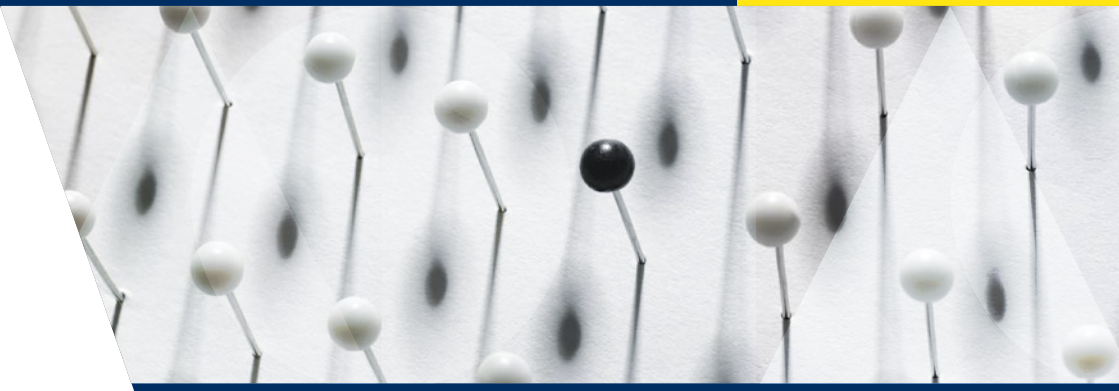
KÄSIKIRJA



Käsikirja Euroopan tietosuojaoikeudesta

vuoden 2018 painos

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

Tämän käsikirjan teksti saatiin valmiiksi huhtikuussa 2018.

Päivitettyjä versioita on myöhemmin saatavilla Euroopan unionin perusoikeusviraston verkkosivustolla osoitteessa fra.europa.eu, Euroopan neuvoston verkkosivustolla osoitteessa coe.int/dataprotection, Euroopan ihmisoikeustuomioistuimen verkkosivustolla oikeuskäytännön kohdalla osoitteessa echr.coe.int ja Euroopan tietosuojavaltuutetun verkkosivustolla osoitteessa edps.europa.eu.

Valokuvat (kansi & sisäpuolella): © iStockphoto

Luxemburg: Euroopan unionin julkaisutoimisto, 2021

Euroopan neuvosto:	ISBN 978-92-871-9832-7		
FRA – print:	ISBN 978-92-9474-789-1	doi:10.2811/23555	TK-05-17-225-FI-C
FRA – PDF:	ISBN 978-92-9474-792-1	doi:10.2811/128160	TK-05-17-225-FI-N

Tämä käsikirja on laadittu englanniksi. Euroopan neuvosto ja Euroopan ihmisoikeustuomioistuin (EIT) eivät vastaa kielitoisintojen laadusta. Tässä käsikirjassa esitetyt mielipiteet eivät sido Euroopan neuvostoa ja Euroopan ihmisoikeustuomioistuinta. Käsikirjassa viitataan erilaisiin lainselitysteoksiin ja käsikirjoihin. Euroopan neuvosto ja EIT eivät vastaa näiden julkaisujen sisällöstä, eivätkä ne välttämättä edusta Euroopan neuvoston ja EIT:n kantoja, vaikka ne on sisällytetty kirjallisuusluetteloon. EIT:n kirjaston verkkosivuilla osoitteessa echr.coe.int/library on lueteltu lisää julkaisuja.

Käsikirja Euroopan tietosuojaoikeudesta

vuoden 2018 painos

Esipuhe

Yhteiskuntiemme digitalisaatio lisääntyy jatkuvasti. Teknisen kehityksen tahti ja henkilötietojen käsittelytapa vaikuttavat meihin kaikkiin joka päivä ja monenlaisilla tavoilla näiden muutosten vuoksi. Yksityisyyden ja henkilötietojen suojan takaavia Euroopan unionin (EU) ja Euroopan neuvoston oikeudellisia kehyksiä on tarkistettu äskettäin.

Eurooppa on tietosuojan eturintamassa koko maailmassa. EU:n tietosuojastandardit perustuvat Euroopan neuvoston yleissopimukseen 108, EU:n säädöksiin, muun muassa yleiseen tietosuoja-asetukseen ja poliisi- ja rikosoikeusviranomaisia koskevaan tietosuojadirektiiviin, sekä Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytäntöihin.

EU:n ja Euroopan neuvoston tekemät tietosuojauudistukset ovat kattavia ja toisinaan monimutkaisia. Niiden vaikutukset ihmisiin ja yrityksiin sekä näiden uudistuksista saamat hyödyt ovat kauaskantoisia. Tämän käsikirjan tavoitteena on lisätä tietoa tietosuojasäännöistä ja parantaa niiden tuntemusta. Se on suunnattu erityisesti oikeusalan toimijoille, jotka eivät ole erikoistuneet tietosuojaan mutta joiden on käsiteltävä tietosuojakysymyksiä työssään.

Käsikirjan ovat laatineet Euroopan unionin perusoikeusvirasto (FRA), Euroopan neuvosto (yhdessä Euroopan ihmisoikeustuomioistuimen kirjaamon kanssa) ja Euroopan tietosuojavaltuutettu. Sillä saatetaan vuoden 2014 painos ajan tasalle, ja se kuuluu perusoikeusviraston ja Euroopan neuvoston yhdessä laatimien oikeudellisten käsikirjojen sarjaan.

Kiitämme Belgian, Georgian, Irlannin, Italian, Monacon, Ranskan, Sveitsin, Unkarin, Viron ja Yhdistyneen kuningaskunnan tietosuojaviranomaisia hyödyllisestä palautteesta käsikirjan laatimisessa. Olemme kiitollisia myös Euroopan komission tietosuojayksikölle ja sen kansainvälisten tietovirtojen ja tietosuojan yksikölle. Kiitämme Euroopan unionin tuomioistuinta asiakirjatuesta käsikirjan valmisteluvaiheessa.

Christos Giakoumopoulos

Euroopan neuvoston ihmisoikeuksia ja oikeusvaltiota käsittelevän osaston pääjohtaja

Giovanni Buttarelli

Euroopan tietosuojavaltuutettu

Michael O'Flaherty

Euroopan unionin perusoikeusviraston johtaja

Sisältö

Lyhenteet

BCR	Yritystä koskevat sitovat tietosuojasäännöt (Binding Corporate Rule)
CCTV	Kameravalvonta (Closed Circuit Television)
CETS	Euroopan neuvoston sopimussarja (Council of Europe Treaty Series)
CRM	Asiakashallintajärjestelmä (Customer relations management)
C-SIS	Schengenin keskustietojärjestelmä
DPA	Tietosuojaviranomainen
DPO	Tietosuojavastaava
EAW	Eurooppalainen pidätysmääräys (European arrest warrant)
EDPB	Euroopan tietosuojaneuvosto
EDPS	Euroopan tietosuojavaltuutettu
EFSA	Euroopan elintarviketurvallisuusviranomainen
EFTA	Euroopan vapaakauppaliitto
EIS	Euroopan ihmisoikeussopimus
EIT	Euroopan ihmisoikeustuomioistuin
EN	Euroopan neuvosto
ENISA	Euroopan unionin verkko- ja tietoturvavirasto
ENU	Europolin kansallinen yksikkö
EPPO	Euroopan syyttäjänvirasto
ESMA	Euroopan arvopaperimarkkinaviranomainen
ETA	Euroopan talousalue
eTEN	Euroopan laajuiset televerkot
EU	Euroopan unioni
eu-LISA	Vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava Euroopan unionin virasto (Tietotekniikkavirasto)
EuroPriSe	Eurooppalainen yksityisyyden suojaa koskeva tunnus (European Privacy Seal)
EUT	Euroopan unionin tuomioistuin (ennen joulukuuta 2009 Euroopan yhteisöjen tuomioistuin)

EUVL	Euroopan unionin virallinen lehti
EY	Euroopan yhteisö
FRA	Euroopan unionin perusoikeusvirasto
GDPR	Yleinen tietosuoja-asetus
GPS	Maailmanlaajuinen paikantamisjärjestelmä
ISP	Internetyhteyden tarjoaja
KP-sopimus	Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus
NGO	Kansalaisjärjestö (Non-governmental organisation)
N-SIS	Schengenin tietojärjestelmän kansallinen osa
OECD	Taloudellisen yhteistyön ja kehityksen järjestö
Perusoikeuskirja	Euroopan unionin perusoikeuskirja
PIN	Henkilökohtainen tunnusluku
PNR	Matkustajarekisteri
SCG	Valvonnan koordinointiryhmä
SEPA	Yhtenäinen euromaksualue
SEU-sopimus	Sopimus Euroopan unionista
SEUT-sopimus	Sopimus Euroopan unionin toiminnasta
SIS	Schengenin tietojärjestelmä
SWIFT	Kansainvälinen maksuliikennejärjestö
TTJ	Tullitietojärjestelmä
TVT	Tieto- ja viestintätekniikka
UDHR	Ihmisoikeuksien yleismaailmallinen julistus
VIS	Viisumitietojärjestelmä
YK	Yhdistyneet kansakunnat
Yleissopimus 108	Yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (Euroopan neuvosto). Euroopan neuvoston ministerikomitea hyväksyi yleissopimuksen 108 muutospöytäkirjan (CETS, nro 223), jäljempänä 'uudistettu yleissopimus 108', Tanskassa Elsinoressa 17.–18. toukokuuta 2018 pidetyssä 128. istunnossaan. Viittauksilla uudistettuun yleissopimukseen 108 tarkoitetaan yleissopimusta sellaisena kuin se on muutettuna pöytäkirjalla CETS nro 223.
YVV	Yhteinen valvontaviranomainen

Käsikirjan käyttäminen

Tässä käsikirjassa luodaan yleiskatsaus Euroopan unionin (EU) ja Euroopan neuvoston (EN) asettamiin tietosuojaa koskeviin oikeudellisiin normeihin. Käsikirja on tarkoitettu avuksi oikeusalan toimijoille, jotka eivät ole erikoistuneet tietosuojaan, kuten asianajajille ja tuomareille, samoin kuin eri organisaatioissa ja elimissä, kuten kansalaisjärjestöissä, työskenteleville henkilöille, jotka voivat joutua käsittelemään tietosuojaan liittyviä oikeudellisia kysymyksiä.

Se on ensisijainen tiedonlähde tietosuojaan liittyvän EU:n lainsäädännön ja Euroopan ihmisoikeussopimuksen (EIS) alalla. Siinä selitetään, miten tietosuojaa säännellään EN:n yleissopimuksessa yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108) ja muissa EN:n oikeudellisissa välineissä.

Kunkin luvun alussa on taulukko, jossa esitetään luvussa käsiteltävien aiheiden kannalta merkitykselliset säännökset. Taulukot koskevat sekä Euroopan neuvoston että EU:n oikeutta, ja niissä on valittuja oikeustapauksia Euroopan ihmisoikeustuomioistuimesta (EIT) ja Euroopan unionin tuomioistuimesta (EUT). Euroopan kahden oikeusjärjestelmän kannalta merkittävät lait esitellään tämän jälkeen yksi kerrallaan siltä osin kuin niitä sovelletaan käsiteltävänä olevaan aiheeseen. Näin lukija näkee, missä kohdissa oikeusjärjestelmät yhtenevät ja missä ne eroavat toisistaan. Tämän on tarkoitus auttaa lukijaa löytämään omaan tilanteeseensa liittyvä tärkein tieto erityisesti, jos tilanteeseen sovelletaan ainoastaan EN:n oikeutta. Taulukon aiheiden käsittelyjärjestys voi hivenen vaihdella luvun sisällön järjestyksestä, jos sen on katsottu helpottavan sisällön ytimekästä esittämistä. Käsikirjassa esitetään myös lyhyt katsaus Yhdistyneiden kansakuntien kehykseen.

Alan toimijat EU:n ulkopuolisissa maissa, jotka ovat Euroopan neuvoston jäsenvaltioita ja siten Euroopan ihmisoikeussopimuksen ja yleissopimuksen 108 osapuolia, saavat omaa maataan koskevaa tietoa suoraan Euroopan neuvostoa käsittelevistä osioista. EU:n ulkopuolisissa maissa olevien alan toimijoiden on myös huomattava, että EU:n yleisen tietosuoja-asetuksen antamisen jälkeen EU:n tietosuojasääntöjä sovelletaan organisaatioihin ja muihin yksiköihin, jotka eivät ole sijoittautuneet EU:hun, jos ne käsittelevät henkilötietoja ja tarjoavat tavaroita ja palveluja rekisteröidyille unionissa tai seuraavat kyseisten rekisteröityjen käyttäytymistä.

EU:n jäsenvaltioiden toimijoiden on etsittävä tietoa molemmista osioista, koska niitä sitovat molemmat oikeudelliset järjestelmät. On syytä panna merkille, että tietosuojasääntöjä uudistettiin ja nykyaikaistettiin samaan aikaan sekä Euroopan

neuvostossa (uudistettu yleissopimus 108, sellaisena kuin se on muutettuna pöytäkirjalla CETS nro 223) että Euroopan unionissa (yleinen tietosuoja-asetus ja direktiivi (EU) 2016/680). Molempien oikeusjärjestelmien sääntelyviranomaiset ovat kiinnittäneet tarkasti huomiota siihen, että näiden kahden oikeudellisen kehyksen välinen yhdenmukaisuus ja yhteensopivuus varmistetaan. Uudistuksilla on siten yhdenmukaistettu entisestään Euroopan neuvoston ja Euroopan unionin tietosuojalainsäädäntöä. Niille, jotka tarvitsevat lisätietoja jostakin tietystä aiheesta, löytyy käsikirjan kohdasta "Kirjallisuutta" luettelo erikoistuneemmasta aineistosta. Yleissopimuksen 108 ja sen vuoden 2001 lisäpöytäkirjan säännökset ovat voimassa muutospöytäkirjan voimaantuloon asti. Niistä saa tietoa käsikirjan vuoden 2014 painoksesta.

Euroopan neuvoston oikeutta esitellään lyhyinä otteina Euroopan ihmisoikeustuomioistuimen (EIT) käsittelemistä asioista. Asiat on valittu EIT:n lukuisista tietosuojaa käsittelevistä tuomioista ja päätöksistä.

EU:n oikeudesta esitetään erilaisia lainsäädännöllisiä toimia, asiaankuuluvia perussopimusten määräyksiä sekä Euroopan unionin perusoikeuskirja, sellaisina kuin niitä on tulkittu Euroopan unionin tuomioistuimen oikeuskäytännössä. Käsikirjassa esitetään myös tietosuojatyöryhmän antamia lausuntoja ja ohjeita. Tietosuojatyöryhmä on neuvoa-antava elin, jolle annettiin tietosuojadirektiivissä tehtäväksi antaa asiantuntijaneuvontaa EU:n jäsenvaltioille ja jonka Euroopan tietosuojaneuvosto (EDPB) on korvannut 25. toukokuuta 2018 alkaen. Myös Euroopan tietosuojavaltuutetun lausunnoista saadaan tärkeitä näkemyksiä EU:n oikeuden tulkinnasta, ja niitä on siksi otettu mukaan käsikirjaan.

Tässä käsikirjassa kuvaillut tai lainatut oikeustapaukset tarjoavat kattavasti esimerkkejä sekä Euroopan ihmisoikeustuomioistuimen että unionin tuomioistuimen oikeuskäytännöstä. Käsikirjan lopussa olevat ohjeet auttavat lukijaa oikeuskäytännön hakemisessa verkosta. Esitetty unionin tuomioistuimen oikeuskäytäntö liittyy aiempaan tietosuojadirektiiviin. Unionin tuomioistuimen tulkintoja voidaan kuitenkin soveltaa edelleen yleisellä tietosuoja-asetuksella vahvistettuihin vastaaviin oikeuksiin ja velvoitteisiin.

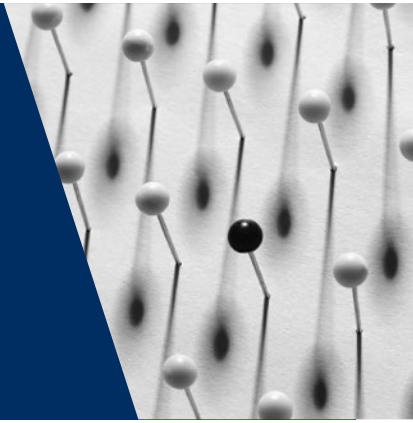
Lisäksi sinitaustaisissa tekstilaatikoissa esitetään käytännönläheisiä esimerkkejä kuvitteellisista tilanteista. Ne auttavat ymmärtämään Euroopan tietosuojasääntöjen soveltamista käytännössä erityisesti silloin, kun aihetta ei ole suoranaisesti käsitelty ihmisoikeustuomioistuimen tai unionin tuomioistuimen oikeuskäytännössä. Muissa tekstilaatikoissa, joissa on harmaa tausta, annetaan esimerkkejä muista lähteistä kuin ihmisoikeustuomioistuimen tai unionin tuomioistuimen oikeuskäytännöstä, kuten lainsäädännöstä ja tietosuojatyöryhmän antamista lausunnoista.

Käsikirjan alussa kuvataan lyhyesti ihmisoikeustuomioistuimen ja unionin tuomioistuimen oikeuden mukaiset kaksi oikeusjärjestelmää (luku 1). Luvuissa 2–10 käsitellään seuraavia asioita:

- tietosuojaan liittyvä terminologia
- Euroopan tietosuojaoikeuden pääperiaatteet
- Euroopan tietosuojaoikeuden säännöt
- riippumaton valvonta
- rekisteröityjen oikeudet ja niiden valvonta
- rajat ylittävät henkilötietojen siirrot ja virrat
- tietosuoja poliisi- ja rikosasioissa
- muut erityiset Euroopan tietosuojasäädökset
- henkilötietojen suojaa koskevat tämän hetken haasteet.

1

Euroopan tietosuojaoikeuden lähtökohdat ja tausta



EU	Käsiteltävät asiat	EN
Oikeus tietosuojaan		
Sopimus Euroopan unionin toiminnasta, 16 artikla Euroopan unionin perusoikeuskirja (perusoikeuskirja), 8 artikla (henkilötietojen suoja) Direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (tietosuojadirektiivi), EYVL 1995, L 281 (voimassa toukokuuhun 2018 saakka) Neuvoston puitepäätös 2008/977/YOS rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta, EUVL 2008, L 350 (voimassa toukokuuhun 2018 saakka) Asetus (EU) 2016/679 luonnollisten henkilöiden suojelusta henkilötietojen käsittelyssä sekä näiden tietojen vapaasta liikkuvuudesta ja direktiivin 95/46/EY kumoamisesta (yleinen tietosuoja-asetus), EUVL 2016, L 119		EIS, 8 artikla (oikeus nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta)

EU	Käsiteltävät asiat	EN
Direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta (poliisi- ja oikeusviranomaisia koskeva tietosuoja), EUVL 2016, L 119 Direktiivi 2002/58/EY henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), EYVL 2002, L 201 Asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EU:n toimielinten tietosuoja-asetus), EYVL 2001, L 8		Uudistettu yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (uudistettu yleissopimus 108)
Rajoitukset henkilötietojen suojaa koskevaan oikeuteen		
Perusoikeuskirja, 52 artiklan 1 kohta Yleinen tietosuoja-asetus, 23 artikla EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 2010		EIS, 8 artiklan 2 kohta. Uudistettu yleissopimus 108, 11 artikla EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 2008
Tasapainottavat oikeudet		
EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 2010	**Yleisesti**	
EUT, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy* [suuri jaosto], 2008 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 2014	**Sananvapaus**	EIT, *Axel Springer AG v. Saksa* [suuri jaosto], nro 39954/08, 2012 EIT, *Mosley v. Yhdistynyt kuningaskunta*, nro 48009/08, 2011 EIT, *Bohlen v. Saksa*, nro 53495/09, 2015

EU	Käsiteltävät asiat	EN
EUT, C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd* [suuri jaosto], 2010 EUT, C-615/13P, *ClientEarth ja PAN Europe v. EFSA*, 2015	Asiakirjojen saatavuus	EIT, *Magyar Helsinki Bizottság v. Unkari* [suuri jaosto], nro 18030/11, 2016
Yleinen tietosuoja-asetus, 90 artikla	Vaitiolovelvollisuus	EIT, *Pruteanu v. Romania*, nro 30181/05, 2015
Yleinen tietosuoja-asetus, 91 artikla	Uskonnon tai vakaumuksen vapaus	
	Taiteen ja tutkimuksen vapaus	EIT, *Vereinigung bildender Künstler v. Itävalta*, nro 68345/01, 2007
EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 2008	Omaisuuden-suoja	
EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 2014 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	Taloudelliset oikeudet	

1.1 Oikeus henkilötietojen suojaan

Keskeiset kohdat

- Euroopan ihmisoikeussopimuksen 8 artiklan mukaan oikeus suojaan henkilötietojen käsittelyltä kuuluu oikeuteen nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta.
- Euroopan neuvoston yleissopimus 108 on ensimmäinen ja tähän mennessä ainoa oikeudellisesti sitova kansainvälinen sopimus, joka koskee erityisesti tietosuojaa. Yleissopimus kävi läpi uudistamisprosessin, jonka päätteeksi hyväksyttiin muutospöytäkirja CETS nro 223.
- EU:n oikeudessa tietosuoja on tunnustettu erilliseksi perusoikeudeksi. Se on vahvistettu EU:n toiminnasta tehdyn sopimuksen 16 artiklassa sekä EU:n perusoikeuskirjan 8 artiklassa.

