az előfizető hozzájárulása; megkülönböztetés azon tagállam szerint, amelyben a nyilvános tudakozószolgálatok és telefonkönyv szolgáltatását nyújtják]

Tele2 Sverige AB kontra Post- och telestyrelsen és *Secretary of State for the Home Department kontra Tom Watson és társai* [nagytanács], C-203/15. és C-698/15. sz. egyesített ügyek, 2016. december 21.

[Az elektronikus közlések titkossága; elektronikus hírközlési szolgáltatók; a forgalmi és a helymeghatározó adatok általános és különbségtétel nélküli megőrzésére vonatkozó kötelezettség; bíróság vagy független közigazgatási szerv előzetes felülvizsgálatának hiánya; az Európai Unió Alapjogi Chartája; az uniós joggal való összeegyeztethetőség]



Tárgymutató

Az Európai Unió Bíróságának ítélkezési gyakorlata

Az Emberi Jogok Európai Bíróságának ítélkezési gyakorlata

A nemzeti bíróságok esetjoga

Az Európai Unió Alapjogi Ügynökségéről további információ olvasható az interneten. Ez az FRA weboldaláról érhető el: https://fra.europa.eu/en.

Az Európai Emberi Jogi Bíróság joggyakorlatával kapcsolatban további információ található a Bíróság honlapján: echr.coe.int. A HUDOC keresőportál révén hozzáférhetők az ítéletek és határozatok angolul, ill. franciául, egyes esetekben azok fordításai más nyelvekre, esetjogi tájékoztatók, sajtóközlemények, valamint a Bíróság munkájával kapcsolatos egyéb tudnivalók (http://HUDOC.echr.coe.int).

Az Európa Tanács publikációihoz való hozzáférés

Az Európa Tanács kiadója a szervezet valamennyi munkaterületével – emberi jogok, jogtudomány, egészségügy, etika, szociális kérdések, környezet, oktatás, kultúra, sport, ifjúság, építészeti örökség – kapcsolatban közzétesz műveket. A könyvek és az elektronikus kiadványok katalógus alapján interneten megrendelhetők: https://book.coe.int/en/.

A virtuális olvasószoba révén az érdeklődők ingyenesen ismerhetik meg a lényegesebb újonnan publikált művek részleteit, ill. egyes hivatalos anyagok teljes szövegét.

Az Európa Tanács egyezményeinek teljes szövege, ill. az azokra vonatkozó tudnivalók a Treaty Office honlapján érhetők el: http://conventions.coe.int/.

Kapcsolatba szeretne lépni az EU-val?

Személyesen

Az Európai Unió területén több Europe Direct információs központ is működik. Keresse meg az Önhöz legközelebb eső központot: https://europa.eu/european-union/contact_hu

Telefonon vagy e-mailben

A Europe Direct központok feladata, hogy megválaszolják a polgárok Európai Unióval kapcsolatos kérdéseit. Vegye igénybe a szolgáltatást

— az ingyenesen hívható telefonszámon: 00 800 6 7 8 9 10 11 (bizonyos szolgáltatók számíthatnak fel díjat a hívásért),
— a rendes díjszabású telefonszámon: (+32 2) 29-99-696, vagy
— e-mailen: https://europa.eu/european-union/contact_hu

Információkat keres az EU-ról?

Online

Az EUROPA portál tájékoztatással szolgál az Európai Unióról az EU összes hivatalos nyelvén: https://europa.eu/european-union/index_hu

Uniós kiadványok

A következő címen uniós kiadványok tölthetők le/rendelhetők meg díjmentesen/fizetés ellenében: https://publications.europa.eu/hu/publications. Ha bizonyos ingyenes kiadványokból több példányra van szüksége, rendeljen a Europe Direct központtól vagy hazájának helyi információs központjától (lásd: https://europa.eu/european-union/contact_hu).

Uniós jogszabályok és kapcsolódó dokumentumok

Az EUR-Lex portálról bármelyik hivatalos nyelven letölthetők az EU jogi tartalmai és az 1952-től megjelenő jogszabályai: http://eur-lex.europa.eu/

Az EU által gondozott nyílt hozzáférésű adatok

A nyílt hozzáférésű adatok európai uniós portálja (http://data.europa.eu/euodp/hu) uniós adatkészletekhez biztosít hozzáférést. Az adatok kereskedelmi és nem kereskedelmi célból egyaránt díjmentesen letölthetők és felhasználhatók.

doi:10.2811/55214 TK-05-17-225-HU-N

FRA
EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS

EUROPEAN COURT OF HUMAN RIGHTS
COUR EUROPÉENNE DES DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

EDPS

Az információs technológiák gyors fejlődésével egyre nagyobb szükség van a személyes adatok erőteljes védelmére, amely jogot az Európai Unió és az Európa Tanács jogi eszközei egyaránt biztosítják. A technológiai fejlesztések kiterjesztik például a felügyelet, a beszélgetések lehallgatása és az adatok tárolása határait, ami új és hatalmas kihívásokat állít e jog biztosítása elé. Ez a kézikönyv azon gyakorló jogászok számára készült, akiknek a jog e fejlődő területe nem a szakterülete. Áttekintést nyújt az EU és az Európa Tanács alkalmazandó jogi keretéről. Kifejti továbbá az ítélkezési gyakorlatot, és összefoglalja az Európai Unió Bírósága és az Emberi Jogok Európai Bírósága legfontosabb ítéleteit. Ezenkívül hipotetikus esetekkel illusztrált gyakorlati példákat mutat be, amelyek e folyton fejlődő területen felmerülő különféle kérdéseket járnak körül.

FRA – AZ EURÓPAI UNIÓ ALAPJOGI ÜGYNÖKSÉGE
Schwarzenbergplatz 11 – 1040 Bécs – Ausztria
Tel. +43 (1) 580 30-0 – Fax +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
@EURightsAgency

EMBERI JOGOK EURÓPAI BÍRÓSÁGA
EURÓPA TANÁCS
67075 Strasbourg Cedex – Franciaország
Tel. +33 (0) 3 88 41 20 18 – Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

EURÓPAI ADATVÉDELMI BIZTOS
Rue Wiertz 60 – 1047 Brüsszel – Belgium
Tel. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

ISBN 978-92-871-9830-3 (ET)
ISBN 978-92-9474-290-2 (FRA)

Az Európai Unió Kiadóhivatala