- EU:n oikeudessa tietosuojaa säänneltiin ensimmäisen kerran vuonna 1995 annetulla tietosuojadirektiivillä.
- Tekniikan nopean kehittymisen vuoksi EU:ssa annettiin vuonna 2016 uutta lainsäädäntöä, jotta tietosuojasäännöt saatiin vastaamaan digitaaliaikaa. Yleistä tietosuoja-asetusta alettiin soveltaa toukokuussa 2018, ja se kumosi tietosuojadirektiivin.
- EU antoi yhdessä yleisen tietosuoja-asetuksen kanssa lainsäädäntöä valtion viranomaisten lainvalvontatarkoituksessa tekemästä henkilötietojen käsittelystä. Direktiivissä (EU) 2016/680 vahvistetaan tietosuojasäännöt ja periaatteet, jotka koskevat henkilötietojen käsittelyä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten.

1.1.1 Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta ja oikeus henkilötietojen suojaan: lyhyt johdanto

Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta ja oikeus henkilötietojen suojaan ovat erillisiä oikeuksia, jotka liittyvät tiiviisti toisiinsa. Oikeus yksityisyyteen – johon EU:n oikeudessa viitataan oikeutena nauttia yksityis- ja perhe-elämän kunnioitusta – ilmaantui kansainväliseen ihmisoikeuslainsäädäntöön vuonna 1948 annetussa ihmisoikeuksien yleismaailmallisessa julistuksessa, jossa se oli yksi suojelluista perusoikeuksista. Pian ihmisoikeusjulistuksen antamisen jälkeen oikeus vahvistettiin myös Euroopassa – Euroopan ihmisoikeussopimuksessa. Se laadittiin vuonna 1950 ja se on sopimuspuolia oikeudellisesti sitova. Ihmisoikeussopimuksessa määrätään, että jokaisella on oikeus nauttia yksityis- ja perhe-elämäänsä, kotiinsa ja kirjeenvaihtoonsa kohdistuvaa kunnioitusta. Viranomaiset eivät saa puuttua tähän oikeuteen, paitsi kun laki sen sallii ja se on välttämätöntä demokraattisessa yhteiskunnassa tärkeiden ja oikeutettujen yleisten etujen turvaamiseksi.

Ihmisoikeusjulistus ja ihmisoikeussopimus hyväksyttiin kauan ennen tietokoneiden ja internetin kehittymistä ja tietoyhteiskunnan nousua. Tämä kehitys on tuonut ihmisille ja yhteiskunnalle merkittäviä etuja parantamalla elämänlaatua, tehokkuutta ja tuottavuutta. Samalla se kuitenkin aiheuttaa uusia riskejä yksityis- ja perhe-elämän kunnioitusta koskevalle oikeudelle. Koska henkilötietojen keräämistä ja käyttämistä varten tarvittiin erityisiä sääntöjä, otettiin käyttöön uusi yksityisyyttä koskeva käsite, ”tiedollinen itsemääräämisoikeus” tai ”oikeus itsemääräämisoikeuteen

henkilötietojen käsittelyssä”.[1] Tämän käsitteen perusteella laadittiin erityisiä säädöksiä, joissa säädetään henkilötietojen suojasta.

Tietoja on suojeltu Euroopassa 1970-luvulta lähtien, kun joissakin valtioissa annettiin lainsäädäntöä viranomaisten ja suuryritysten suorittaman henkilötietojen käsittelyn valvonnasta[2]. Sen jälkeen annettiin tietosuojasäädöksiä Euroopan tasolla[3], ja vuosien myötä tietosuojasta kehittyi erillinen arvo, jota ei enää sisällytetä yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen. Tietosuoja tunnustetaan EU:n oikeusjärjestyksessä perusoikeudeksi, joka on erillään yksityis- ja perhe-elämän kunnioitusta koskevasta perusoikeudesta. Tämä erottelu herättää kysymyksen näiden kahden oikeuden välisestä suhteesta ja niiden eroista.

Oikeus nauttia yksityis- ja perhe-elämän kunnioitusta ja oikeus henkilötietojen suojaan liittyvät tiiviisti toisiinsa. Molemmilla pyritään suojelemaan samanlaisia arvoja eli ihmisten itsemääräämisoikeutta ja ihmisarvoa takaamalla heille henkilökohtainen tila, jossa he voivat kehittää vapaasti persoonallisuuttaan, ajatella ja muotoilla mielipiteitään. Ne ovat siten olennainen edellytys muiden perusoikeuksien käyttämiselle. Niitä ovat muun muassa ilmaisunvapaus, rauhanomainen kokoontumis- ja yhdistymisvapaus ja uskonnonvapaus.

Oikeuksien erot liittyvät niiden muotoiluun ja soveltamisalaan. Yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen liittyy yleinen puuttumiskielto, johon sovelletaan joitakin yleistä etua koskevia perusteita, joilla puuttuminen voidaan tietyissä tapauksissa perustella. Henkilötietojen suojaa pidetään uutena ja aktiivisena

1 Saksan liittovaltion perustuslakituomioistuin vahvisti oikeuden itsemääräämisoikeuteen henkilötietojen käsittelyssä vuonna 1983 asiassa *Volkszählungsurteil* annetussa tuomiossa, BVerfGE Bd. 65, S. 1ff. Tuomioistuin katsoi, että itsemääräämisoikeus henkilötietojen käsittelyssä perustuu henkilöllisyyden suojaa koskevaan perusoikeuteen, joka on suojattu Saksan perustuslaissa. EIT katsoi vuonna 2017 antamassaan tuomiossa, että ihmisoikeussopimuksen 8 artiklassa annetaan tietynlainen itsemääräämisoikeus, kun henkilötietoja käsitellään. Ks. EIT, *Satakunnan Markkinapörssi Oy ja Satamedia Oy v. Suomi* [suuri jaosto], nro 931/13, 27.6.2017, 137 kohta.

2 Saksan Hessenin osavaltiossa annettiin vuonna 1970 ensimmäinen tietosuojalaki, jota sovellettiin vain kyseisessä osavaltiossa. Ruotsissa annettiin vuonna 1973 maailman ensimmäinen kansallinen tietosuojalaki. 1980-luvun loppuun mennessä tietosuojalainsäädäntöä oli otettu käyttöön useissa Euroopan maissa (Alankomaissa, Ranskassa, Saksassa ja Yhdistyneessä kuningaskunnassa).

3 Euroopan neuvoston yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108) hyväksyttiin vuonna 1981. EU hyväksyi ensimmäisen kattavan tietosuojasäädöksensä vuonna 1995: direktiivi 95/46/EY yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta.

oikeutena[4], joka sisältää tarkastus- ja arviointijärjestelmän (*checks and balances*), jolla suojataan ihmisiä aina, kun näiden henkilötietoja käsitellään. Käsittelyssä on noudatettava henkilötietojen suojan olennaisia osatekijöitä eli riippumatonta valvontaa ja rekisteröityjen oikeuksien kunnioittamista.[5]

Euroopan unionin perusoikeuskirjan 8 artiklassa sekä vahvistetaan oikeus henkilötietojen suojaan että selitetään kyseiseen oikeuteen liittyvät ydinarvot. Siinä määrätään, että tietojen käsittelyn on oltava asianmukaista ja sen on tapahduttava tiettyä tarkoitusta varten ja asianomaisen henkilön suostumuksella tai muun laissa säädetyn käsittelyn oikeuttavan perusteen nojalla. Jokaisella on oltava oikeus tutustua henkilötietoihinsa ja saada ne oikaistuksi. Riippumattoman viranomaisen on valvottava näiden sääntöjen noudattamista.

Oikeus henkilötietojen suojaan on voimassa aina, kun henkilötietoja käsitellään. Se on siten laajempi kuin oikeus nauttia yksityis- ja perhe-elämän kunnioitusta. Kaikkea henkilötietojen käsittelyä on suojattava asianmukaisesti. Tietosuoja koskee kaikenlaisia henkilötietoja ja tietojenkäsittelyä riippumatta niiden suhteesta ja vaikutuksesta yksityisyyteen. Henkilötietojen käsittely voi myös loukata oikeutta yksityisyyteen, kuten jäljempänä olevissa esimerkeissä osoitetaan. Tietosuojasääntöjen soveltamisen aloittamiseksi ei kuitenkaan tarvitse osoittaa, että yksityiselämän suojaa on loukattu.

Oikeus yksityisyyteen koskee tilanteita, joissa henkilön etu tai ”yksityis- ja perhe-elämä” on vaarantunut. ”Yksityis- ja perhe-elämän” käsitettä on tulkittu oikeuskäytännössä laajasti, kuten tässä käsikirjassa osoitetaan. Sen on tulkittu koskevan henkilökohtaisia tilanteita, arkaluonteisia tai luottamuksellisia tietoja, tietoja, jotka voisivat vaikuttaa haitallisesti yleisön näkemykseen henkilöstä, ja jopa henkilön työelämään ja julkiseen käytökseen liittyviä näkökohtia. Puuttuminen ”yksityis- ja perhe-elämään” on kuitenkin arvioitava tapauskohtaisesti taustan ja tosiseikkojen perusteella.

Sitä vastoin kaikki toimet, joihin liittyy henkilötietojen käsittelyä, voivat kuulua tietosuojasääntöjen soveltamisalaan ja antaa oikeuden henkilötietojen suojaan. Kun

4 Julkisasiamies Eleanor Sharpston kuvasi, että asiassa vedotaan kahteen eri oikeuteen: ”perinteiseen” yksityisyyden suojaa koskevaan oikeuteen ja ”uudempaan” tietosuojaa koskevaan oikeuteen. Ks. EUT, yhdistetyt asiat C-92/09 ja C-93/02, *Volker und Markus Schecke GbR v. Land Hessen, julkisasiamies Sharpstonin ratkaisuehdotus*, 17.6.2010, 71 kohta.

5 Hustinx, P., Euroopan tietosuojavaltuutetun puheita ja artikkeleja, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, heinäkuu 2013.

esimerkiksi työnantaja tallentaa työntekijöiden nimiin ja palkkoihin liittyvää tietoa, pelkästään näiden tietojen tallentamista ei voida katsoa puuttumiseksi yksityiselämään. Puuttumisesta voisi kuitenkin olla kyse esimerkiksi silloin, jos työnantaja siirtäisi työntekijöiden henkilötietoja kolmansille osapuolille. Työnantajien on joka tapauksessa noudatettava tietosuojasääntöjä, koska työntekijöiden tietojen tallentaminen on tietojenkäsittelyä.

Esimerkki: Asiassa *Digital Rights Ireland*[6] EU:n tuomioistuinta pyydettiin päättämään direktiivin 2006/24/EY pätevyydestä EU:n perusoikeuskirjassa vahvistettujen henkilötietojen suojaa ja yksityis- ja perhe-elämän kunnioitusta koskevien perusoikeuksien kannalta. Direktiivissä vaaditaan yleisesti saatavilla olevia sähköisiä viestintäpalveluja tai yleisiä viestintäverkkoja säilyttämään kansalaisten televiestintätietoja enintään kahden vuoden ajan, jotta voidaan varmistaa, että tiedot ovat käytettävissä vakavan rikollisuuden tutkintaa, selvittämistä ja syyteharkintaa varten. Säädös koski vain metatietoja, sijaintitietoja ja tietoja, joita tarvitaan tilaajan tai käyttäjän tunnistamiseen. Se ei koskenut sähköisen viestinnän sisältöä.

Tuomioistuin katsoi, että direktiivi merkitsee puuttumista henkilötietojen suojan perusoikeuteen, koska ”direktiivissä säädetään henkilötietojen käsittelystä”[7]. Lisäksi se katsoi, että direktiivi puuttui oikeuteen nauttia yksityiselämän kunnioitusta[8]. Direktiivin mukaisesti säilytettyjen henkilötietojen kokonaisuus, jonka toimivaltaiset viranomaiset voisivat saada käyttöönsä, voisi ”mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituisista tai väliaikaisista oleskelupaikoista, päivittäisestä tai muusta liikkumisesta, tekemisestä sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään”[9]. Näihin kahteen oikeuteen puuttuminen oli laajaperäistä ja erityisen vakavaa.

6 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

7 *Ibid.*, 36 kohta.

8 *Ibid.*, 32–35 kohta.

9 *Ibid.*, 27 kohta.

Tuomioistuin totesi, että direktiivi 2006/24/EY on pätemätön, ja katsoi, että vaikka sen tavoitteet ovat hyväksyttäviä, puuttuminen henkilötietojen suojan ja yksityis- ja perhe-elämän kunnioittamisen oikeuksiin on vakavaa eikä se rajoitu vain siihen, mikä on ehdottoman välttämätöntä.

1.1.2 Kansainvälinen lainsäädäntökehys: Yhdistyneet kansakunnat

Yhdistyneiden kansakuntien lainsäädäntökehyksessä henkilötietojen suojaa ei tunnusteta perusoikeudeksi, vaikka oikeus yksityisyyteen on kauan sitten vakiintunut perusoikeus kansainvälisessä oikeusjärjestelmässä. Ihmisoikeuksien yleismaailmallisen julistuksen yksityis- ja perhe-elämän kunnioittamista koskevassa 12 artiklassa[10] säädettiin – kansainvälisessä säädöksessä ensimmäistä kertaa – että henkilöllä on oikeus saada suojaa muiden, erityisesti valtion, puuttumiselta yksityiselämäänsä. Vaikka ihmisoikeusjulistus ei ole sitova, sillä on merkittävä asema kansainvälisen ihmisoikeuslainsäädännön perussäädöksenä, ja se on vaikuttanut muiden ihmisoikeussäädösten kehittymiseen Euroopassa. Kansalaisoikeuksia ja poliittisia oikeuksia koskeva kansainvälinen yleissopimus (KP-yleissopimus) tuli voimaan vuonna 1976. Siinä määrätään, että kenenkään yksityiselämään, perheeseen, kotiin tai kirjeenvaihtoon ei saa mielivaltaisesti tai laittomasti puuttua eikä hyökätä hänen kunniaansa ja mainettaan vastaan. KP-yleissopimus on kansainvälinen sopimus, joka velvoittaa 169 sopimusosapuoltaan kunnioittamaan ja varmistamaan henkilöiden kansalaisoikeuksia, myös yksityisyyttä.

Yhdistyneet kansakunnat on vuoden 2013 jälkeen antanut yksityisyyttä koskevista kysymyksistä kaksi päätöslauselmaa, joissa käsitellään oikeutta yksityisyyteen digitaalisella ajalla[11]. Niillä vastataan uusien teknologioiden kehitykseen ja paljastuksiin joissakin valtioissa toteutetusta joukkovalvonnasta (Snowdenin paljastukset). Niissä tuomitaan voimakkaasti joukkovalvonta ja korostetaan vaikutusta, joka tällaisella valvonnalla voi olla yksityisyyttä ja ilmaisuvapautta koskeviin perusoikeuksiin ja elävän ja demokraattisen yhteiskunnan toimintaan. Vaikka päätöslauselmat eivät ole oikeudellisesti sitovia, ne ovat käynnistäneet merkittävän kansainvälisen korkean tason poliittisen keskustelun yksityisyydestä, uusista teknologioista ja valvonnasta.

10 Yhdistyneet kansakunnat (YK), Ihmisoikeuksien yleismaailmallinen julistus (ihmisoikeusjulistus), 10. joulukuuta 1948.

11 Ks. YK:n yleiskokous, Resolution on the right to privacy in the digital age, A/RES/68/167, New York, 18.12.2013; ja YK:n yleiskokous, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, New York, 19.11.2014.

Niiden ansiosta myös perustettiin toimi yksityisyyttä koskevan oikeuden erikoisraportoijalle, jonka tehtävänä on edistää ja suojata tätä oikeutta. Raportoijan erityistehtäviin kuuluu muun muassa kerätä tietoa yksityisyyteen liittyvistä kansallisista käytännöistä ja kokemuksista sekä uusista teknologioista johtuvista haasteista. Hänen tehtävänään on myös vaihtaa ja edistää parasta käytäntöä ja tunnistaa mahdollisia esteitä.

Kun aiemmissa päätöslauselmissa keskityttiin joukkovalvonnan kielteisiin vaikutuksiin ja valtioiden vastuuseen rajoittaa tiedusteluviranomaisten valtuuksia, uudemmat päätöslauselmat heijastavat Yhdistyneissä kansakunnissa yksityisyydestä käytävän keskustelun keskeistä kehitystä.[12] Vuosina 2016 ja 2017 annetuissa päätöslauselmissa vahvistetaan, että tiedusteluvirastojen valtuuksia on rajoitettava, ja tuomitaan joukkovalvonta. Niissä kuitenkin myös todetaan yksiselitteisesti, että yritysten kasvavat valmiudet kerätä, käsitellä ja käyttää henkilötietoja voivat aiheuttaa riskin yksityisyyttä koskevan oikeuden käyttämiselle digitaaliajalla. Valtion viranomaisten vastuun lisäksi päätöslauselmissa korostetaan siten yksityisen sektorin vastuuta ihmisoikeuksien kunnioittamisessa ja kehotetaan yrityksiä tiedottamaan käyttäjille henkilötietojen keräämisestä, käyttämisestä, jakamisesta ja säilyttämisestä sekä laatimaan avoimet käsittelykäytännöt.

1.1.3 Euroopan ihmisoikeussopimus

Euroopan neuvosto (EN) perustettiin toisen maailmansodan jälkimainingeissa saattamaan Euroopan maat yhteen oikeusvaltion, demokratian, ihmisoikeuksien ja sosiaalisen kehityksen edistämiseksi. Tätä tarkoitusta varten se hyväksyi vuonna 1950 Euroopan ihmisoikeussopimuksen, joka tuli voimaan vuonna 1953.

Sopimuspuolilla on kansainvälinen velvollisuus noudattaa ihmisoikeussopimusta. Kaikki Euroopan neuvoston jäsenvaltiot ovat nyt saattaneet sopimuksen osaksi kansallista lainsäädäntöään, mikä edellyttää niiden noudattavan sopimuksen määräyksiä. Sopimuspuolten on kunnioitettava sopimuksessa määrättyjä oikeuksia toteuttaessaan toimia tai käyttäessään valtuuksia. Se koskee myös kansallisen turvallisuuden puolesta toteutettuja toimia. Euroopan ihmisoikeustuomioistuimen ennakkopäätökset ovat koskeneet valtion toimia kansallista

12 YK:n yleiskokous, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, New York, 16.11.2016; YK:n ihmisoikeusneuvosto, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, 22.3.2017.

turvallisuuslainsäädäntöä ja -käytäntöä koskevilla arkaluonteisilla aloilla.[13] Tuomioistuin ei ole epäröinyt vahvistaa, että valvontatoimet ovat puuttumista yksityis- ja perhe-elämän kunnioitukseen.[14]

Euroopan ihmisoikeustuomioistuin perustettiin Ranskan Strasbourgiin vuonna 1959. Sen tehtävänä on varmistaa, että sopimuspuolet täyttävät ihmisoikeussopimuksen mukaiset velvollisuutensa. Ihmisoikeustuomioistuin varmistaa, että valtiot täyttävät sopimuksen mukaiset velvoitteensa tutkimalla yksityishenkilöiden, ryhmien, kansalaisjärjestöjen ja oikeushenkilöiden tekemiä valituksia sopimuksen rikkomisesta. Ihmisoikeustuomioistuin voi myös tarkastella valtioiden välisiä asioita, joissa yksi tai useampi Euroopan neuvoston jäsenvaltio on nostanut kanteen toista jäsenvaltiota vastaan.

Vuonna 2018 Euroopan neuvostoon kuului 47 jäsenvaltiota, joista 28 on myös EU:n jäsenvaltioita. Euroopan ihmisoikeustuomioistuimessa kantajan ei tarvitse olla sopimuspuolen kansalainen, mutta väitettyjen loukkausten on pitänyt tapahtua jonkin sopimuspuolen oikeudenkäyttöalueella.

Oikeus henkilötietojen suojaan kuuluu ihmisoikeussopimuksen 8 artiklassa turvattuihin oikeuksiin. Kyseisessä artiklassa taataan oikeus nauttia yksityis- ja perhe-elämään, kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta ja määrätään ehdot, joilla tätä oikeutta voidaan rajoittaa.[15]

Euroopan ihmisoikeustuomioistuin on tutkinut useita tilanteita, joissa on noussut esiin kysymys tietosuojasta. Ne ovat koskeneet muun muassa telekuuntelua[16], valvonnan eri muotoja sekä yksityisellä että julkisella sektorilla[17] ja suojaa viranomaisten suorittamaa henkilötietojen tallentamista vastaan[18]. Yksityis- ja perhe-elämän kunnioitus ei ole ehdoton oikeus, koska yksityisyyttä koskevan oikeuden käyttäminen voisi vaarantaa muut oikeudet, kuten ilmaisuvapauden ja tiedonsaantioikeuden,

13 Ks. esim. EIT, *Klass ym. v. Saksa*, nro 5029/71, 6.9.1978; EIT, *Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000 ja EIT, *Szabó ja Vissy v. Unkari*, nro 37138/14, 12.1.2016.

14 *Ibid.*

15 Euroopan neuvosto, Euroopan ihmisoikeussopimus, CETS nro 005, 1950.

16 Ks. esim. EIT, *Malone v. Yhdistynyt kuningaskunta*, nro 8691/79, 2.8.1984; EIT, *Copland v. Yhdistynyt kuningaskunta*, nro 62617/00, 3.4.2007, tai EIT, *Mustafa Sezgin Tanrıkulu v. Turkki*, nro 27473/06, 18.7.2017.

17 Ks. esim. EIT, *Klass ym. v. Saksa*, nro 5029/71, 6.9.1978; EIT, *Uzun v. Saksa*, nro 35623/05, 2.9.2010.

18 Ks. esim. EIT, *Roman Zakharov v. Venäjä* [suuri jaosto], nro 47143/06, 4.12.2015; EIT, *Szabó ja Vissy v. Unkari*, nro 37138/14, 12.1.2016.

ja päinvastoin. Tuomioistuin pyrkii siksi löytämään tasapainon kyseessä olevien eri oikeuksien välillä. Se on tarkentanut, että ihmisoikeussopimuksen 8 artiklaan sisältyy paitsi valtioiden velvollisuus pitäytyä toimista, jotka saattavat rikkoa tätä sopimuksessa vahvistettua oikeutta, myös tietyissä olosuhteissa positiivinen velvoite turvata aktiivisesti yksityis- ja perhe-elämän kunnioittaminen.[19] Monia näistä asioista esitellään tarkemmin asianmukaisissa luvuissa.

1.1.4 Euroopan neuvoston yleissopimus 108

Tietotekniikan kehittyminen 1960-luvulla loi tarpeen kehittää yksityiskohtaisemmat säännöt henkilöiden suojelemiseksi suojaamalla heidän henkilötietojaan. Euroopan neuvoston ministerikomitea antoi 1970-luvun puolivälissä erilaisia henkilötietojen suojelua koskevia julkilausumia, jotka perustuivat Euroopan ihmisoikeussopimuksen 8 artiklaan[20]. Vuonna 1981 avattiin allekirjoitettavaksi yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä (yleissopimus 108)[21]. Yleissopimus 108 oli tuolloin ja on edelleen ainoa oikeudellisesti sitova kansainvälinen sopimus tietosuojan alalla.

Yleissopimusta 108 sovelletaan kaikkeen henkilötietojen käsittelyyn sekä yksityisellä että julkisella sektorilla, kuten esimerkiksi henkilötietojen käsittelyyn oikeuslaitoksessa ja lainvalvontaviranomaisissa. Se suojaa yksilöitä väärinkäytöltä, jota henkilötietojen käsittelyn yhteydessä voi tapahtua, ja samalla pyrkii sääntelemään henkilötietojen siirtoa rajojen yli. Henkilötietojen käsittelyn osalta yleissopimuksessa vahvistetut periaatteet koskevat erityisesti tietojen oikeudenmukaista ja laillista keruuta ja automaattista käsittelyä määriteltyä lainmukaista tarkoitusta varten. Tämä tarkoittaa, että tietoja ei pitäisi käyttää määritellyn tarkoituksen kanssa yhteensopimattomalla tavalla eikä säilyttää pidempään kuin on tarpeellista määritellyn tarkoituksen kannalta. Periaatteet koskevat myös tietojen laatua, erityisesti tietojen asianmukaisuutta, tarpeellisuutta, oikeasuhteisuutta (ne eivät saa olla liiallisia) sekä virheettömyyttä.

19 Ks. esim. EIT, *I v. Suomi*, nro 20511/03, 17.7.2008; EIT, *K.U. v. Suomi*, nro 2872/02, 2.12.2008.

20 Euroopan neuvoston ministerikomitea (1973), julkilausuma (73) 22 henkilöiden yksityisyyden suojelusta yksityissektorin sähköisten tietopankkien yhteydessä, 26.9.1973; Euroopan neuvoston ministerikomitea (1974), julkilausuma (74) 29 henkilöiden yksityisyyden suojelusta julkisen sektorin sähköisten tietopankkien yhteydessä, 20.9.1974.

21 Euroopan neuvosto, yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, CETS nro 108, 1981.

Sen lisäksi, että yleissopimuksessa annetaan henkilötietojen käsittelyyn liittyviä takeita, siinä kielletään ”arkaluonteisten” henkilötietojen, kuten rotua, politiikkaa, terveyttä, uskontoa, sukupuolielämää tai rikosrekisteriä koskevien tietojen, käsitteleminen ilman riittäviä oikeudellisia suojatoimia.

Yleissopimuksessa myös vahvistetaan yksilön oikeus saada tietää, että hänestä on tallennettu tietoja, ja oikeus saada tarvittaessa korjata tietoja. Yleissopimuksessa asetettuja oikeuksia voidaan rajoittaa vain, jos välttämätön etu, kuten valtion turvallisuus tai puolustus, edellyttää sitä. Yleissopimuksessa mahdollistetaan lisäksi henkilötietojen vapaa siirto sopimuspuolien välillä ja asetetaan tiettyjä rajoituksia siirroille sellaisiin maihin, joissa ei ole vahvistettu säädöksillä riittävää suojaa.

Yleissopimus 108 sitoo sen ratifioineita valtioita. EIT ei valvo sitä oikeudellisesti, mutta se on otettu huomioon EIT:n oikeuskäytännössä ihmisoikeussopimuksen 8 artiklan yhteydessä. EIT:n vuosien aikana antamien tuomioiden mukaan henkilötietojen suoja on tärkeä osa oikeutta nauttia yksityis- ja perhe-elämän kunnioitusta (8 artikla). Tuomioistuin on käyttänyt yleissopimuksen 108 periaatteita ohjeena määrittäessään, onko tähän perusoikeuteen puututtu.[22]

Yleissopimuksessa 108 vahvistettujen yleisten periaatteiden ja sääntöjen viemiseksi eteenpäin EN:n ministerikomitea on antanut useita suosituksia, jotka eivät ole oikeudellisesti sitovia. Nämä suositukset ovat vaikuttaneet tietosuojalainsäädännön kehittymiseen Euroopassa. Esimerkiksi vuosien ajan Euroopassa ainoa säädös, joka ohjasi henkilötietojen käyttöä poliisitoimen alalla, oli poliisiasioita koskeva suositus[23]. Suosituksen periaatteita otettiin mukaan myöhempään EU:n lainsäädäntöön, jossa niitä kehitettiin edelleen. Ne koskevat muun muassa tapaa, jolla henkilötietoja sisältäviä tiedostoja säilytetään, sekä tarvetta laatia selkeät säännöt henkilöille, jotka voivat käyttää näitä tiedostoja.[24] Uudemmissa suosituksissa pyritään puuttumaan digitaaliajan haasteisiin, esimerkiksi tietojenkäsittelyyn työsuhteen yhteydessä (ks. luku 9).

Kaikki EU:n jäsenvaltiot ovat ratifioineet yleissopimuksen 108. Vuonna 1999 yleissopimukseen 108 ehdotettiin muutoksia, joiden nojalla EU:sta saattoi tulla

22 Ks. esim. EIT, *Z v. Suomi*, nro 22009/93, 25.2.1997.

23 Euroopan neuvoston ministerikomitean suositus R (87) 15 jäsenvaltioille henkilötietojen käytön sääntelemisestä poliisialalla, Strasbourg, 17.9.1987.

24 Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL L 281, 23.11.1995.

sopimuksen osapuoli, mutta muutokset eivät koskaan tulleet voimaan.[25] Vuonna 2001 hyväksyttiin yleissopimuksen 108 lisäpöytäkirja. Siinä otettiin käyttöön säännöksiä maan rajan yli tapahtuvasta tietojen siirrosta sopimuksen ulkopuolisiin niin kutsuttuihin kolmansiin maihin ja kansallisen tietosuojaviranomaisen pakollisesta perustamisesta.[26]

Yleissopimukseen 108 voivat liittyä myös Euroopan neuvoston ulkopuoliset maat. Yleissopimus voisi toimia yleismaailmallisena normina, ja avoimuutensa ansiosta se voisi auttaa edistämään tietosuojaa koko maailmassa. Tällä hetkellä yleissopimukseen 108 kuuluu 51 maata. Niitä ovat kaikki Euroopan neuvoston jäsenvaltiot (47 maata), Uruguay, joka liittyi elokuussa 2013 ensimmäisenä Euroopan ulkopuolisena maana, sekä Mauritius, Senegal ja Tunisia, jotka liittyivät vuosina 2016 ja 2017.

Yleissopimusta uudistettiin äskettäin. Vuonna 2011 toteutettu julkinen kuuleminen auttoi vahvistamaan työn kaksi tärkeintä tavoitetta: yksityisyyden suojaa digitaalialalla on vahvistettava ja yleissopimuksen seurantamekanismeja on tehostettava. Näihin tavoitteisiin keskityttiin uudistamisprosessissa, joka saatiin päätökseen, kun yleissopimuksen 108 muutospöytäkirja hyväksyttiin (pöytäkirja CETS nro 223). Työtä tehtiin rinnakkain kansainvälisten tietosuojasäädösten muiden uudistusten kanssa ja vuonna 2012 käynnistetyn EU:n tietosuojasääntöjen uudistuksen ohella. Euroopan neuvoston ja EU:n sääntelyviranomaiset ovat pitäneet tarkasti huolta näiden kahden oikeudellisen kehyksen yhdenmukaisuuden ja yhteensopivuuden varmistamisesta. Uudistamisessa on säilytetty yleissopimuksen yleinen joustavuus ja vahvistettu sen mahdollisuutta toimia tietosuojalainsäädännön yleismaailmallisena normina. Siinä on vahvistettu ja vakiinnutettu tärkeitä periaatteita ja annettu yksilöille uusia oikeuksia. Sillä on myös lisätty henkilötietoja käsittelevien yhteisöjen vastuuta ja varmistettu entistä laajempi osoitusvelvollisuus. Ihmisillä, joiden henkilötietoja käsitellään, on nyt esimerkiksi oikeus saada tietoa kyseisen tietojenkäsittelyn perusteluista ja oikeus vastustaa käsittelyä. Yleissopimuksella pyritään myös torjumaan profiloinnin lisääntyvää käyttöä verkkomaailmassa. Siinä vahvistetaan henkilöiden oikeus siihen, että heitä koskevia päätöksiä ei tehdä ainoastaan automaattisen käsittelyn perusteella ottamatta heidän omia näkemyksiään huomioon. Yleissopimuksen käytännön täytäntöönpanon kannalta olennaiseksi katsotaan se,

25 Euroopan neuvosto, ministerikomitean Strasbourgissa 15. kesäkuuta 1999 hyväksymät muutokset yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa käsittelyssä (ETS nro 108).

26 Euroopan neuvosto, valvontaviranomaisia ja maan rajan yli tapahtuvaa tietojen siirtoa koskeva lisäpöytäkirja yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, CETS nro 181, 2001. Yleissopimuksen 108 uudistamisen jälkeen lisäpöytäkirjaa ei enää sovelleta, koska sen säännökset on saatettu ajan tasalle ja yhdistetty uudistettuun yleissopimukseen 108.

että riippumattomat valvontaviranomaiset valvovat tehokkaasti tietosuojasääntöjen noudattamista. Sen takia uudistetussa yleissopimuksessa korostetaan, että valvontaviranomaisille on annettava tehokkaat valtuudet ja tehtävät, ja niiden on pystyttävä suorittamaan tehtävänsä riippumattomasti.

1.1.5 Euroopan unionin tietosuojalainsäädäntö

EU:n oikeus koostuu perussopimuksista ja johdetusta oikeudesta. Perussopimukset, eli sopimus Euroopan unionista (SEU) ja sopimus Euroopan unionin toiminnasta (SEUT), ovat kaikkien EU:n jäsenvaltioiden hyväksymiä. Niitä kutsutaan myös EU:n primaarioikeudeksi. EU:n toimielimet antavat asetuksia, direktiivejä ja päätöksiä perussopimusten mukaisten valtuuksiensa nojalla. Näitä säädöksiä kutsutaan EU:n johdetuksi oikeudeksi.

Tietosuoja EU:n primaarioikeudessa

Euroopan yhteisöjen alkuperäisissä perussopimuksissa ei viitattu ihmisoikeuksiin eikä niiden suojeluun, koska Euroopan talousyhteisö suunniteltiin alun perin alueelliseksi järjestöksi, jossa keskitytään taloudelliseen yhdentymiseen ja sisämarkkinoiden luomiseen. Euroopan yhteisön perustamisen ja kehittämisen taustalla oleva perusperiaate – joka on nykyäänkin yhtä pätevä – on annetun toimivallan periaate. Tämän periaatteen mukaisesti unioni toimii ainoastaan jäsenvaltioiden sille perussopimuksissa antaman toimivallan rajoissa, kuten EU:n perussopimuksissa todetaan. Euroopan neuvostosta poiketen EU:n perussopimukset eivät sisällä yksiselitteistä toimivaltaa perusoikeusasioissa.

Euroopan unionin tuomioistuin teki kuitenkin merkittäviä tulkintoja perussopimuksista, kun sen käsiteltäväksi tuli asioita, joissa epäiltiin ihmisoikeusrikkomuksia EU:n lainsäädännön soveltamisalaan kuuluvilla aloilla. Yksilöiden suojelemiseksi tuomioistuin saattoi perusoikeudet osaksi niin kutsuttuja Euroopan oikeuden yleisiä periaatteita. Unionin tuomioistuimen mukaan nämä yleiset periaatteet vastaavat sitä, mitä kansallisissa perustuslaeissa ja ihmisoikeussopimuksissa, ja etenkin Euroopan ihmisoikeussopimuksessa, säädetään ihmisoikeuksien suojelusta. Unionin tuomioistuin ilmoitti varmistavansa, että näitä periaatteita noudatetaan EU:n lainsäädännössä.

EU tiedosti, että sen politiikka voi vaikuttaa ihmisoikeuksiin ja lisäksi se oli asettanut tavoitteekseen kansalaisläheisyyden. Tämän seurauksena EU vahvisti Euroopan unionin perusoikeuskirjan vuonna 2000. Perusoikeuskirjaan sisältyy monipuolisesti

Euroopan kansalaisten kansalaisoikeuksia sekä poliittisia, taloudellisia ja sosiaalisia oikeuksia, jotka perustuvat jäsenvaltioille yhteisiin valtiosääntöperinteisiin ja kansainvälisiin velvollisuuksiin. Perusoikeuskirjassa määritellyt oikeudet on jaettu kuuteen lukuun: ihmisarvo, vapaudet, tasa-arvo, yhteisvastuu, kansalaisten oikeudet ja lainkäyttö.

Perusoikeuskirja oli alun perin vain poliittinen asiakirja, mutta siitä tuli oikeudellisesti sitova[27] osa EU:n primaarioikeutta (ks. SEU-sopimuksen 6 artiklan 1 kohta), kun Lissabonin sopimus tuli voimaan 1. joulukuuta 2009.[28] Perusoikeuskirjan säännökset on osoitettu EU:n toimielimille ja elimille, ja se velvoittaa ne kunnioittamaan perusoikeuskirjassa lueteltuja oikeuksia tehtäviään täyttäessään. Perusoikeuskirjan säännökset sitovat jäsenvaltioita myös niiden soveltaessa EU:n oikeutta.

Sen lisäksi, että perustamissopimuksessa taataan oikeus yksityis- ja perhe-elämän kunnioittamiseen (7 artikla), siinä vahvistetaan oikeus henkilötietojen suojaan (8 artikla) niin, että tämä suoja yksiselitteisesti korotetaan EU:n oikeuden mukaiseksi perusoikeudeksi. Velvollisuus kunnioittaa ja suojata tätä oikeutta koskee paitsi EU:n toimielimiä myös jäsenvaltioita, kun ne soveltavat unionin oikeutta (perusoikeuskirjan 51 artikla). Vuosia tietosuojadirektiivin antamisen jälkeen laaditun perusoikeuskirjan 8 artiklan on ymmärrettävä ilmentävän jo voimassa olevaa EU:n lainsäädäntöä. Siksi perusoikeuskirjassa ei pelkästään mainita 8 artiklan 1 kohdassa oikeutta tietosuojaan vaan myös viitataan 8 artiklan 2 kohdassa tietosuojan pääperiaatteisiin. Lisäksi perusoikeuskirjan 8 artiklan 3 kohdassa varmistetaan, että riippumaton viranomainen valvoo periaatteiden noudattamista.

Lissabonin sopimuksen tekeminen oli virstanpylväs henkilötietojen suojaa koskevan lainsäädännön kehittämisessä. Sen nojalla Euroopan unionin perusoikeuskirjasta tuli primaarioikeuden tasolla oikeudellisesti sitova asiakirja ja samalla oikeudesta henkilötietojen suojaan tuli itsenäinen perusoikeus. Tästä oikeudesta säädetään nimenomaisesti SEUT-sopimuksen 16 artiklassa, joka sisältyy EU:n yleisiä periaatteita käsittelevään perussopimuksen osaan. Perussopimuksen 16 artiklassa säädetään myös uudesta oikeusperustasta, jonka nojalla EU:lle annetaan yleinen lainsäädäntövalta tietosuoja-asioissa. Tämä kehitys on merkittävää, koska EU:n tietosuojasäännöt – erityisesti tietosuojadirektiivi – perustuivat alun perin sisämarkkinoiden oikeusperustaan ja siihen, että kansallisia lakeja oli lähennettävä, jotta tiedot voisivat liikkua esteettä EU:ssa. SEUT-sopimuksen 16 artiklassa säädetään nyt

27 EU (2012), Euroopan unionin perusoikeuskirja, EUVL 2012, C 326.

28 Ks. Euroopan unionista tehdyn sopimuksen konsolidoitu toisinto (2012), EUVL 2012, C 326; ja Euroopan unionin toiminnasta tehdyn sopimuksen konsolidoitu toisinto (2012), EUVL 2012, C 326.

riippumattomasta oikeusperustasta tietosuojaa koskevalle nykyaikaisella ja kattavalle lähestymistavalle. Se koskee kaikkia EU:n toimivaltaan kuuluvia asioita, muun muassa poliisiyhteistyötä ja oikeudellista yhteistyötä rikosasioissa. SEUT-sopimuksen 16 artiklassa vahvistetaan myös, että riippumattomat valvontaviranomaiset valvovat sen mukaan annettujen tietosuojasääntöjen noudattamista. SEUT-sopimuksen 16 artikla oli oikeusperusta vuonna 2016 tehdylle tietosuojasääntöjen kokonaisvaltaiselle uudistukselle. Silloin annettiin yleinen tietosuoja-asetus ja poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi (ks. jäljempänä).

Yleinen tietosuoja-asetus

Vuodesta 1995 toukokuuhun 2018 asti EU:n pääasiallinen oikeudellinen väline tietosuojan alalla oli yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta 24 päivänä lokakuuta 1995 annettu Euroopan parlamentin ja neuvoston direktiivi 95/46/EY (tietosuojadirektiivi)[29]. Se annettiin vuonna 1995, jolloin useat jäsenvaltiot olivat jo säätäneet kansallisia tietosuojalakeja[30], koska näitä lakeja oli yhdenmukaistettava, jotta voitiin varmistaa korkeatasoinen suoja ja henkilötietojen vapaa liikkuminen eri jäsenvaltioiden välillä. Tavaroiden, palvelujen ja henkilöiden vapaa liikkuvuus sisämarkkinoilla edellytti tietojen vapaata siirtoa, jota ei olisi voitu toteuttaa, elleivät jäsenvaltiot olisi voineet luottaa yhtenäiseen korkeaan tietosuojan tasoon.

Tietosuojadirektiivi perustui kansallisilla laeissa ja yleissopimuksessa 108 jo oleviin tietosuojaperiaatteisiin, joita usein myös laajennettiin direktiivissä. Tietosuojadirektiivissä hyödynnettiin yleissopimuksen 108 11 artiklassa annettua mahdollisuutta myöntää laajempi suoja. Erityisesti riippumattoman valvonnan käyttöönotto tietosuojasääntöjen noudattamisen parantamiseksi tehosti merkittävästi Euroopan tietosuojalainsäädännön toimivuutta. Tämä sisällytettiinkin vuonna 2001 Euroopan neuvoston oikeuteen yleissopimuksen 108 lisäpöytäkirjalla. Tämä kertoo tiiviistä vuorovaikutuksesta kahden välineen välillä ja niiden myönteisestä vaikutuksesta toisiinsa vuosien mittaan.

29 Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 1995, L 281.

30 Saksan Hessenin osavaltiossa annettiin vuonna 1970 maailman ensimmäinen tietosuojalaki, jota sovellettiin vain kyseisessä osavaltiossa. Ruotsissa annettiin *Datalagen* vuonna 1973; Saksassa annettiin *Bundesdatenschutzgestez* vuonna 1976; ja Ranskassa annettiin *Loi relatif à l'informatique, aux fichiers et aux libertés* vuonna 1977. Yhdistyneessä kuningaskunnassa annettiin *Data Protection Act* vuonna 1984. Alankomaissa annettiin *Wet Persoonregistraties* vuonna 1989.

Tietosuojadirektiivillä luotiin yksityiskohtainen ja kokonaisvaltainen tietosuojajärjestelmä EU:hun. Direktiivejä ei kuitenkaan EU:n oikeusjärjestelmässä sovelleta suoraan vaan ne on saatettava osaksi jäsenvaltioiden kansallista lainsäädäntöä. Jäsenvaltioilla on pakostakin harkintavaltaa direktiivin saattamisessa osaksi lainsäädäntöään. Vaikka direktiivillä oli tarkoitus saada aikaan täydellinen yhdenmukaistaminen[31] (ja korkeatasoinen suoja), käytännössä se saatettiin jäsenvaltioissa eri tavoin osaksi kansallista lainsäädäntöä. Tämän vuoksi EU:ssa laadittiin erilaisia tietosuojasääntöjä, joiden määritelmiä ja sääntöjä tulkittiin eri tavoin kansallisissa laeissa. Myös valvonnan tasot ja seuraamusten ankaruus olivat erilaisia eri jäsenvaltioissa. Lisäksi tietotekniikassa oli tapahtunut huomattavia muutoksia sen jälkeen, kun direktiivi oli laadittu 1990-luvun puolivälissä. Kaikkien näiden syiden vuoksi EU:n tietosuojalainsäädäntöä oli uudistettava.

Uudistus johti vuosia kestäneiden tiiviiden keskustelujen jälkeen yleisen tietosuoja-asetuksen antamiseen huhtikuussa 2016. Keskustelut siitä, että EU:n tietosuojasääntöjä on uudistettava, alkoivat vuonna 2009, kun komissio käynnisti julkisen kuulemisen henkilötietojen suojaa koskevan perusoikeuden tulevasta oikeudellisesta kehyksestä. Komissio julkaisi ehdotuksen asetukseksi tammikuussa 2012. Siitä alkoi neuvotteluihin perustuva pitkä lainsäädäntöprosessi Euroopan parlamentin ja Euroopan unionin neuvoston välillä. Yleisessä tietosuoja-asetuksessa oli sen antamisen jälkeen kahden vuoden siirtymäaika. Sitä alettiin soveltaa täysimääräisesti 25. toukokuuta 2018, kun tietosuojadirektiivi kumottiin.

Yleisen tietosuoja-asetuksen antamisella vuonna 2016 uudistettiin EU:n tietosuojalainsäädäntöä, josta tehtiin perusoikeuksien suojeluun soveltuva digitaaliajan taloudelliset ja sosiaaliset haasteet huomioon ottaen. Yleisessä tietosuoja-asetuksessa säilytetään tietosuojadirektiivissä säädetyt ydinperiaatteet ja rekisteröidyn oikeudet sekä kehitetään niitä. Siinä on myös otettu käyttöön uusia velvoitteita, joiden mukaan organisaation on toteutettava sisäänrakennettu ja oletusarvoinen tietosuoja, nimitettävä joissakin olosuhteissa tietosuojavastaava, noudatettava uutta oikeutta tietojen siirtämisestä järjestelmästä toiseen sekä osoitusvelvollisuuden periaatetta. EU:n lainsäädännön mukaan asetuksia sovelletaan suoraan eikä kansallista täytäntöönpanoa tarvita. Yleisestä tietosuoja-asetuksesta saadaan niin ollen yhdet yhtenäiset tietosuojasäännöt koko EU:hun. Näin koko EU:ssa on yhdenmukaiset tietosuojasäännöt, joilla saadaan aikaan oikeusvarmuus, joka voi hyödyttää talouden toimijoita ja yksityishenkilöitä ”rekisteröityinä”.

31 EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011, 29 kohta.

Vaikka yleistä tietosuoja-asetusta sovelletaan suoraan, jäsenvaltioiden odotetaan kuitenkin saattavan voimassa olevat kansalliset tietosuojalakinsa ajan tasalle siten, että ne ovat täysin asetuksen mukaisia. Johdanto-osan 10 kappaleessa jäsenvaltioille annetaan myös liikkumavaraa tiettyjen säännösten osalta. Asetuksessa vahvistetut keskeiset säännöt ja periaatteet ja siinä yksityishenkilöille myönnetyt vahvat oikeudet muodostavat suuren osan käsikirjasta. Ne esitetään seuraavissa luvuissa. Asetuksessa on kattavat säännöt alueellisesta soveltamisalasta. Se koskee EU:hun sijoittautuneita yrityksiä, ja sen lisäksi se koskee EU:n ulkopuolelle sijoittautuneita rekisterinpitäjiä ja henkilötietojen käsittelijöitä, jotka tarjoavat tavaroita tai palveluja rekisteröidyille EU:ssa tai seuraavat näiden käyttäytymistä EU:ssa. Koska useilla ulkomaisilla teknologiayrityksillä on keskeinen osuus Euroopan markkinoilla ja miljoonia asiakkaita EU:ssa, EU:n tietosuojasääntöjen soveltaminen näihin yrityksiin on tärkeää, jotta voidaan varmistaa yksityishenkilöiden suoja sekä taata tasapuoliset toimintaedellytykset.

Tietosuoja lainvalvonnassa – direktiivi (EU) 2016/680

Kumotussa tietosuojadirektiivissä säädettiin kokonaisvaltaisesta tietosuojajärjestelmästä. Tätä järjestelmää on nyt parannettu entisestään antamalla yleinen tietosuoja-asetus. Vaikka kumotun tietosuojadirektiivin soveltamisala oli kattava, se rajoittui sisämarkkinoihin kuuluviin toimiin ja muiden viranomaisten kuin lainvalvontaviranomaisten toimiin. Siksi oli annettava erityisiä säädöksiä, jotta tietosuojan ja muiden oikeutettujen etujen välille saataisiin selkeyttä ja tasapainoa ja jotta voitaisiin vastata tiettyjen alojen erityisen olennaisiin haasteisiin. Tämä koskee lainvalvontaviranomaisten tekemää tietojenkäsittelyä koskevia sääntöjä.

Ensimmäinen tätä asiaa sääntelevä EU:n säädös oli neuvoston puitepäätös 2008/977/YOS rikosasioissa tehtävässä poliisi- ja oikeudellisessa yhteistyössä käsiteltävien henkilötietojen suojaamisesta. Sen sääntöjä sovellettiin vain jäsenvaltioiden välillä vaihdettaviin tietoihin poliisi- ja oikeusasioista. Sen soveltamisalaan ei kuulunut lainvalvontaa varten kotimaassa tehty henkilötietojen käsittely.

Direktiivi (EU) 2016/680 luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten

seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta[32], johon viitataan poliisi- ja rikosoikeusviranomaisia koskevana tietosuojadirektiivinä, korjasi tämän tilanteen. Direktiivi annettiin rinnakkain yleisen tietosuoja-asetuksen kanssa, ja se kumosi puitepäätöksen 2008/977/YOS. Siinä vahvistettiin henkilötietojen suojan kokonaisvaltainen järjestelmä lainvalvonnassa ja otettiin huomioon yleiseen turvallisuuteen liittyvän tietojenkäsittelyn erityisominaisuudet. Kun yleisessä tietosuoja-asetuksessa säädetään yleisistä säännöistä henkilöiden suojelemiseksi henkilötietojen käsittelyssä ja kyseisten tietojen vapaan liikkumisen varmistamiseksi EU:ssa, direktiivissä esitetään tietosuojaa koskevia erityisiä sääntöjä rikosasioissa tehtävän oikeudellisen yhteistyön ja poliisiyhteistyön aloilla. Jos toimivaltainen viranomainen käsittelee henkilötietoja rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia varten, sovelletaan direktiiviä (EU) 2016/680. Jos toimivaltaiset viranomaiset käsittelevät henkilötietoja muita kuin edellä mainittuja tarkoituksia varten, sovelletaan yleisen tietosuoja-asetuksen yleistä järjestelmää. Edeltäjästään (neuvoston puitepäätös 2008/977/YOS) poiketen direktiivin (EU) 2016/680 soveltamisala yltää lainvalvontaviranomaisten kotimaassa tekemään henkilötietojen käsittelyyn eikä sitä rajoiteta kyseisten tietojen vaihtamiseen jäsenvaltioiden kesken. Direktiivin tarkoituksena on myös saada aikaan tasapaino yksilöiden oikeuksien ja turvallisuuteen liittyvän käsittelyn oikeutettujen etujen välillä.

Tätä varten direktiivissä varmistetaan oikeus henkilötietojen suojaan ja ydinperiaatteet, joiden on määrä kattaa tietojenkäsittely, noudattaen tarkasti yleisessä tietosuoja-asetuksessa vahvistettuja sääntöjä ja periaatteita. Yksilöiden oikeudet ja rekisterinpitäjille säädetyt velvollisuudet – esimerkiksi tietoturvan, sisäänrakennetun ja oletusarvoisen tietosuojan ja tietoturvaloukkauksia koskevien ilmoitusten osalta – muistuttavat yleisen tietosuoja-asetuksen oikeuksia ja velvollisuuksia. Direktiivissä otetaan myös huomioon vakavat kehittyvät teknologiset haasteet, joilla voi olla erityisen raskas vaikutus yksilöihin, kuten lainvalvontaviranomaisten käyttämät profilointitekniikat, ja pyritään puuttumaan niihin. Periaatteessa ainoastaan automaattiseen käsittelyyn, myös profilointiin, perustuvat päätökset on kiellettävä[33]. Ne eivät myöskään saa perustua arkaluonteisiin tietoihin. Näihin periaatteisiin sovelletaan

32 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta, EUVL L 119, 4.5.2016.

33 Poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin 11 artiklan 1 kohta.

tiettyjä direktiivissä säädettyjä poikkeuksia. Tällainen käsittely ei myöskään saa johtaa yhdenkään henkilön syrjintään[34].

Direktiivissä on myös sääntöjä rekisterinpitäjien osoitusvelvollisuuden varmistamiseksi. Niiden on nimettävä tietosuojavastaava, joka valvoo tietosuojasääntöjen noudattamista, antaa yhteisölle ja käsittelyä tekeville työntekijöille tietoa ja neuvontaa näiden velvollisuuksista ja tekee yhteistyötä valvontaviranomaisen kanssa. Henkilötietojen käsittelyä poliisi- ja rikosoikeusalalla valvovat nyt riippumattomat valvontaviranomaiset. Sekä yleisessä tietosuojan oikeudellisessa järjestelmässä että lainvalvonnan ja rikosasioiden erityisessä tietosuojajärjestelmässä on noudatettava yhtä lailla EU:n perusoikeuskirjan vaatimuksia.

Poliisi- ja rikosoikeusviranomaisia koskevassa tietosuojadirektiivissä vahvistettu erityisjärjestelmä poliisiyhteistyössä ja oikeudellisessa yhteistyössä tehtävää tietojenkäsittelyä varten kuvataan yksityiskohtaisesti luvussa 8.

Sähköisen viestinnän tietosuojadirektiivi

Myös sähköisen viestinnän alalla erityiset tietosuojasäännöt katsottiin välttämättömiksi. Internetin, kiinteän verkon ja mobiilipuhelinverkon kehittymisen myötä oli tärkeää varmistaa, että käyttäjien oikeuksia yksityisyyteen ja luottamuksellisuuteen kunnioitetaan. Direktiivissä 2002/58/EY[35] henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (direktiivi yksityisyyden suojasta ja sähköisestä viestinnästä tai sähköisen viestinnän tietosuojadirektiivi) asetetaan säännöt henkilötietojen turvallisuudesta näissä verkoissa, henkilötietojen tietoturvaloukkauksista ilmoittamisesta ja viestinnän luottamuksellisuudesta.

Turvallisuuden takaamiseksi sähköisten viestintäpalvelujen tarjoajien on muun muassa varmistettava, että tietojen saanti rajoitetaan ainoastaan luvansaaneisiin henkilöihin, ja toteutettava toimenpiteitä, joilla estetään henkilötietojen tuhoutuminen, katoaminen tai tahaton vahingoittuminen[36]. Jos verkon turvallisuuteen kohdistuu erityinen riski, tarjoajien on ilmoitettava tilaajille riskistä[37]. Jos tietoturvaa loukataan toteutetuista turvatoimenpiteistä huolimatta, palveluntarjoajien on ilmoitettava

34 *Ibid.*, 11 artiklan 2 ja 3 kohta.

35 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, EYVL L 201 (direktiivi yksityisyyden suojasta ja sähköisestä viestinnästä tai sähköisen viestinnän tietosuojadirektiivi).

36 Sähköisen viestinnän tietosuojadirektiivi, 4 artiklan 1 kohta.

37 *Ibid.*, 4 artiklan 2 kohta.

henkilötietojen tietoturvaloukkauksesta toimivaltaiselle kansalliselle viranomaiselle, joka vastaa direktiivin täytäntöönpanosta ja valvonnasta. Palveluntarjoajien on myös ilmoitettava henkilötietojen tietoturvaloukkauksista yksilöille siinä tapauksessa, että loukkaus vaikuttaa todennäköisesti kielteisesti heidän henkilötietoihinsa tai yksityisyyteensä[38]. Viestinnän luottamuksellisuus edellyttää, että viestinnän ja metatietojen kuuntelu, salakuuntelu, tallentaminen tai muunlaiset telepakkokeinot tai valvonta kielletään periaatteessa. Direktiivissä myös kielletään ei-toivottu viestintä (johon viitataan usein ”roskapostina”), elleivät käyttäjät ole antaneet siihen suostumustaan. Siinä on myös sääntöjä evästeiden tallentamisesta tietokoneille ja laitteille. Näistä negatiivisista ydinvelvoitteista käy selkeästi ilmi, että viestinnän luottamuksellisuus liittyy tiiviisti perusoikeuskirjan 7 artiklassa vahvistetun yksityis- ja perhe-elämän kunnioitusta koskevan oikeuden ja 8 artiklassa vahvistetun henkilötietojen suojaa koskevan oikeuden suojaamiseen.

Komissio julkaisi tammikuussa 2017 ehdotuksen asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä. Sen tarkoituksena on korvata sähköisen viestinnän tietosuojadirektiivi. Uudistuksen tavoitteena on mukauttaa sähköistä viestintää koskevia sääntöjä yleisessä tietosuoja-asetuksessa vahvistettuun uuteen tietosuojajärjestelmään. Uusi asetus on suoraan sovellettavissa koko EU:ssa; kaikkien yksilöiden sähköisen viestinnän suoja on samalla tasolla, ja televiestintäpalvelujen tarjoajat ja alan toimijat hyötyvät selkeydestä, oikeusvarmuudesta ja yksistä yhtenäisistä säännöistä koko EU:ssa. Sähköisen viestinnän luottamuksellisuudesta ehdotettuja sääntöjä sovelletaan myös uusiin toimijoihin, jotka tarjoavat sähköisen viestinnän palveluja, jotka eivät kuulu sähköisen viestinnän tietosuojadirektiivin soveltamisalaan. Direktiivi kattoi vain perinteisten televiestintäpalvelujen tarjoajat. Kun viestien lähettämiseen tai soittamiseen käytetään jatkuvasti enemmän Skypen, WhatsAppin, Facebook Messengerin ja Viberin kaltaisia palveluja, nämä internetissä tapahtuvassa jakelussa käytettävät palvelut (ns. over-the-top- eli OTT-palvelut) kuuluvat nyt asetuksen soveltamisalaan, ja niiden on noudatettava sen tietosuojaa, yksityisyyden suojaa ja tietoturvaa koskevia vaatimuksia. Sähköisen viestinnän sääntöjä koskeva lainsäädäntöprosessi oli tämän käsikirjan julkaisemisen aikana edelleen käynnissä.

Asetus (EY) N:o 45/2001

Koska tietosuojadirektiiviä voitiin soveltaa vain EU:n jäsenvaltioihin, tarvittiin toinen säädös varmistamaan tietosuoja, kun henkilötietoja käsitellään EU:n toimielimissä ja

38 *Ibid.*, 4 artiklan 3 kohta.

elimissä. Asetus (EY) N:o 45/2001 yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EU:n toimielinten tietosuoja-asetus)[39], täyttää tämän tehtävän.

Asetuksessa (EY) N:o 45/2001 noudatetaan tarkasti EU:n yleisen tietosuojajärjestelmän periaatteita, ja siinä sovelletaan kyseisiä periaatteita tietojenkäsittelyyn, jota EU:n toimielimet ja elimet tekevät tehtäviään suorittaessaan. Asetuksella perustetaan lisäksi riippumaton valvontaviranomainen, Euroopan tietosuojavaltuutettu (EDPS), valvomaan sen säännösten soveltamista. Euroopan tietosuojavaltuutetulle on annettu valvontavaltuudet ja velvollisuus valvoa henkilötietojen käsittelyä EU:n toimielimissä ja elimissä sekä ottaa vastaan ja tutkia valitukset tietosuojasääntöjen väitetyistä rikkomisista. Viranomainen myös antaa EU:n toimielimille ja elimille neuvontaa kaikista henkilötietojen suojaa koskevista asioista, muun muassa uusista lainsäädäntöehdotuksista ja tietojenkäsittelyyn liittyvien sisäisten sääntöjen laatimisesta.

Euroopan komissio antoi tammikuussa 2017 ehdotuksen uudeksi asetukseksi tietojenkäsittelystä EU:n toimielimissä. Se kumoaa nykyisen asetuksen. Sähköisen viestinnän tietosuojadirektiivin uudistuksen tavoin asetuksen (EY) N:o 45/2001 uudistuksella uudistetaan sen sääntöjä ja mukautetaan ne yleisen tietosuoja-asetuksen nojalla luotuun uuteen tietosuojajärjestelmään.

Euroopan unionin tuomioistuimen tehtävä

Euroopan unionin tuomioistuimella on lainkäyttövalta määritettäessä, onko jäsenvaltio täyttänyt EU:n tietosuojalainsäädännön mukaiset velvollisuutensa, ja tulkittaessa EU:n lainsäädäntöä, jotta voidaan varmistaa sen tehokas ja yhtenäinen soveltaminen kaikissa jäsenvaltioissa. Sen jälkeen, kun tietosuojadirektiivi annettiin vuonna 1995, on kertynyt huomattava määrä oikeuskäytäntöä, joka selkeyttää tietosuojaperiaatteiden sekä perusoikeuskirjan 8 artiklassa vahvistetun henkilötietojen suojaa koskevan oikeuden soveltamisalaa ja merkitystä. Vaikka direktiivi on kumottu ja uusi säädös – yleinen tietosuoja-asetus – on nyt voimassa, voimassa oleva oikeuskäytäntö on edelleen asiaankuuluvaa ja pätevää EU:n tietosuojaperiaatteiden tulkinnassa ja soveltamisessa siinä määrin, että tietosuojadirektiivin ydinperiaatteet ja -käsitteet on säilytetty yleisessä tietosuoja-asetuksessa.

39 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001, L 8.

1.2 Henkilötietojen suojaa koskevan oikeuden rajoitukset

Keskeiset kohdat

- Oikeus henkilötietojen suojaan ei ole ehdoton oikeus. Sitä voidaan tarvittaessa rajoittaa yleisen edun vuoksi tai toisten ihmisten oikeuksien ja vapauksien suojelemiseksi.
- Yksityis- ja perhe-elämän kunnioitusta ja henkilötietojen suojaa koskevien oikeuksien rajoittamisen ehdot luetellaan ihmisoikeussopimuksen 8 artiklassa ja perusoikeuskirjan 52 artiklan 1 kohdassa. Niitä on kehitetty ja tulkittu Euroopan ihmisoikeustuomioistuimen ja Euroopan unionin tuomioistuimen oikeuskäytännössä.
- Euroopan neuvoston tietosuojalainsäädännön mukaan henkilötietojen käsittely on lainmukaista puuttumista yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen, ja se voidaan tehdä vain, jos
  - siitä säädetään lailla
  - sillä on laillinen tarkoitus
  - siinä noudatetaan perusoikeuksien ja -vapauksien keskeistä sisältöä
  - se on oikeasuhteista ja välttämätöntä demokraattisessa yhteiskunnassa laillisen tarkoituksen saavuttamiseksi.
- EU:n oikeusjärjestelmässä asetetaan samanlaisia ehtoja perusoikeuskirjassa suojattujen perusoikeuksien käytön rajoituksille. Kaikki perusoikeuksien, myös henkilötietojen suojan, rajoitukset voivat olla lainmukaisia vain, jos
  - niistä on säädetty lailla
  - niissä noudatetaan oikeuden keskeistä sisältöä
  - ne ovat välttämättömiä suhteellisuusperiaatteen mukaisesti ja
  - ne vastaavat unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Perusoikeuskirjan 8 artiklan mukainen perusoikeus henkilötietojen suojaan ei kuitenkaan ole ehdoton oikeus, ”vaan se on suhteutettava siihen tehtävään, joka sillä on yhteiskunnassa”[40]. Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoi-

40 Ks. esim. EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010, 48 kohta.

keuskirjan 7 ja 8 artiklassa tunnustetun kaltaisten oikeuksien käyttämistä voidaan rajoittaa, jos näistä rajoituksista säädetään lailla, jos niissä kunnioitetaan kyseisten oikeuksien ja vapauksien olennaista sisältöä ja jos ne suhteellisuusperiaatteen mukaisesti ovat välttämättömiä ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia[41]. Euroopan ihmisoikeussopimuksessa tietosuoja taataan puolestaan 8 artiklassa, ja sitä koskevan oikeuden käyttämistä voidaan rajoittaa tarvittaessa oikeutetun tavoitteen saavuttamiseksi. Tässä osassa viitataan ihmisoikeussopimuksen mukaisiin puuttumista koskeviin ehtoihin, joita on tulkittu ihmisoikeustuomioistuimen oikeuskäytännössä, sekä perusoikeuskirjan 52 artiklan mukaisiin lainmukaisia rajoituksia koskeviin ehtoihin.

1.2.1 Edellytykset Euroopan ihmisoikeussopimuksen mukaiselle oikeutetulle puuttumiselle oikeuden käyttämiseen

Henkilötietojen käsittely voi olla puuttumista rekisteröidyn oikeuteen nauttia yksityis- ja perhe-elämän kunnioitusta, joka suojataan ihmisoikeussopimuksen 8 artiklassa[42]. Kuten edellä on selitetty (ks. 1.1.1 kohta ja 1.1.4 kohta), EU:n oikeusjärjestelmästä poiketen ihmisoikeussopimuksessa ei vahvisteta henkilötietojen suojaa erilliseksi perusoikeudeksi. Sen sijaan henkilötietojen suoja kuuluu oikeuksiin, joita suojataan oikeudella nauttia yksityis- ja perhe-elämän kunnioitusta. Näin ollen mikä tahansa toiminta, johon kuuluu henkilötietojen käsittelyä, ei voi kuulua ihmisoikeussopimuksen 8 artiklan soveltamisalaan. Sen 8 artiklan soveltaminen edellyttää, että ensin on määritettävä, onko yksityinen etu tai henkilön yksityiselämä vaarantunut. Euroopan ihmisoikeustuomioistuin on koko oikeuskäytännössään käsitellyt ”yksityis- ja perhe-elämää” laajana käsitteenä, johon kuuluu näkökohtia myös työelämästä ja julkisesta käyttäytymisestä. Se on myös todennut, että henkilötietojen suoja on tärkeä osa yksityis- ja perhe-elämän kunnioitusta koskevaa oikeutta. Yksityis- ja perhe-elämän laajasta tulkinnasta huolimatta mikä tahansa käsittely ei sellaisenaan vaaranna 8 artiklalla suojattuja oikeuksia.

Jos ihmisoikeustuomioistuin katsoo, että kyseessä oleva käsittelytoimi vaikuttaa yksilön oikeuteen nauttia yksityis- ja perhe-elämän kunnioitusta, se tutkii, onko

41 *Ibid.*, 50 kohta.

42 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 8.12.2008, 67 kohta.

puuttuminen perusteltua. Oikeus yksityis- ja perhe-elämän kunnioitukseen ei ole ehdoton oikeus, vaan sitä on punnittava muita oikeutettuja etuja ja oikeuksia vasten ja se on saatettava tasapainoon niiden kanssa. Tämä koskee sekä muiden henkilöiden etuja (yksityisiä etuja) että koko yhteiskunnan etuja (julkisia etuja).

Puuttumista voidaan perustella seuraavilla kumulatiivisilla ehdoilla:

Lainmukaisuus

EIT:n oikeuskäytännön nojalla oikeuteen puuttuminen on lainmukaista, jos se perustuu kansalliseen lakiin, joka täyttää tietyt vaatimukset. Lain on oltava asianomaisten henkilöiden saatavilla ja sen seurausten on oltava ennakoitavia[43]. Sääntöä pidetään ennakoitavana, jos se on muotoiltu niin selkeästi, että jokainen voi – tarvittaessa asianmukaisella opastuksella – noudattaa sitä toiminnassaan[44]. Lailta tässä yhteydessä vaadittu täsmällisyys riippuu aihealueesta[45].

Esimerkkejä: Asiassa *Rotaru v. Romania*[46] kantaja väitti, että hänen oikeuttaan nauttia yksityis- ja perhe-elämän kunnioitusta rikottiin, koska Romanian tiedustelupalvelun rekisterissä käytettiin hänen henkilötietojaan sisältävää tiedostoa. EIT totesi, että vaikka Romanian laki salli kansalliseen turvallisuuteen vaikuttavien salaisten tiedostojen keräämisen, tallentamisen ja arkistoimisen, siinä ei asetettu näille viranomaisten harkintavaltaan jätetyille valtuuksille mitään rajoituksia. Kansallisessa lainsäädännössä ei esimerkiksi määritelty, minkä tyyppisiä tietoja voitiin käsitellä, mihin ihmisryhmiin valvontatoimia saatettiin kohdistaa, missä olosuhteissa toimenpiteitä voitiin toteuttaa tai mitä menettelyjä oli noudatettava. Siksi tuomioistuin totesi, että kansallinen laki ei täyttänyt ihmisoikeussopimuksen 8 artiklassa määrättyä ennakoitavuuden vaatimusta ja että kyseistä artiklaa oli rikottu.

43 EIT, *Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 16.2.2000, 50 kohta; ks. myös EIT, *Kopp v. Sveitsi*, nro 23224/94, 25.3.1998, 55 kohta, ja EIT, *Iordachi ym. v. Moldova*, nro 25198/02, 10.2.2009, 50 kohta.

44 EIT, *Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 16.2.2000, 56 kohta; ks. myös EIT, *Malone v. Yhdistynyt kuningaskunta*, nro 8691/79, 2.8.1984, 66 kohta; EIT, *Silver ym. v. Yhdistynyt kuningaskunta*, nrot 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25.3.1983, 88 kohta.

45 EIT, *The Sunday Times v. Yhdistynyt kuningaskunta*, nro 6538/74, 26.4.1979, 49 kohta; ks. myös EIT, *Silver ym. v. Yhdistynyt kuningaskunta*, nrot 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25.3.1983, 88 kohta.

46 EIT, *Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000, 57 kohta; ks. myös EIT, *Association for European Integration and Human Rights ja Ekimdzhiev v. Bulgaria*, nro 62540/00, 28.6.2007; EIT, *Shimovolos v. Venäjä*, nro 30194/09, 21.6.2011; ja EIT, *Vetter v. Ranska*, nro 59842/00, 31.5.2005.

Asiassa *Taylor-Sabori v. Yhdistynyt kuningaskunta*[47] kantaja oli ollut poliisivalvonnan kohteena. Poliisi oli kohdistanut kantajaan telepakkokeinoja käyttämällä tämän hakulaitteen ”kloonia”. Kantaja oli myöhemmin pidätetty ja asetettu syytteeseen osallisuudesta huumekauppaan. Osa syyttäjän aineistosta koostui poliisin puhtaaksikirjoittamista hakulaitteen viesteistä. Kantajan oikeudenkäynnin aikaan Yhdistyneessä kuningaskunnassa ei kuitenkaan ollut lainsäädäntöä, jolla olisi säännelty yksityisten televiestintäjärjestelmien kautta lähetettyihin viesteihin kohdistuneita pakkokeinoja. Näin ollen kantajan oikeuksiin puuttuminen ei ollut tapahtunut ”lainmukaisesti”. EIT totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Asiassa *Vukota-Bojić v. Sveitsi*[48] oli kyse siitä, että vakuutusyhtiön palkkaamat yksityisetsivät seurasivat salaa naista, joka haki korvausta sosiaalivakuutuksesta. Tuomioistuin katsoi, että vaikka kantelun kohteena olleen valvonnan oli tilannut yksityinen vakuutusyhtiö, kyseinen yhtiö oli kuitenkin saanut valtiolta oikeuden tarjota pakollisesta sairausvakuutuksesta johtuvia etuuksia ja kerätä vakuutusmaksuja. Valtio ei voinut väistää sopimuksen mukaista vastuutaan siirtämällä velvollisuutensa yksityisille elimille tai henkilöille. Kansallisessa lainsäädännössä oli annettava riittävät takeet väärinkäytöltä, jotta ihmisoikeussopimuksen 8 artiklan mukaisiin oikeuksiin puuttuminen on lainmukaista. Tuomioistuin katsoi tässä asiassa, että ihmisoikeussopimuksen 8 artiklaa oli rikottu, koska kansallisessa lainsäädännössä ei ollut ilmaistu riittävän selkeästi laajuutta ja tapaa, jolla julkisina viranomaisina toimiville vakuutusyhtiöille siirrettyä harkintavaltaa voidaan käyttää vakuutuskiistoissa vakuutetun salaista seurantaa varten. Siinä ei etenkään ollut riittäviä takeita väärinkäyttöä vastaan.

Laillinen tarkoitus

Laillinen tarkoitus voi olla jompikumpi mainituista julkisista eduista tai muiden henkilöiden oikeuksien ja vapauksien suojeleminen. Puuttumisen oikeuttavia laillisia tarkoituksia voivat olla ihmisoikeussopimuksen 8 artiklan 2 kohdan mukaisesti kansalliseen ja yleiseen turvallisuuteen tai maan taloudelliseen hyvinvointiin liittyvät edut, epäjärjestyksen tai rikollisuuden estäminen, terveyden tai moraalin suojaaminen ja muiden henkilöiden oikeuksien ja vapauksien turvaaminen.

47 EIT, *Taylor-Sabori v. Yhdistynyt kuningaskunta*, nro 47114/99, 22.10.2002.

48 EIT, *Vukota-Bojić v. Sveitsi*, nro 61838/10, 18.10.2016, 77 kohta.

Esimerkki: Asiassa *Peck v. Yhdistynyt kuningaskunta*[49] kantaja oli yrittänyt tehdä itsemurhan kadulla viiltämällä ranteensa, mutta hän ei ollut huomannut, että valvontakamera oli tallentanut tämän yrityksen. Kun poliisit, jotka olivat seuranneet valvontakameraa, olivat pelastaneet hänet, poliisiviranomainen luovutti valvontakameran kuvaaman aineiston tiedotusvälineille, jotka julkaisivat sen peittämättä kantajan kasvoja. Euroopan ihmisoikeustuomioistuin katsoi, ettei viranomaisilla ollut merkittävää tai riittävää syytä luovuttaa aineistoa yleisölle pyytämättä kantajalta lupaa tai peittämättä hänen henkilöllisyyttään. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Välttämättömyys demokraattisessa yhteiskunnassa

Euroopan ihmisoikeustuomioistuin on todennut, että välttämättömyyden käsite edellyttää, että oikeuteen puuttuminen on vastaus pakottavaan yhteiskunnalliseen tarpeeseen ja erityisesti että se on oikeassa suhteessa lailliseen tarkoitukseen[50]. Arvioidessaan, onko toimenpide välttämätön pakottavan yhteiskunnallisen tarpeen käsittelemiseksi, ihmisoikeustuomioistuin tutkii sen merkitystä ja soveltuvuutta tavoitteena olevan päämäärän kannalta. Siinä se voi ottaa huomioon, pyritäänkö puuttumisella ratkaisemaan ongelma, jolla voisi olla haitallinen vaikutus yhteiskuntaan, jos siihen ei puututa, tai onko näyttöä siitä, että puuttuminen voi lieventää kyseistä haitallista vaikutusta, ja mitä laajempia yhteiskunnallisia näkökohtia kysymykseen liittyy.[51] Esimerkiksi se, että turvallisuuspalvelut keräävät ja tallentavat sellaisten yksilöiden henkilötietoja, joilla on havaittu olevan yhteyksiä terroristiliikkeisiin, olisi puuttumista yksilöiden oikeuteen nauttia yksityis- ja perhe-elämän kunnioituksesta. Sillä kuitenkin vastattaisiin vakavaan ja pakottavaan yhteiskunnalliseen tarpeeseen: kansalliseen turvallisuuteen ja terrorismin torjuntaan. Välttämättömyystestin läpäisemiseksi puuttumisen on myös oltava oikeasuhteista. Ihmisoikeustuomioistuimen oikeuskäytännössä oikeasuhteisuus kuuluu välttämättömyyden käsitteeseen. Oikeasuhteisuus edellyttää, että ihmisoikeussopimuksella suojattuihin oikeuksiin ei puututa enempää kuin on tarpeen laillisen tarkoituksen saavuttamiseksi. Oikeasuhteisuutta testattaessa on tärkeää ottaa huomioon puuttumisen laajuus, erityisesti se, miten moneen ihmiseen se vaikuttaa, ja takeet tai vastalauseet,

49 EIT, *Peck v. Yhdistynyt kuningaskunta*, nro 44647/98, 28.1.2003, 85 kohta.

50 EIT, *Leander v. Ruotsi*, nro 9248/81, 26.3.1987, 58 kohta.

51 Yksilöiden suojelua henkilötietojen käsittelyssä koskevan työryhmän (tietosuojatyöryhmä) (2014), *lausunto välttämättömyys- ja oikeasuhteisuuskäsitteiden soveltamisesta ja tietosuojasta lainvalvonta-alalla*, WP 211, Bryssel, 27.2.2014, s. 7–8.

jotka ovat käytössä puuttumisen laajuuden tai yksilöiden oikeuksiin kohdistuvien haitallisten vaikutusten rajoittamiseksi.[52]

Esimerkki: Asiassa *Khelili v. Sveitsi*[53] poliisi huomasi tarkastuksen yhteydessä, että kantajalla oli käyntikortteja, joissa luki: ”Kaunis kolmekymppinen nainen haluaisi tavata miehen, jonka kanssa voisi joskus käydä lasillisella tai ulkona. Puhelinnumero – –”. Kantaja väitti, että poliisi oli löytönsä jälkeen kirjannut naisen poliisirekisteriin prostituoituna, vaikka tämä kielsi harjoittavansa kyseistä ammattia. Kantaja vaati, että sana ”prostituoitu” poistetaan poliisirekisteristä. EIT myönsi, että periaatteessa henkilötietojen säilyttäminen sillä perusteella, että henkilö voisi syyllistyä toiseen rikokseen, saattoi olla joissakin olosuhteissa oikeasuhteista. Kantajan tapauksessa väite laittomasta prostituutiosta vaikutti kuitenkin liian epämääräiseltä ja yleisluonteiselta, eikä sen tueksi ollut konkreettista näyttöä, sillä kantajaa ei ollut koskaan tuomittu laittomasta prostituutiosta, joten väitettä ei näin ollen voitu perustella pakottavalla yhteiskunnallisella tarpeella ihmisoikeussopimuksen 8 artiklassa tarkoitetulla tavalla. Tuomioistuin otti huomioon kantajan oikeuksiin puuttumisen vakavuuden ja katsoi, että oli viranomaisten tehtävä todistaa kantajasta säilytettyjen tietojen todenmukaisuus. Näin ollen tuomioistuin totesi, ettei sanan ”prostituoitu” säilyttäminen poliisirekisterissä vuosien ajan ollut välttämätöntä demokraattisessa yhteiskunnassa. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Esimerkki: Asioissa *S. ja Marper v. Yhdistynyt kuningaskunta*[54] molemmat kantajat oli pidätetty ja asetettu syytteeseen rikoksista. Poliisi otti heidän sormenjälkensä ja dna-tunnisteensa poliisista ja rikostodisteista annetun säädöksen mukaisesti. Kantajia ei kuitenkaan koskaan tuomittu rikoksista. Tuomioistuin totesi toisen syyttömäksi ja toista vastaan aloitettu rikosoikeudenkäynti keskeytettiin. Poliisi oli kuitenkin tallentanut ja säilönyt heidän sormenjälkensä, dna-tunnisteensa ja solunäytteensä tietokantaan. Kansallisen säädöksen nojalla niitä voitiin säilyttää rajattomasti. Vaikka Yhdistynyt kuningaskunta väitti, että tietojen säilyttäminen auttoi tulevien rikoksentekijöiden tunnistamisessa, jolloin laillisena tarkoituksena oli rikosten estäminen ja paljastaminen, ihmisoikeustuomioistuin katsoi, että puuttuminen hakijoiden oikeuteen nauttia yksityis- ja perhe-elämän kunnioitusta oli perusteeton. Se

52 *Ibid.*, s. 9–11.

53 EIT, *Khelili v. Sveitsi*, nro 16188/07, 18.10.2011.

54 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008.

muistutti, että tietosuojan ydinperiaatteet edellyttävät, että henkilötietojen säilyttäminen on oikeassa suhteessa keräämisen tarkoitukseen ja että säilytysaikoja on rajoitettava. Tuomioistuin myönsi, että tietokannan laajentaminen tuomittujen henkilöiden dna-profiilien lisäksi kaikkiin epäiltyihin henkilöihin, joita ei ollut tuomittu, olisi voinut auttaa rikosten estämisessä ja paljastamisessa Yhdistyneessä kuningaskunnassa. Sen mielestä kyseessä kuitenkin oli säilytysvaltuuksien yleisyys ja valikoimattomuus[55].

Koska solunäytteissä on runsaasti geeni- ja terveystietoja, puuttuminen hakijoiden yksityiselämää koskevaan oikeuteen oli erityisen tunkeilevaa. Sormenjälkiä ja näytteitä voitiin ottaa pidätetyiltä henkilöitä ja säilyttää niitä ilman määräaikaa poliisin tietokannassa riippumatta rikoksen luonteesta ja vakavuudesta. Tämä päti jopa pieniin rikoksiin, joista ei anneta vankeusrangaistusta. Lisäksi syyttömiksi todetuilla henkilöillä oli vain rajoitettu mahdollisuus pyytää henkilötietojensa poistamista. EIT kiinnitti erityistä huomiota myös siihen, että toinen kantaja oli pidätyksen aikaan vasta 11-vuotias. Alaikäisen, jota ei ole tuomittu, henkilötietojen säilyttäminen voi olla erityisen haitallista tämän haavoittuvuuden vuoksi ja siksi, että sillä on merkitystä hänen kehitykselleen ja integroitumiselleen yhteiskuntaan[56]. Tuomioistuin katsoi yksimielisesti, että tietojen säilyttäminen muodosti suhteettoman puuttumisen kantajien oikeuteen nauttia yksityiselämänsä kunnioitusta eikä sitä voitu katsoa välttämättömäksi demokraattisessa yhteiskunnassa.

Esimerkki: Asiassa *Leander v. Ruotsi*[57] EIT katsoi, että kansallisen turvallisuuden kannalta tärkeisiin tehtäviin hakevien henkilöiden salainen tutkiminen ei itsessään ollut vastoin vaatimusta, joka koski välttämättömyyttä demokraattisessa yhteiskunnassa. Kansallisessa lainsäädännössä rekisteröityjen etujen suojelemiseksi säädetyt erityiset suojatoimet – kuten parlamentin ja oikeuskanslerin harjoittama valvonta – saivat EIT:n päätymään siihen johtopäätökseen, että Ruotsissa käytössä ollut työntekijöiden tarkastusjärjestelmä täytti ihmisoikeussopimuksen 8 artiklan 2 kohdan vaatimukset. Laajan harkintavaltansa ansiosta vastaajana ollut valtio saattoi oikeutetusti katsoa, että kantajan tapauksessa kansallisen turvallisuuden edut menivät yksilön etujen edelle. Tuomioistuin totesi, ettei ihmisoikeussopimuksen 8 artiklaa ollut rikottu.

55 *Ibid.*, 119 kohta.

56 *Ibid.*, 124 kohta.

57 EIT, *Leander v. Ruotsi*, nro 9248/81, 26.3.1987, 59 ja 67 kohta.

1.2.2 EU:n perusoikeuskirjassa määritellyt edellytykset oikeuden lailliselle rajoittamiselle

Perusoikeuskirjan rakenne ja sanamuoto ovat erilaiset kuin ihmisoikeussopimuksen. Perusoikeuskirjassa ei mainita puuttumista turvattuihin oikeuksiin, mutta siinä on määräys, jonka nojalla voidaan rajoittaa perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien käyttöä.

Perusoikeuskirjan 52 artiklan 1 kohdan mukaan perusoikeuskirjassa tunnustettujen oikeuksien ja vapauksien – kuten henkilötietojen suojaa koskevan oikeuden – käyttämistä voidaan rajoittaa ainoastaan, jos rajoitukset

- on säädetty lailla; ja
- ne noudattavat tietosuojaa koskevan oikeuden olennaista sisältöä; ja
- ne ovat välttämättömiä suhteellisuusperiaatteen mukaisesti;[58] ja
- ne vastaavat unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Koska henkilötietojen suoja on perusoikeuskirjan 8 artiklalla suojattu erillinen ja itsenäinen perusoikeus EU:n oikeusjärjestelmässä, kaikki henkilötietojen käsittely on sellaisenaan puuttumista tähän oikeuteen. On merkityksetöntä, liittyvätkö kyseiset henkilötiedot yksilön yksityis- ja perhe-elämään, ovatko ne arkaluonteisia tai onko rekisteröidyille aiheutunut jollakin tavalla hankaluutta. Puuttumisen lainmukaisuus edellyttää, että sen on noudatettava kaikkia perusoikeuskirjan 52 artiklan 1 kohdassa lueteltuja ehtoja.

Rajoituksista on säädetty lailla

Henkilötietojen suojaa koskevan oikeuden rajoituksista täytyy säätää lailla. Tämä vaatimus edellyttää, että rajoitusten täytyy perustua oikeusperustaan, joka on asianmukaisesti saatavilla ja jonka seuraukset ovat ennakoitavia. Se on myös pitänyt muotoilla riittävän selkeästi, että jokainen voi ymmärtää velvoitteensa ja noudattaa sitä toiminnassaan. Oikeusperustassa on myös selkeästi määritettävä tapa, jolla toimivaltaiset viranomaiset voivat käyttää valtuuksiaan yksilöiden

58 Henkilötietojen suojaa koskevaa perusoikeutta rajoittavien toimenpiteiden välttämättömyyden arvioinnista on tietoa sitä koskevissa ohjeissa: EDPS (2017), *Necessity Toolkit*, Bryssel, 11.4.2017.

suojelemiseksi mielivaltaiselta puuttumiselta, sekä valtuuksien soveltamisala. Tämä tulkinta muistuttaa EIT:n oikeuskäytännön mukaista vaatimusta ”lainmukaisesta puuttumisesta”[59]. Onkin katsottu, että perusoikeuskirjassa käytetyllä ilmaisulla ”ainoastaan lailla” olisi oltava vastaavanlainen ulottuvuus kuin kyseisellä ilmaisulla on Euroopan ihmisoikeussopimuksen yhteydessä[60]. Unionin tuomioistuimen on otettava EIT:n oikeuskäytäntö ja etenkin sen vuosien mittaan rakentama oikeuden käsite huomioon tulkitessaan perusoikeuskirjan 52 artiklan 1 kohdan ulottuvuutta[61].

Oikeuden keskeisen sisällön noudattaminen

EU:n oikeusjärjestyksessä kaikissa perusoikeuskirjalla suojattujen perusoikeuksien rajoituksissa on noudatettava kyseisten oikeuksien keskeistä sisältöä. Se tarkoittaa, että rajoitukset, joiden laajuuden ja tunkeilevuuden vuoksi perusoikeus menettää perussisältönsä, eivät ole perusteltuja. Jos oikeuden keskeinen sisältö vaarantuu, rajoitus on katsottava lainvastaiseksi, eikä silloin tarvitse enää arvioida, palveleeko se yleistä etua koskevaa tavoitetta ja täyttääkö se tarpeellisuus- ja oikeasuhteisuuskriteerit.

Esimerkki: Asia *Schrems*[62] koski yksilöiden suojelua henkilötietojen siirrossa kolmansiin maihin, tässä tapauksessa Yhdysvaltoihin. Maximillian Schrems, joka on Itävallan kansalainen ja joka oli ollut Facebookin käyttäjä useita vuosia, teki Irlannin tietosuojavaltuutetulla kantelun, jossa hän vaati tätä kieltämään Facebookin irlantilaista tytäryhtiötä siirtämästä hänen henkilötietojaan Facebook Inc:lle ja Yhdysvalloissa sijaitseville palvelimille, joissa henkilötietoja käsitellään. Hänen mielestään Yhdysvalloissa voimassa olevat oikeussäännöt ja käytännöt eivät takaa Yhdysvaltojen alueella säilytetyille henkilötiedoille riittävää suojaa. Hän viittasi tässä yhteydessä paljastuksiin, jotka Edward Snowden, yhdysvaltalainen väärinkäytösten paljastaja, oli tehnyt vuonna 2013 Yhdysvaltojen tiedustelupalvelujen tiedustelutoimista.

59 EDPS (2017), *Necessity Toolkit*, Bryssel, 11.4.2017, s. 4; ks. myös EUT, *tuomioistuimen lausunto 1/15 (suuri jaosto)*, 26.7.2017.

60 EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen ja Secretary of State for the Home Department v. Tom Watson, Peter Brice, Geoffrey Lewis, julkisasiamiehen Saugmandsgaard Øen ratkaisuehdotus*, 19.7.2016, 140 kohta.

61 EUT, C-70/10, *Scarlet Extended SA v. Société belge des auteurs compositeurs et éditeurs (SABAM), julkisasiamies Cruz Villalónin* ratkaisuehdotus,14.4.2011, 100 kohta.

62 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

Snowden oli paljastanut, että kansallinen turvallisuusvirasto National Security Agency oli salakuunnellut suoraan Facebookin kaltaisten yritysten palvelimia ja pystynyt lukemaan chat-keskustelujen ja yksityisviestien sisältöä.

Tietojen siirrot Yhdysvaltoihin perustuivat komission vuonna 2000 tekemään päätökseen tietosuojan tason riittävyydestä. Sen nojalla tietoja pystyttiin siirtämään yhdysvaltalaisille yrityksille, jotka ilmoittavat suojaavansa EU:sta siirrettyjä henkilötietoja ja noudattavansa niin sanottuja safe harbor -periaatteita. Kun asia tuli Euroopan unionin tuomioistuimen käsiteltäväksi, se tutki komission päätöksen pätevyyden perusoikeuskirjan perusteella. Se muistutti, että perusoikeuksien suojaa EU:ssa koskevat poikkeukset ja rajoitukset toteutetaan sen rajoissa, mikä on ehdottomasti tarpeen. Euroopan unionin tuomioistuin katsoi, että säännöstöllä, jonka nojalla viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön, ”loukataan yksityiselämän kunnioitusta koskevan perusoikeuden, sellaisena kuin se taataan perusoikeuskirjan 7 artiklassa, keskeistä sisältöä”. Oikeus jäisi täysin merkityksettömäksi, jos Yhdysvaltojen valtion viranomaisten sallittaisiin päästä sähköiseen viestintään sattumanvaraisesti ilman mitään sellaisia objektiivisia perusteluja, jotka perustuisivat kansallista turvallisuutta tai rikollisuuden ehkäisemistä koskeviin asianomaiseen henkilöön erikseen liittyviin konkreettisiin syihin, ja ilman tällaisiin käytäntöihin liittyviä riittäviä takeita vallan väärinkäyttöä vastaan.

Unionin tuomioistuin katsoi myös, että ”säännöstö, jossa yksityisille ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi”, ei ole tehokasta oikeussuojaa ja puolueetonta tuomioistuinta koskevan oikeuden (perusoikeuskirjan 47 artikla) mukainen. Näin ollen safe harbor -päätöksellä ei pystytty Yhdysvalloissa varmistamaan perusoikeuksien suojan sellaista tasoa, joka pääosiltaan vastaa tasoa, joka taataan unionissa direktiivin nojalla, kun sitä tulkitaan perusoikeuskirjan valossa. Siksi Euroopan unionin tuomioistuin totesi päätöksen pätemättömäksi.[63]

63 Euroopan unionin tuomioistuimen päätös todeta komission päätös 520/2000/EY pätemättömäksi perustui myös muihin syihin, joita käsitellään tämän käsikirjan muissa osissa. Tuomioistuin katsoi erityisesti, että päätös rajoitti lainvastaisesti kansallisten tietosuojan valvontaviranomaisten valtuuksia. Safe harbor -järjestelmässä ei myöskään ollut yksilöiden saatavilla oikeussuojakeinoja, jos he olisivat halunneet tutustua henkilötietoihinsa ja/tai saada ne oikaistuksi tai poistetuksi. Näin ollen vaarannettiin myös perusoikeuskirjan 47 artiklassa vahvistettu perusoikeus tehokkaisiin oikeussuojakeinoihin ja puolueettomaan tuomioistuimeen

Esimerkki: Asiassa *Digital Rights Ireland*[64] Euroopan unionin tuomioistuin tutki direktiivin 2006/24/EY (tietojen säilyttämistä koskeva direktiivi) yhteensopivuutta perusoikeuskirjan 7 ja 8 artiklan kanssa. Direktiivillä velvoitetaan sähköiset viestintäpalvelut säilyttämään liikenne- ja paikkatietoja vähintään kuusi kuukautta ja enintään 24 kuukautta ja antamaan toimivaltaisille viranomaisille oikeus saada kyseisiä tietoja vakavien rikosten torjuntaa, tutkintaa, selvittämistä ja syyteharkintaa varten. Direktiivissä ei anneta lupaa sähköisen viestinnän sisällön säilyttämiseen. Euroopan unionin tuomioistuin pani merkille, että tiedot, joita palvelujen tarjoajien on säilytettävä, ovat muun muassa viestinnän lähteen ja kohteen jäljittämiseksi ja tunnistamiseksi tarvittavat tiedot, viestinnän päivämäärä, kellonaika ja kesto sekä soittajan puhelinnumero ja valittu numero sekä IP-protokollaosoite. Näiden tietojen ”kokonaisuus voi mahdollistaa hyvin tarkkojen päätelmien tekemisen niiden henkilöiden, joiden tietoja on säilytetty, yksityiselämästä, kuten elämäntavoista, vakituisista tai väliaikaisista oleskelupaikoista, päivittäisestä tai muusta liikkumisesta, tekemisestä sekä näiden henkilöiden sosiaalisista suhteista ja heidän sosiaalisesta ympäristöstään”.

Näin ollen direktiivin mukainen henkilötietojen säilyttäminen merkitsi erityisen vakavaa puuttumista yksityis- ja perhe-elämän kunnioitusta ja henkilötietojen suojaa koskeviin oikeuksiin. Tuomioistuin kuitenkin katsoi, että puuttuminen ei ole omiaan aiheuttamaan haittaa kyseisten oikeuksien sisällölle. Yksityis- ja perhe-elämän kunnioitusta koskevan oikeuden sisältöä ei vaarannettu, koska direktiivissä ei sallita tiedon saamista sähköisen viestinnän sisällöstä sellaisenaan. Myöskään henkilötietojen suojaa koskevan oikeuden keskeinen sisältö ei vaarantunut, koska direktiivin mukaan sähköisten viestintäpalvelujen tarjoajien on noudatettava tiettyjä tietosuojaa ja tietoturvaa koskevia periaatteita ja suoritettava tietojen suojaamiseksi asianmukaisia teknisiä ja organisatorisia toimia.

Välttämättömyys ja oikeasuhteisuus

Perusoikeuskirjan 52 artiklan 1 kohdassa säädetään, että suhteellisuusperiaatteen mukaisesti perusoikeuskirjassa tunnustettuihin perusoikeuksiin voidaan tehdä rajoituksia ainoastaan, jos ne ovat välttämättömiä.

64 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

Rajoitus voi olla **välttämätön**, jos tavoitteena olevan yleisen edun saavuttamiseksi on toteutettava toimenpiteitä. Välttämättömyys kuitenkin edellyttää Euroopan unionin tuomioistuimen tulkinnan mukaan, että toteutettavat toimenpiteet ovat lievempiä kuin muut vaihtoehdot saman tavoitteen saavuttamiseen. Yksityis- ja perhe-elämän kunnioitusta ja henkilötietojen suojaa koskevien oikeuksien rajoittamisessa Euroopan unionin tuomioistuin soveltaa tiukkaa välttämättömyystestiä ja katsoo, että ”poikkeukset ja rajoitukset on toteutettava täysin välttämättömän rajoissa”. Jos rajoitus katsotaan täysin välttämättömäksi, on myös arvioitava, onko se oikeasuhteinen.

Oikeasuhteisuus tarkoittaa, että rajoituksesta saatavien etujen on oltava suurempia kuin haitat, joita se aiheuttaa kyseessä olevien perusoikeuksien käyttämiselle[65]. Rajoitusten on tärkeää sisältää riittävät suojatoimet, jotta voidaan vähentää haittoja ja riskejä yksityis- ja perhe-elämän kunnioitusta ja henkilötietojen suojaa koskevien oikeuksien käyttämiselle.

Esimerkki: Asiassa *Volker und Markus Schecke*[66] Euroopan unionin tuomioistuin totesi, että neuvosto ja komissio ovat ylittäneet suhteellisuusperiaatteen noudattamisen rajat säätäessään kaikkien luonnollisten henkilöiden, jotka ovat tiettyjen maatalousrahastojen tuensaajia, henkilötietojen julkaisemisesta tekemättä eroa sellaisten merkityksellisten kriteerien mukaan kuin ajanjaksot, joina kyseiset henkilöt ovat saaneet tällaisia tukia, niiden toistuvuus tai niiden laji ja suuruus.

Tästä syystä tuomioistuin piti tarpeellisena todeta pätemättömiksi tietyt neuvoston asetuksen (EY) N:o 1290/2005 säännökset ja asetuksen (EY) N:o 259/2008 kokonaisuudessaan.[67]

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

66 EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010, 89 ja 86 kohta.

67 Neuvoston asetus (EY) N:o 1290/2005, annettu 21 päivänä kesäkuuta 2005, yhteisen maatalouspolitiikan rahoituksesta, EUVL 2005, L 209; komission asetus (EY) N:o 259/2008, annettu 18 päivänä maaliskuuta 2008, neuvoston asetuksen (EY) N:o 1290/2005 soveltamista koskevista yksityiskohtaisista säännöistä Euroopan maatalouden tukirahaston (maataloustukirahaston) ja Euroopan maaseudun kehittämisen maatalousrahaston (maaseuturahaston) varoja saavia tuensaajia koskevien tietojen julkaisemisen osalta, EUVL 2008, L 76.

Esimerkki: Asiassa *Digital Rights Ireland*[68] Euroopan unionin tuomioistuin katsoi, että tietojen säilyttämistä koskevasta direktiivistä johtuva puuttuminen yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen ei vaarantanut kyseisen oikeuden keskeistä sisältöä, koska direktiivissä kiellettiin sähköisen viestinnän sisällön säilyttäminen. Se katsoi kuitenkin, että direktiivi ei ollut yhteensopiva perusoikeuskirjan 7 ja 8 artiklan kanssa, ja totesi sen pätemättömäksi. Koska liikenne- ja paikkatiedot voitaisiin koota ja niitä voitaisiin käsitellä kokonaisuutena, niitä voitaisiin analysoida ja laatia yksityiskohtainen kuva yksilöiden yksityiselämästä, joten se merkitsi erityisen vakavaa puuttumista näihin oikeuksiin. Euroopan unionin tuomioistuin otti huomioon, että direktiivissä velvoitetaan kaikkien kiinteän puhelimen, matkapuhelimen, internetyhteyden, internetsähköpostin ja internetpuhelimen liikennetietojen säilyttämiseen. Näin ollen direktiivi koskee kaikkia sellaisia sähköisiä viestintävälineitä, joiden käyttö on hyvin laajaa jokaisen jokapäiväisessä elämässä. Käytännössä se merkitsi puuttumista, joka vaikuttaa lähes kaikkiin Euroopan asukkaisiin. Unionin tuomioistuimen mukaan liikenne- ja paikkatietojen säilyttäminen voisi tämän puuttumisen laajuuden ja vakavuuden vuoksi olla perusteltua vain vakavan rikollisuuden torjumiseksi. Direktiivissä ei myöskään säädetty objektiivisesta perusteesta, jonka nojalla voitaisiin varmistaa, että toimivaltaisten kansallisten viranomaisten oikeus saada säilytettäviä tietoja rajoittuu täysin välttämättömään. Direktiivi ei myöskään sisällä aineellisia ja menettelyllisiä edellytyksiä, joiden perusteella kansalliset viranomaiset voivat saada säilytettäviä tietoja ja käyttää niitä, eikä se edellytä joko tuomioistuimen tai itsenäisen hallinnollisen yksikön etukäteistä tarkastusta.

Euroopan unionin tuomioistuin päätyi samanlaiseen johtopäätökseen yhdistetyissä asioissa *Tele2 Sverige AB v. Post- och telestyrelsen* ja *Secretary of State for the Home Department v. Tom Watson ym.*[69] Ne koskivat kaikkien tilaajien ja rekisteröityjen käyttäjien liikenne- ja paikkatietoja ja ”kaikkia sähköisiä viestintävälineitä ja kaikkia liikennetietoja” eikä säännöstö tee ”erottelua eikä aseta rajoituksia tai poikkeuksia asetetun tavoitteen perusteella”[70]. Tässä asiassa se, oliko henkilö suoraan tai epäsuorasti yhteydessä vakaviin rikoksiin vai ei tai oliko hänen viestintänsä merkityksellistä

68 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014, 39 kohta.

69 EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB v. Post- och telestyrelsen ja Secretary of State for the Home Department v. Tom Watson* ym. [suuri jaosto], 21.12.2016, 105–106 kohta.

70 *Ibid.*, 105 kohta.

kansallisen turvallisuuden kannalta vai ei, ei ollut edellytys hänen tietojensa säilyttämiselle. Koska säilytettävien tietojen ja yleistä turvallisuutta koskevaa uhkaa tai ajanjaksoa tai maantieteellisesti määriteltyjä alueita koskevien rajoitusten välillä ei ollut vaadittua yhteyttä, Euroopan unionin tuomioistuin katsoi, että kansallinen säännöstö ylitti täysin välttämättömän rajat vakavan rikollisuuden torjunnassa[71].

Euroopan tietosuojavaltuutettu on omaksunut samanlaisen lähestymistavan aiheeseen *välttämättömyyttä käsittelevissä ohjeissaan*[72]. Ohjeiden tarkoituksena on auttaa arvioimaan ehdotettujen toimenpiteiden yhdenmukaisuutta tietosuojaa koskevan EU:n lainsäädännön kanssa. Ohjeet laadittiin, jotta asiasta vastaavat EU:n päättäjät ja lainsäätäjä saisivat entistä paremmat valmiudet laatia tai tarkistaa toimenpiteitä, joihin kuuluu henkilötietojen käsittelyä ja joilla rajoitetaan henkilötietojen suojaa koskevaa oikeutta ja muita perusoikeuskirjassa vahvistettuja oikeuksia ja vapauksia.

Yleisen edun mukaiset tavoitteet

Kaikkien perusoikeuskirjassa tunnustettujen oikeuksien harjoittamisen rajoitusten on myös aidosti vastattava unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia, jotta ne olisivat perusteltuja. Muiden henkilöiden oikeuksien ja vapauksien suojelun tarpeen osalta henkilötietojen suojaa koskeva oikeus toimii usein vuorovaikutuksessa muiden perusoikeuksien kanssa. Tällaisesta vuorovaikutuksesta esitetään yksityiskohtainen analyysi 1.3 kohdassa. Yleisen edun mukaisiin tavoitteisiin kuuluvat Euroopan unionista tehdyn sopimuksen 3 artiklassa vahvistetut EU:n yleiset tavoitteet, kuten rauhan ja EU:n kansojen hyvinvoinnin edistäminen, yhteiskunnallisen oikeudenmukaisuuden ja sosiaalisen suojelun edistäminen, sellaisen vapauden, turvallisuuden ja oikeuden alueen luominen, jolla taataan henkilöiden vapaa liikkuvuus yhdessä sellaisten asianmukaisten toimenpiteiden kanssa, joilla ehkäistään ja torjutaan rikollisuutta, sekä muut perussopimusten erityismääräyksillä suojatut tavoitteet ja edut.[73] Yleisessä tietosuoja-asetuksessa täsmennetään lisää perusoikeuskirjan 52 artiklan 1 kohtaa tältä kannalta: asetuksen 23 artiklan 1 kohdassa luetellaan joukko yleisen edun mukaisia tavoitteita, jotka katsotaan oikeutetuiksi syiksi rajoittaa yksilöiden oikeuksia, jos rajoituksessa noudatetaan keskeisiltä osin henkilötietojen suojaa

71 *Ibid.*, 107 kohta.

72 EDPS (2017), *Necessity Toolkit*, Bryssel, 11.4.2017.

73 Euroopan unionin perusoikeuskirjan selitykset (2007/C 303/02), EUVL 2007, C 303, s. 17–35.

koskevaa oikeutta ja se on välttämätön ja oikeasuhteinen toimenpide. Mainittuja yleisen edun mukaisia tavoitteita ovat muun muassa kansallinen turvallisuus ja puolustus, rikosten ennalta estäminen, unionille tai jäsenvaltiolle tärkeä taloudellinen tai rahoituksellinen etu, kansanterveys ja sosiaaliturva.

Yleisen edun mukainen tavoite, johon rajoituksella pyritään, on määritettävä ja selitettävä riittävän tarkasti, koska rajoituksen välttämättömyyttä arvioidaan sen perusteella. Rajoituksen tavoitteen ja ehdotettujen toimenpiteiden selkeä ja yksityiskohtainen kuvaus on ratkaisevan tärkeää, jotta sen välttämättömyys voidaan arvioida[74]. Tavoite, johon pyritään, ja rajoituksen välttämättömyys ja oikeasuhteisuus liittyvät tiiviisti toisiinsa.

Esimerkki: Asia *Schwarz v. Stadt Bochum*[75] koski yksityiselämän kunnioitusta koskevan oikeuden ja henkilötietojen suojaa koskevan oikeuden rajoituksia, jotka aiheutuvat sormenjälkien ottamisesta ja tallentamisesta, kun jäsenvaltion viranomaiset myöntävät passeja[76]. Kantaja haki Bochumin kaupungilta (Stadt Bochum) passia, mutta kieltäytyi antamasta sormenjälkiään, minkä vuoksi Bochumin kaupunki hylkäsi hänen passihakemuksensa. Hän nosti sitten kanteen saksalaisessa tuomioistuimessa vaatien, että passi annettaisiin ilman, että häneltä otettaisiin sormenjäljet. Saksalainen tuomioistuin esitti Euroopan unionin tuomioistuimelle ennakkoratkaisupyynnön, jossa se kysyi, onko jäsenvaltioiden myöntämien passien ja matkustusasiakirjojen turvatekijöitä ja biometriikkaa koskevista vaatimuksista annetun asetuksen (EY) N:o 2252/2004 1 artiklan 2 kohta pätevä.

Euroopan unionin tuomioistuin huomautti, että sormenjäljet **ovat henkilötietoja**, koska ne objektiivisesti sisältävät luonnollisia henkilöitä koskevia ainutkertaisia tietoja ja mahdollistavat heidän täsmällisen tunnistamisensa, ja että sormenjälkien ottaminen ja tallentaminen on käsittelyä. Kyseinen käsittely, johon sovelletaan asetuksen (EY) N:o 2252/2004 1 artiklan 2 kohtaa, on uhka oikeudelle nauttia yksityiselämän kunnioitusta ja oikeudelle henkilötietojen suojaan.[77] Perusoikeuskirjan 52 artiklan 1 kohdassa kuitenkin sallitaan näiden oikeuksien käyttämisen rajoittaminen, kunhan näistä rajoituksista säädetään lailla kyseisten oikeuksien keskeistä sisältöä

74 EDPS (2017), *Necessity Toolkit*, Bryssel, 11.4.2017, s. 4.

75 EUT, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17.10.2013.

76 *Ibid.*, 33–36 kohta.

77 *Ibid.*, 27–30 kohta.

kunnioittaen ja kunhan ne suhteellisuusperiaatteen mukaisesti ovat tarpeellisia ja vastaavat tosiasiallisesti unionin tunnustamia yleisen edun mukaisia tavoitteita tai tarvetta suojella muiden henkilöiden oikeuksia ja vapauksia.

Tässä asiassa Euroopan unionin tuomioistuin pani ensinnäkin merkille, että passien myöntämiseen liittyvästä sormenjälkien ottamisesta ja tallentamisesta aiheutuvasta rajoituksesta on katsottava **säädetyn lailla**, koska näistä toimenpiteistä säädetään asetuksen (EY) N:o 2252/2004 1 artiklan 2 kohdassa. Toiseksi asetuksen tavoitteena on passien väärentämisen ehkäiseminen ja niiden väärinkäytön estäminen. Asetuksen 1 artiklan 2 kohdalla pyritään näin ollen muun muassa estämään laiton saapuminen unionin alueelle eli sillä pyritään unionin hyväksymään yleisen edun mukaiseen tavoitteeseen. Kolmanneksi unionin tuomioistuimen käytettävissä olleista tiedoista ei ilmennyt eikä asiassa myöskään ollut väitetty, että käsiteltävässä asiassa tarkoitetuilla rajoituksilla ei kunnioitettaisi näiden oikeuksien keskeistä sisältöä. Neljänneksi sormenjälkien tallentaminen kyseisessä säännöksessä tarkoitettuun erittäin turvalliseen tallennusvälineeseen edellyttää teknistä kehittyneisyyttä. Tällaisella tallentamisella saatetaan vähentää passien väärentämisriskiä ja helpottaa niiden aitoutta EU:n rajoilla tutkivien viranomaisten tehtävää. Määräävää ei ole se, ettei kyseinen menetelmä ole täysin luotettava. Vaikka sillä ei täysin suljetakaan pois sitä, että maahan päästetään henkilöitä, joilla ei ole tähän lupaa, riittää, että sillä vähennetään huomattavasti tällaisen maahanpääsyn riskiä. Edellä esitetyn nojalla Euroopan unionin tuomioistuin totesi, että asetuksen (EY) N:o 2252/2004 1 artiklan 2 kohdassa tarkoitetut sormenjälkien ottaminen ja tallentaminen soveltuivat kyseisellä asetuksella olevien tavoitteiden ja näin ollen sen päämäärän toteuttamiseen, joka on henkilöiden laittoman unionin alueelle saapumisen estäminen.[78]

Seuraavaksi Euroopan unionin tuomioistuin arvioi, onko kyseinen käsittely **tarpeellista**, ja muistutti, että kyseessä olevalla toimella tarkoitetaan vain kahden sormenjäljen ottamista. Sormet ovat lisäksi yleensä muiden henkilöiden nähtävillä, joten kyse ei ole intiimiluonteisesta toimenpiteestä. Samoin kuin kasvokuvan ottamisella, silläkään ei aiheuteta asianomaiselle erityistä fyysistä tai psyykkistä haittaa. Toisaalta on syytä todeta, että unionin tuomioistuimessa käydyssä oikeudenkäynnissä esille tuotu ainoa todellinen vaihtoehto sormenjälkien ottamiselle on kuvan ottaminen silmän

78 *Ibid.*, 35–45 kohta.

värikalvosta. Unionin tuomioistuimelle esitetyssä asiakirja-aineistossa ei ollut seikkoja, jotka olisivat osoittaneet, että viimeksi mainitulla menettelyllä loukattaisiin perusoikeuskirjan 7 ja 8 artiklassa tunnustettuja oikeuksia vähemmän kuin sormenjälkien ottamisella. Kahden mainitun menetelmän tehokkuudesta on lisäksi todettava, että on kiistatonta, että värikalvon tunnistamiseen pohjautuvan menetelmän teknologinen valmius ei yllä samalle tasolle sormenjälkiin pohjautuvan menetelmän kanssa. Värikalvon tunnistamismenettely on lisäksi tällä hetkellä huomattavasti sormenjälkien vertailumenetelmää kalliimpi, ja tästä syystä se soveltuu huonommin yleiseen käyttöön. Unionin tuomioistuimen tietoon ei myöskään ollut saatettu, että olemassa olisi toimenpiteitä, joilla riittävän tehokkaasti voitaisiin myötävaikuttaa sen tavoitteen toteuttamiseen, joka on passien suojaaminen väärinkäyttöä vastaan, ja joilla samalla loukattaisiin perusoikeuskirjan 7 ja 8 artiklassa tunnustettuja oikeuksia vähemmän kuin sormenjälkien ottamiseen pohjautuvalla menetelmällä.[79]

Euroopan unionin tuomioistuin totesi, että asetuksen (EY) N:o 2252/2004 4 artiklan 3 kohdassa täsmennetään nimenomaisesti, että sormenjälkiä saadaan käyttää ainoastaan passin aitouden toteamiseksi ja sen haltijan henkilöllisyyden varmistamiseksi, kun taas asetuksen 1 artiklan 2 kohdan mukaan sormenjäljet tallennetaan vain itse passiin, joka jää haltijansa yksinomaiseen hallintaan. Asetuksessa ei näin ollen säädetä oikeusperustasta sen perusteella kerättyjen tietojen keskittämiselle tai käyttämiselle muihin tarkoituksiin kuin siihen, joka on pyrkiä estämään henkilöiden laiton pääsy unionin alueelle.[80] Kaikkien edellä esitettyjä näkökohtien nojalla Euroopan unionin tuomioistuin totesi, ettei ennakkoratkaisukysymystä tutkittaessa tullut esille asetuksen (EY) N:o 2252/2004 1 artiklan 2 kohdan pätevyyteen vaikuttavia seikkoja.

Perusoikeuskirjan ja Euroopan ihmisoikeussopimuksen (ECHR) välinen suhde

Erilaisesta sanamuodosta huolimatta perusoikeuskirjan 52 artiklan 1 kohdassa tarkoitetut oikeuksien lainmukaisia rajoituksia koskevat ehdot tuovat mieleen ihmisoikeussopimuksen oikeutta yksityis- ja perhe-elämän kunnioituksesta nauttimiseen koskevan 8 artiklan 2 kohdan. Euroopan unionin tuomioistuin ja Euroopan

79 EUT, C-291/12, *Michael Schwarz v. Stadt Bochum*, 17.10.2013, 46–53 kohta.

80 *Ibid.*, 56–61 kohta.

ihmisoikeustuomioistuin viittaavat oikeuskäytännössään usein toistensa tuomioihin. Se kuuluu tuomioistuinten väliseen vuoropuheluun, jonka tavoitteena on tietosuojasääntöjen sopusointuinen tulkinta. Perusoikeuskirjan 52 artiklan 3 kohdassa todetaan seuraavaa: ”Siltä osin kuin tämän perusoikeuskirjan oikeudet vastaavat ihmisoikeuksien ja perusvapauksien suojaamista koskevassa eurooppalaisessa yleissopimuksessa taattuja oikeuksia, niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa.” Perusoikeuskirjan 8 artikla ei kuitenkaan vastaa suoraan mitään ihmisoikeussopimuksen artiklaa[81]. Perusoikeuskirjan 52 artiklan 3 kohta koskee kummassakin oikeusjärjestyksessä suojattujen oikeuksien sisältöä ja soveltamisalaa eikä niiden rajoittamisen ehtoja. Kun kyse on kahden tuomioistuimen laajemmasta vuoropuhelusta ja yhteistyöstä, Euroopan unionin tuomioistuin voi kuitenkin ottaa analyyseissaan huomioon ihmisoikeussopimuksen 8 artiklan mukaiset lainmukaista rajoittamista koskevat kriteerit sellaisina kuin Euroopan ihmisoikeustuomioistuin on niitä tulkinnut. Ihmisoikeustuomioistuin voi puolestaan viitata perusoikeuskirjan mukaisiin lainmukaista rajoittamista koskeviin ehtoihin. Joka tapauksessa olisi myös otettava huomioon, että perusoikeuskirjan 8 artiklassa ei ole ihmisoikeussopimuksessa täydellistä vastinetta, joka viittaa henkilötietojen suojaan ja erityisesti rekisteröidyn oikeuksiin, käsittelyn oikeutettuihin perusteisiin ja riippumattoman viranomaisen suorittamaan valvontaan. Joitakin perusoikeuskirjan 8 artiklan osatekijöitä on Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä, jota on kehitetty ihmisoikeussopimuksen 8 artiklan nojalla ja joka liittyy yleissopimukseen 108[82]. Tällä yhteydellä varmistetaan, että Euroopan unionin tuomioistuin ja Euroopan ihmisoikeustuomioistuin saavat toisiltaan vaikutteita tietosuojaa koskevissa asioissa.

1.3 Vuorovaikutus muiden oikeuksien ja oikeutettujen etujen kanssa

Keskeiset kohdat

- Oikeus tietosuojaan toimii usein vuorovaikutuksessa muiden oikeuksien kanssa, kuten sananvapauden ja tiedon vastaanottamista ja levittämistä koskevan oikeuden kanssa.

81 EDPS (2017), *Necessity Toolkit*, Bryssel, 11.4.2017, s. 6.

82 Euroopan unionin perusoikeuskirjan selitykset (2007/C 303/02), selitys 8 artiklaan.

- Tämä vuorovaikutus on usein ristiriitaista: joissakin tilanteissa henkilötietojen suojaa koskevan oikeuden ja jonkin toisen oikeuden välillä on jännitettä, kun taas joissakin tilanteissa oikeus henkilötietojen suojaan tosiasiallisesti varmistaa tuon toisen oikeuden kunnioittamisen. Tästä on kyse esimerkiksi sananvapauden osalta, koska vaitiolovelvollisuus on yksityiselämän kunnioitusta koskevan oikeuden osatekijä.
- Muiden henkilöiden oikeuksien ja vapauksien suojelun tarve on yksi kriteereistä, joita käytetään arvioimaan henkilötietojen suojaa koskevan oikeuden rajoittamisen lainmukaisuutta.
- Tuomioistuinten on punnittava eri oikeuksia, jotta ne voidaan sovittaa yhteen.
- Yleisen tietosuoja-asetuksen mukaan jäsenvaltioiden on sovitettava yhteen oikeus henkilötietojen suojaan sekä oikeus sananvapauteen ja tiedonvälityksen vapauteen.
- Jäsenvaltiot voivat myös antaa kansallisessa lainsäädännössä nimenomaisia sääntöjä, joilla sovitetaan yhteen oikeus henkilötietojen suojaan sekä virallisten asiakirjojen julkisuus ja vaitiolovelvollisuus.

Oikeus henkilötietojen suojaan ei ole ehdoton oikeus. Sen lainmukaisen rajoittamisen ehdoista on kerrottu edellä. Yksi sekä Euroopan neuvoston että Euroopan unionin oikeudessa tunnustettu peruste oikeuksien lainmukaisille rajoituksille on se, että puuttuminen tietosuojaan on välttämätöntä muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi. Kun tietosuoja on vuorovaikutuksessa muiden oikeuksien kanssa, sekä Euroopan ihmisoikeustuomioistuin että Euroopan unionin tuomioistuin ovat toistuvasti todenneet, että ihmisoikeussopimuksen 8 artiklan ja perusoikeuskirjan 8 artiklan soveltamisen ja tulkinnan yhteydessä on punnittava muitakin oikeuksia.[83] Tasapainon saavuttamisesta on useita tärkeitä esimerkkejä.

Tuomioistuinten tekemän punnitsemisen lisäksi valtiot voivat tarvittaessa antaa lainsäädäntöä, jolla oikeus henkilötietojen suojaan sovitetaan yhteen muiden oikeuksien kanssa. Tämän vuoksi yleisessä tietosuoja-asetuksessa säädetään useista kansallisten poikkeusten aloista.

Sananvapauden osalta jäsenvaltioiden on yleisen tietosuoja-asetuksen mukaan sovitettava lainsäädännöllä yhteen ”tämän asetuksen mukainen oikeus henkilötietojen suojaan sekä oikeus sananvapauteen ja tiedonvälityksen vapauteen, mukaan

83 EIT, *Von Hannover v. Saksa (nro 2)* [suuri jaosto], nrot 40660/08 ja 60641/08, 7.2.2012; EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 2411.2011, 48 kohta; EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 29.1.2008, 68 kohta.

lukien käsittely journalistisia tarkoituksia ja akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten"[84]. Jäsenvaltiot voivat myös antaa lakeja, joilla voidaan sovittaa yhteen tietosuoja sekä virallisten asiakirjojen julkisuus ja vaitiolovelvollisuus, jotka on suojattu yksityiselämän kunnioitusta koskevan oikeuden muotona[85].

1.3.1 Sananvapaus

Sananvapaus on yksi eniten tietosuojaa koskevan oikeuden kanssa vuorovaikutuksessa olevista oikeuksista.

Sananvapaus on turvattu perusoikeuskirjan 11 artiklassa ("Sananvapaus ja tiedonvälityksen vapaus"). Oikeus sisältää "mielipiteenvapauden sekä vapauden vastaanottaa ja levittää tietoja tai ajatuksia viranomaisten siihen puuttumatta ja alueellisista rajoista riippumatta". Sananvapauden ja tiedonvälityksen vapaudella turvataan sekä perusoikeuskirjan 11 artiklan että ihmisoikeussopimuksen 10 artiklan mukaan oikeus tietojen välittämisen lisäksi niiden *vastaanottamiseen*.

Sananvapauden rajoitusten on noudatettava perusoikeuskirjan 52 artiklan 1 kohdassa säädettyjä kriteereitä, jotka on kuvattu edellä. Lisäksi perusoikeuskirjan 11 artikla vastaa ihmisoikeussopimuksen 10 artiklaa. Perusoikeuskirjan 52 artiklan 3 kohdan mukaan, siltä osin kuin perusoikeuskirjan oikeudet vastaavat ihmisoikeussopimuksessa taattuja oikeuksia, "niiden merkitys ja kattavuus ovat samat kuin mainitussa yleissopimuksessa". Perusoikeuskirjan 11 artiklassa taatulle oikeudelle ei siis voida laillisesti asettaa rajoituksia, jotka menevät ihmisoikeussopimuksen 10 artiklan 2 kohdassa säädettyjä oikeuksia pidemmälle, toisin sanoen rajoituksista on säädettävä laissa ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa "muiden henkilöiden maineen tai oikeuksien turvaamiseksi". Nämä oikeudet kattavat erityisesti oikeuden nauttia yksityis- ja perhe-elämän kunnioituksesta ja oikeuden henkilötietojen suojaan.

Henkilötietojen suojaamisen ja sananvapauden välistä suhdetta säädellään yleisen tietosuoja-asetuksen 85 artiklalla, jonka otsikkona on "Käsittely ja sananvapaus ja tiedonvälityksen vapaus". Tämän artiklan mukaan jäsenvaltioiden on sovitettava yhteen oikeus henkilötietojen suojaan sekä oikeus sananvapauteen ja tiedonvälityksen vapauteen. Erityisesti käsittelylle journalistisia tarkoituksia varten tai akateemisen, taiteellisen tai kirjallisen ilmaisun tarkoituksia varten on säädettävä vapautuksia

84 Yleinen tietosuoja-asetus, 85 artikla.

85 *Ibid.*, 86 ja 90 artikla.

tai poikkeuksia yleisen tietosuoja-asetuksen tietyistä luvuista, jos ne ovat tarpeen henkilötietojen suojaa koskevan oikeuden sovittamiseksi yhteen sananvapauden ja tiedonvälityksen vapauden kanssa.

Esimerkki: Asiassa *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy*[86] Euroopan unionin tuomioistuinta pyydettiin määrittelemään tietosuojan suhde lehdistönvapauteen[87]. Tuomioistuimen piti tarkastella, miten Markkinapörssi ja Satamedia olivat levittäneet tekstiviestipalvelussa noin 1,2 miljoonan luonnollisen henkilön verotietoja, jotka ne olivat saaneet laillisesti Suomen veroviranomaisilta. Suomen tietosuojaviranomainen oli päätöksessään vaatinut yhtiötä lopettamaan näiden tietojen levittämisen. Markkinapörssi ja Satamedia kyseenalaistivat tämän päätöksen kansallisessa tuomioistuimessa, joka pyysi Euroopan unionin tuomioistuimelta selvennystä tietosuojadirektiivin tulkintaan. Tuomioistuimen piti erityisesti varmistaa, oliko veroviranomaisten saataville saattamien henkilötietojen käsittely siten, että matkapuhelinten käyttäjät voivat saada muiden luonnollisten henkilöiden verotietoja, katsottava yksinomaan journalistisia tarkoituksia varten toteutetuksi toiminnaksi. Todettuaan, että yhtiön toteuttama toiminta oli tietosuojadirektiivin 3 artiklan 1 kohdassa tarkoitettua ”henkilötietojen käsittelyä”, tuomioistuin siirtyi tulkitsemaan direktiivin 9 artiklaa (henkilötietojen käsittelystä ja ilmaisuvapaudesta). Tuomioistuin toi ensin esiin sananvapauden tärkeyden kaikissa demokraattisissa yhteiskunnissa ja jatkoi, että siihen liittyviä käsitteitä, journalismin käsite mukaan lukien, on tulkittava laajasti. Seuraavaksi tuomioistuin huomautti, että näiden kahden perusoikeuden välisen tasapainon löytämiseksi tietosuojaa koskevaan oikeuteen säädettyjä poikkeuksia ja rajoituksia on toteutettava vain täysin välttämättömän rajoissa. Asian olosuhteissa tuomioistuin katsoi, että Markkinapörssin ja Satamedian toteuttamien toimintojen kaltaisia toimintoja, jotka koskevat kansallisen lainsäädännön nojalla julkisista asiakirjoista peräisin olevia tietoja, voidaan pitää ”journalistisina toimintoina”, jos niiden tarkoituksena on tietojen, mielipiteiden tai ajatusten ilmaiseminen yleisölle millä tahansa

86 EUT, C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy* [suuri jaosto], 16.12.2008, 56, 61 ja 62 kohta.

87 Asia koski tietosuojadirektiivin 9 artiklan, joka nyt on korvattu yleisen tietosuoja-asetuksen 85 artiklalla, tulkintaa. Artiklassa todetaan seuraavaa: ”Jäsenvaltioiden on säädettävä ainoastaan journalistisia tarkoituksia tai taiteellisen tai kirjallisen ilmaisun tarkoituksia varten toteutettua henkilötietojen käsittelyä varten poikkeuksista ja vapautuksista tästä luvusta, IV luvusta ja VI luvusta, ainoastaan jos ne osoittautuvat välttämättömiksi yksityisyyttä koskevan oikeuden ja ilmaisuvapautta koskevien sääntöjen yhteensovittamisessa.”

tiedonsiirron välineellä. Tuomioistuin myös totesi, että näitä toimintoja eivät harjoita ainoastaan joukkotiedotusyritykset, ja ne voivat liittyä voiton tavoitteluun. Euroopan unionin tuomioistuin jätti kuitenkin kansallisen tuomioistuimen tehtäväksi arvioida, oliko tämä ollut tarkoituksena kyseisessä asiassa.

Myös Euroopan ihmisoikeustuomioistuin tutki samaa asiaa sen jälkeen, kun kansallinen tuomioistuin oli päättänyt Euroopan unionin tuomioistuimelta saatujen ohjeiden perusteella, että valvontaviranomaisen määräys lopettaa kaikkien verotietojen julkaisu oli oikeutettua puuttumista yhtiön sananvapauteen. Ihmisoikeustuomioistuin säilytti tämän lähestymistavan[88]. Se katsoi, että vaikka yhtiöiden oikeuteen välittää tietoja oli puututtu, puuttuminen oli lainmukaista, sillä oli laillinen tarkoitus ja se oli välttämätöntä demokraattisessa yhteiskunnassa.

Tuomioistuin muistutti oikeuskäytännön kriteereistä, joiden pitäisi ohjata kansallisia viranomaisia ja itse Euroopan ihmisoikeustuomioistuinta, kun sananvapautta punnitaan yksityiselämän kunnioittamista koskevan oikeuden kanssa. Kun kyse on poliittisesta puheesta tai yleistä etua koskevaa aihetta käsittelevästä keskustelusta, tiedon vastaanottamista ja välittämistä koskevan oikeuden rajoittamiseen on vain vähän mahdollisuuksia, koska yleisöllä on oikeus saada tietoa, ja se on olennainen oikeus demokraattisessa yhteiskunnassa[89]. Lehtiartikkeleiden, joiden ainoana tarkoituksena on tyydyttää tietyn lukijakunnan uteliaisuutta henkilön yksityiselämästä, ei voida kuitenkaan katsoa edistävän yleistä etua koskevaa keskustelua. Journalistisia tarkoituksia varten tietosuojasäännöistä tehdyn poikkeuksen tarkoituksena on antaa toimittajille mahdollisuus saada, kerätä ja käsitellä tietoa journalistisen toimintansa suorittamiseksi. Näin ollen olikin yleisen edun mukaista antaa kantelun tehneiden yhtiöiden kerätä ja käsitellä suuria määriä kyseessä olevia verotustietoja. Tuomioistuimen mielestä ei kuitenkaan ollut yleisen edun mukaista, että kyseistä käsittelemätöntä tietoa levitettiin sanomalehdissä lajittelematta, muuttamatta ja analysoimatta sitä mitenkään. Verotusta koskevat tiedot ovat saattaneet saada yleisön uteliaat jäsenet luokittelemaan yksilöitä näiden taloudellisen tilanteen perusteella, ja ne ovat ehkä tyydyttäneet yleisön tiedonjanoa muiden yksityiselämästä. Tämän ei voida katsoa edistävän yleisen edun mukaista keskustelua.

88 EIT, *Satakunnan Markkinapörssi Oy ja Satamedia Oy v. Suomi* [suuri jaosto], nro 931/13, 27.6.2017.

89 *Ibid.*, 169 kohta.

Esimerkki: Asiassa *Google Spain*[90] Euroopan unionin tuomioistuin pohti, pitikö Googlen poistaa kantajan taloudellisia vaikeuksia koskevat vanhentuneet tiedot hakutulosten luettelostaan. Kun Googlen hakukoneella tehtiin haku kantajan nimellä, sen tuloksena saatiin linkkejä vanhoihin sanomalehtiartikkeleihin, joissa mainittiin hänet konkurssimenettelyn yhteydessä. Kantaja katsoi tämän rikkovan hänen oikeuttaan yksityis- ja perhe-elämän kunnioitukseen ja henkilötietojen suojaan, koska menettely oli päättynyt vuosia sitten ja tällaiset viittaukset olivat merkityksettömiä.

Euroopan unionin tuomioistuin selvensi ensin, että internetin hakukoneiden ja henkilötietoja antavien hakutulosten avulla voidaan laatia yksityiskohtainen profiili yksilöstä. Koska yhteiskunta digitalisoituu jatkuvasti enemmän, vaatimus siitä, että henkilötiedot ovat täsmällisiä ja että niiden julkaisussa ei mennä pidemmälle kuin on välttämätöntä, eli jaetaan tietoja yleisölle, on olennaista yksilöiden tietosuojan korkean tason varmistamisessa. Hakukoneen ylläpitäjän on ”rekisterinpitäjänä varmistettava vastuidensa, valtuuksiensa ja mahdollisuuksiensa yhteydessä se, että käsittely täyttää [EU:n lainsäädännön] vaatimukset”, jotta takeet saavat täyden vaikutuksensa. Tämä tarkoittaa, että oikeus saada omat henkilötietonsa poistetuksi, kun käsittely ei ole enää välttämätöntä tai se on vanhentunutta, koskee myös hakukoneiden ylläpitäjiä, joiden katsotaan olevan rekisterinpitäjiä eikä pelkästään henkilötietojen käsittelijöitä (ks. 2.3.1 kohta).

Tutkiessaan, pitääkö Googlen poistaa kantajaan liittyvät linkit, Euroopan unionin tuomioistuin katsoi, että tietyissä olosuhteissa yksilöillä on oikeus saada henkilötietonsa poistetuksi internetin hakukoneen hakutuloksista. Tähän oikeuteen voidaan vedota, kun yksilöön liittyvät tiedot ovat virheellisiä, epäasianmukaisia tai epäolennaisia tai ne ovat liian laajoja siihen tarkoitukseen, jossa niitä käsitellään. Euroopan unionin tuomioistuin tunnusti, että tämä oikeus ei ole ehdoton. Sitä on punnittava suhteessa muihin oikeuksiin, erityisesti suureen yleisön etuun ja oikeuteen saada tietoa. Kaikki poistamispyynnöt on arvioitava tapauskohtaisesti, jotta saadaan tasapaino aikaan toisaalta rekisteröidyn henkilötietojen suojaa ja yksityis- ja perhe-elämän kunnioitusta koskevien perusoikeuksien ja toisaalta kaikkien internetin käyttäjien oikeutettujen etujen välillä. Tuomioistuin antoi ohjeita tekijöistä, jotka on otettava punninnassa huomioon. Kyseessä olevien tietojen luonne on

90 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 81–83 kohta.

erityisen tärkeä tekijä. Jos tiedot ovat arkaluonteisia yksilön yksityiselämän kannalta ja jos tietojen saatavuus ei ole yleisen edun mukaista, tietosuoja ja yksityisyydensuoja ohittaisivat suuren yleisön tiedonsaantioikeuden. Jos taas osoittautuu, että rekisteröity on julkisuuden henkilö tai että tietojen luonne oikeuttaa niiden antamisen suuren yleisön saataville, puuttuminen tietosuojaa ja yksityisyydensuojaa koskeviin perusoikeuksiin on oikeutettua.

Tietosuojatyöryhmä antoi tuomion perusteella ohjeet Euroopan unionin tuomioistuimen päätöksen täytäntöönpanosta. Ohjeissa on luettelo yleisistä kriteereistä, joita valvontaviranomaiset voivat käyttää käsitellessään kanteluita, jotka liittyvät yksilöiden esittämiin poistamispyyntöihin. Viranomaiset voivat käyttää kriteereitä myös ohjeina oikeuksien punninnassa.[91]

Euroopan ihmisoikeustuomioistuin on antanut useita tärkeitä ennakkopäätöksiä tietosuojaa koskevan oikeuden sovittamisesta yhteen sananvapauden kanssa.

Esimerkki: Asiassa *Axel Springer AG v. Saksa*[92] Euroopan ihmisoikeustuomioistuin katsoi, että kanteen esittäneelle yhtiölle annettu kieltomääräys, jolla estettiin kanteen esittänyttä yhtiötä julkaisemasta artikkelia tunnetun näyttelijän pidätyksestä ja tuomitsemisesta, rikkoi ihmisoikeussopimuksen 10 artiklaa. Tuomioistuin toisti perusteet, jotka se oli antanut oikeuskäytännössään, kun se oli punninnut ilmaisunvapauden oikeutta suhteessa oikeuteen nauttia yksityiselämän kunnioitusta:

- koskiko tapahtuma, jota julkaistu artikkeli käsitteli, yleistä etua
- oliko asianosainen julkisuuden henkilö
- miten tiedot oli saatu ja olivatko ne luotettavia.

Tuomioistuin totesi, että näyttelijän pidätys ja tuomio olivat julkinen oikeudellinen tosiasia ja siten koskivat yleistä etua, ja lisäksi, että näyttelijä oli riittävän tunnettu, jotta häntä saatettiin luonnehtia julkisuuden henkilöksi, ja että tiedot oli saatu syyttäjän virastosta eikä kumpikaan osapuoli kiistänyt

91 Tietosuojatyöryhmä (2014), *Guidelines on the implementation of the CJEU judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, WP 225, Bryssel, 26.11.2014.

92 EIT, *Axel Springer AG v. Saksa* [suuri jaosto], nro 39954/08, 7.2.2012, 90 ja 91 kohta.

julkaistujen tietojen todenmukaisuutta. Näin ollen yhtiölle määrätyt julkaisurajoitukset eivät olleet kohtuullisia suhteessa oikeutettuun tavoitteeseen suojella kantajan yksityiselämää. Tuomioistuin totesi, että ihmisoikeussopimuksen 10 artiklaa oli rikottu.

Esimerkki: Asiassa *Coudec ja Hachette Filipacchi Associés v. Ranska*[93] oli kyse siitä, että ranskalaisessa viikkolehdessä oli julkaistu Nicole Costen haastattelu, jossa tämä väitti, että Monacon ruhtinas Albert on hänen poikansa isä. Haastattelussa myös kuvattiin Costen ja ruhtinaan suhdetta sekä tapaa, jolla ruhtinas reagoi lapsen syntymään. Sen yhteydessä esitettiin myös kuvia ruhtinaasta lapsen kanssa. Ruhtinas Albert nosti kanteen kustantamoa vastaan yksityis- ja perhe-elämän suojaa koskevan oikeutensa rikkomisesta. Ranskalaiset tuomioistuimet katsoivat, että artikkelin julkaisu oli aiheuttanut ruhtinas Albertille peruuttamatonta vahinkoa, ja määräsivät kustantamon maksamaan vahingonkorvauksia ja julkaisemaan tiedot tuomiosta lehden etusivulla.

Lehden julkaisijat veivät asian Euroopan ihmisoikeustuomioistuimeen, koska katsoivat, että ranskalaisten tuomioistuinten päätöksellä puututtiin perusteettomasti niiden sananvapautta koskevaan oikeuteen. Tuomioistuimen piti punnita ruhtinas Albertin oikeutta nauttia yksityis- ja perhe-elämän kunnioitusta suhteessa julkaisijan sananvapautta koskevaan oikeuteen ja suuren yleisön tiedonsaantioikeuteen. Tärkeitä näkökohtia olivat myös Nicole Costen oikeus kertoa tarinansa yleisölle ja lapsen etu saada isän ja lapsen suhde virallisesti tunnustetuksi.

Tuomioistuin katsoi, että haastattelun julkaiseminen merkitsi puuttumista ruhtinaan yksityiselämään ja tutki, oliko puuttuminen välttämätöntä. Se katsoi, että julkaisu käsitteli julkisuuden henkilöä ja yleistä etua koskevaa asiaa, koska tieto ruhtinaan lapsesta oli Monacon kansalaisten edun mukaista, sillä perinnöllisen monarkian tulevaisuus liittyy erottamattomasti jälkeläisten olemassaoloon ja on siten yleisöä koskettava aihe.[94] Tuomioistuin pani myös merkille, että artikkelin avulla Nicole Coste lapsineen oli pystynyt käyttämään oikeuttaan sananvapauteen. Kansalliset tuomioistuimet eivät olleet ottaneet asianmukaisesti huomioon Euroopan ihmisoikeustuomioistuimen oikeuskäytännön myötä kehittyneitä periaatteita ja kriteereitä punnitessaan

93 EIT, *Coudec ja Hachette Filipacchi Associés v. Ranska* [suuri jaosto], nro 40454/07, 10.11.2015.

94 *Ibid.*, 104–116 kohta.

yksityis- ja perhe-elämän kunnioitusta koskevaa oikeutta suhteessa sananvapautta koskevaan oikeuteen. Se totesi, että Ranska oli rikkonut Euroopan ihmisoikeussopimuksen sananvapautta koskevaa 10 artiklaa.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä yksi oikeuksien punnitsemisen kannalta keskeinen peruste on se, liittyykö käsiteltävä ilmaisu yleistä etua koskevaan keskusteluun.

Esimerkki: Asiassa *Mosley v. Yhdistynyt kuningaskunta*[95] kansallinen viikkolehti oli julkaissut intiimejä valokuvia kantajasta. Tämä nosti siviilikanteen julkaisijaa vastaan, ja julkaisija määrättiin maksamaan vahingonkorvauksia. Rahallisesta korvauksesta huolimatta hän valitti olevansa edelleen yksityisyydensuojaa koskevan oikeutensa rikkomisen uhri, koska hän ei ollut voinut hakea kieltomääräystä ennen kyseisten valokuvien julkaisemista, sillä lehdellä ei ollut mitään velvollisuutta ilmoittaa ennalta aikomuksestaan julkaista aineistoa, joka saattoi loukata henkilön oikeutta yksityisyyteen.

Euroopan ihmisoikeustuomioistuin totesi, että vaikka tällaista aineistoa levitetään yleensä enemmän viihde- kuin opetustarkoituksiin, se nauttii epäilemättä ihmisoikeussopimuksen 10 artiklan mukaista suojaa, joka saattaisi hävitä ihmisoikeussopimuksen 8 artiklan vaatimuksille, jos tieto olisi luonteeltaan yksityistä ja intiimiä eikä sen levittäminen olisi mitenkään yleisen edun mukaista. Rajoituksiin, jotka voisivat toimia sensuurina ennen julkaisemista, on kuitenkin kiinnitettävä erityistä huomiota. Otettuaan huomioon ennakkoilmoitusvaatimuksen mahdollisen oikeuksia rajoittavan vaikutuksen, epävarmuuden tällaisen vaatimuksen tehokkuudesta ja näissä asioissa sallitun laajan harkintavallan, tuomioistuin totesi, ettei 8 artikla edellyttänyt oikeudellisesti sitovaa ennakkoilmoitusvaatimusta. Näin ollen tuomioistuin totesi, ettei 8 artiklaa ollut rikottu.

Esimerkki: Asiassa *Bohlen v. Saksa*[96] kantaja, tunnettu laulaja ja taiteellinen tuottaja, oli julkaissut omaelämäkerran, josta hänen piti myöhemmin poistaa muutamia kappaleita tuomioistuimen tuomioiden perusteella. Tarinaa kerrottiin laajasti kansallisissa tiedotusvälineissä, ja tupakkayhtiö käynnisti tapahtumaan viittaavan humoristisen mainoskampanjan, jossa käytettiin

95 EIT, *Mosley v. Yhdistynyt kuningaskunta*, nro 48009/08, 10.5.2011, 129 ja 130 kohta.

96 EIT, *Bohlen v. Saksa*, nro 53495/09, 19.2.2015, 45–60 kohta.

kantajan etunimeä ilman hänen suostumustaan. Kantaja haki mainostavalta yhtiöltä turhaan vahingonkorvauksia ja väitti, että hänen ihmisoikeussopimuksen 8 artiklan mukaisia oikeuksiaan oli loukattu. Euroopan ihmisoikeustuomioistuin toisti kriteerinsä, jotka ohjaavat yksityis- ja perhe-elämän kunnioitusta koskevan oikeuden punnitsemista suhteessa sananvapauteen ja totesi, että 8 artiklaa ei ollut rikottu. Kantaja oli julkisuuden henkilö, ja mainoksessa ei viitattu yksityiskohtaisesti hänen yksityiselämäänsä vaan julkiseen tapahtumaan, josta oli jo kerrottu tiedotusvälineissä ja joka oli osa julkista keskustelua. Mainos oli lisäksi humoristinen, eikä siinä ollut mitään kielteistä tai kantajaa halventavaa.

Esimerkki: Asiassa *Biriuk v. Liettua*[97] kantaja esitti Euroopan ihmisoikeustuomioistuimelle, että Liettua ei ollut täyttänyt velvollisuuttaan turvata kantajalle oikeus nauttia yksityiselämän kunnioitusta. Se johtui siitä, että vaikka merkittävä sanomalehti oli loukannut vakavasti hänen yksityisyyttään, asiaa tutkineet kansalliset tuomioistuimet olivat myöntäneet hänelle mitättömän pienet rahalliset vahingonkorvaukset. Muiden kuin rahallisten vahingonkorvausten myöntämisessä kansalliset tuomioistuimet olivat soveltaneet kansallisen lainsäädännön säännöksiä tietojen tarjoamisesta yleisölle. Niissä säädettiin matalasta ylärajasta muille kuin rahallisille vahingonkorvauksille, jotka johtuivat siitä, että tiedotusvälineet levittivät lainvastaisesti yleisölle tietoa henkilön yksityiselämästä. Asiassa oli kyse siitä, että Liettuan suurin päivälehti julkaisi etusivun artikkelin, jossa kerrottiin, että kantaja oli HIV-positiivinen. Artikkelissa myös arvosteltiin kantajan käytöstä ja kyseenalaistettiin hänen moraalikäsityksensä.

Euroopan ihmisoikeustuomioistuin muistutti, että henkilötietojen – erityisesti potilastietojen – suoja on olennaisen tärkeä edellytys sille, että henkilö voi nauttia ihmisoikeussopimuksen mukaisesta oikeudesta yksityis- ja perhe-elämän kunnioitukseen. Terveystietojen luottamuksellisuus on erityisen tärkeää, koska potilastietojen (tässä tapauksessa kantajan HIV-infektion) julkistaminen voi vaikuttaa huomattavasti henkilön yksityis- ja perhe-elämään, työtilanteeseen ja asemaan yhteiskunnassa. Tuomioistuin piti erityisen tärkeänä sitä, että sanomalehdessä esitettyjen tietojen mukaan sairaalan hoitohenkilökunta oli antanut tietoa kantajan HIV-infektiosta selkeästi vaitiolovelvollisuutensa vastaisesti. Puuttuminen kantajan yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen ei siis ollut lainmukainen.

97 EIT, *Biriuk v. Liettua*, nro 23373/03, 25.11.2008.

Artikkeli julkaistiin lehdessä, ja sananvapaus on myös ihmisoikeussopimuksen mukainen perusoikeus. Tutkiessaan, voisiko yleinen etu oikeuttaa tällaisten tietojen julkaisemisen kantajasta, tuomioistuin totesi, että julkaisun päätarkoitus oli lisätä sanomalehden myyntiä tyydyttämällä lukijoiden uteliaisuutta. Sellaisen tarkoituksen ei voitu katsota edistävän mitään yhteiskunnan yleistä etua koskevaa keskustelua. Koska asiassa oli kyse lehdistönvapauden törkeästä väärinkäytöstä, vahingonkorvausten vakava rajoittaminen ja kansallisen lainsäädännön mukaiset aineettomista vahingoista määrätyt mitättömät vahingonkorvaukset tarkoittivat, että Liettua ei ollut täyttänyt positiivista velvoitettaan turvata kantajan oikeus nauttia yksityiselämän kunnioitusta. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Sananvapautta koskeva oikeus ja henkilötietojen suojaa koskeva oikeus eivät ole aina ristiriidassa. Toisinaan henkilötietojen tehokas suoja takaa myös sananvapauden.

Esimerkki: Euroopan unionin tuomioistuin totesi asiassa *Tele2 Sverige*, että direktiivin 2006/24/EY (tietojen säilyttämistä koskeva direktiivi) sisältämä puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin perusoikeuksiin on ”laajamittaista, ja se on katsottava erityisen vakavaksi. Lisäksi tietojen säilyttäminen ja niiden myöhempi käyttö ilman, että tilaajalle tai rekisteröidylle käyttäjälle ilmoitetaan siitä, voi aiheuttaa kyseisille ihmisille [...] tunteen siitä, että heidän yksityiselämänsä on jatkuvan tarkkailun kohteena”. Tuomioistuin totesi myös, että liikenne- ja paikkatietojen yleinen säilyttäminen voi vaikuttaa sähköisten viestintävälineiden käyttöön ja ”näin ollen näiden välineiden käyttäjien perusoikeuskirjan 11 artiklassa taatun sananvapauden harjoittamiseen”[98]. Näin ollen tietosuojasäännöillä loppujen lopuksi edistetään sananvapauden käyttöä, koska niissä vaaditaan ankaria suojatoimia, jotta tietoja ei säilytetä yleisesti.

Tiedonsaantioikeus on myös osa sananvapautta. Hallinnon avoimuuden merkitys demokraattisen yhteiskunnan toiminnalle ymmärretään yhä paremmin. Avoimuus

98 EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB vastaan Post- och telestyrelsen ja Secretary of State for the Home Department vastaan Tom Watson ym.* [suuri jaosto], 21.12.2016, 101 kohta; EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym.* ja *Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014, 28 kohta.

on yleisen edun mukainen tavoite, joka voi siten oikeuttaa puuttumiseen tietosuojaa koskevaan oikeuteen, jos se on välttämätöntä ja oikeasuhteista, kuten 1.2 kohdassa selitetään. Kahden viime vuosikymmenen aikana oikeus saada viranomaisten hallussa olevia asiakirjoja on tunnustettu jokaisen EU:n kansalaisen sekä jokaisen luonnollisen henkilön ja oikeushenkilön, jonka asuinpaikka tai rekisteröity toimipaikka on EU:n jäsenvaltiossa, tärkeäksi oikeudeksi.

Euroopan neuvoston oikeudessa on mahdollista vedota virallisten asiakirjojen saatavuutta koskevassa suosituksessa määriteltyihin periaatteisiin. Kyseisen suosituksen pohjalta laadittiin virallisten asiakirjojen saatavuutta koskeva yleissopimus (yleissopimus 205)[99].

EU:n oikeudessa oikeus saada asiakirjoja on vahvistettu Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi annetussa asetuksessa (EY) N:o 1049/2001 (asiakirjojen saatavuutta koskeva asetus)[100]. Perusoikeuskirjan 42 artiklassa ja SEUT-sopimuksen 15 artiklan 3 kohdassa tämä oikeus on laajennettu kattamaan ”unionin toimielinten, elinten ja laitosten asiakirjat niiden tallennemuodosta riippumatta”.

Oikeus saada asiakirjoja voi olla ristiriidassa henkilötietojen suojaa koskevan oikeuden kanssa, jos asiakirja sisältää muiden henkilötietoja. Yleisen tietosuoja-asetuksen 86 artiklassa säädetään selkeästi, että viranomaiset tai yhteisöt voivat luovuttaa viranomaisten tai yhteisöjen hallussa olevien virallisten asiakirjojen sisältämiä henkilötietoja unionin oikeuden[101] tai jäsenvaltion lainsäädännön mukaisesti, jotta voidaan sovittaa yhteen virallisten asiakirjojen julkisuus ja tämän asetuksen mukainen oikeus henkilötietojen suojaan.

Viranomaisten hallussa olevien asiakirjojen tai tietojen saantia koskevia pyyntöjä voidaan näin ollen joutua punnitsemaan niiden henkilöiden tietosuojaoikeutta vasten, joiden tietoja pyydetyt asiakirjat sisältävät.

99 Euroopan neuvosto, ministerikomitea (2002), suositus R (81) 19 ja suositus Rec(2002)2 virallisten asiakirjojen saatavuudesta, 21.2.2002; Euroopan neuvosto, virallisten asiakirjojen saatavuutta koskeva yleissopimus, CETS nro 205, 18.6.2009. Yleissopimus ei ole vielä tullut voimaan.

100 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1049/2001, annettu 30 päivänä toukokuuta 2001, Euroopan parlamentin, neuvoston ja komission asiakirjojen saamisesta yleisön tutustuttavaksi, EYVL 2001, L 145.

101 Perusoikeuskirjan 42 artikla, SEUT-sopimuksen 15 artiklan 3 kohta ja asetus (EY) N:o 1049/2009.

Esimerkki: Asiassa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*[102] Euroopan unionin tuomioistuin joutui ottamaan kantaa siihen, oliko EU:n lainsäädännössä vaadittu EU:n maataloustukien saajien nimien ja heidän saamiensa määrien julkaiseminen suhteellisuusperiaatteen mukaista. Julkaisemisen tavoitteena on lisätä avoimuutta ja edistää julkisten varojen asianmukaista käyttöä hallinnossa koskevaa julkista valvontaa. Useat tuensaajat riitauttivat julkaisemisen oikeasuhteisuuden.

Tuomioistuin toi esiin, että oikeus henkilötietojen suojaan ei ole ehdoton oikeus, ja se katsoi, että tietojen, joissa mainitaan kahden EU:n maatalousrahaston tuensaajien nimet ja heidän saamansa tarkat määrät, julkaisemisessa internetsivustolla on kyse puuttumisesta tuensaajien oikeuteen nauttia yksityiselämänsä kunnioitusta yleensä ja erityisesti heidän oikeuteensa saada henkilötiedoilleen suojaa.

Tuomioistuimen mukaan tällainen puuttuminen perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin oikeuksiin oli ollut lainmukaista ja vastannut EU:n tunnustamaa yleisen edun mukaista tavoitetta, joka oli yhteisön varojen käytön avoimuuden lisääminen. Tuomioistuin katsoi kuitenkin, että kyseisistä EU:n maatalousrahastoista tukea saavien luonnollisten henkilöiden nimien ja heidän saamiensa tarkkojen määrien julkaiseminen oli suhteeton toimenpide eikä sitä voitu perustella perusoikeuskirjan 52 artiklan 1 kohdalla. Se totesi, että demokraattisessa yhteiskunnassa on tärkeää, että verovelvolliset saavat tietoja julkisten varojen käytöstä. Koska ”avoimuutta koskevalla tavoitteella ei voida katsoa olevan mitään automaattista etusijaa suhteessa henkilötietojen suojaa koskevaan oikeuteen”[103], EU:n toimielimet olivat velvollisia saattamaan tasapainoon unionin intressin taata toimiensa avoimuus ja yksityiselämän suojaa ja tietosuojaa koskevien oikeuksien harjoittamisen rajoituksen, josta tuensaajat kärsivät julkaisemisen vuoksi.

Euroopan unionin tuomioistuin katsoi, että EU:n toimielimet eivät olleet tehneet tätä punnintaa asianmukaisesti, koska oli mahdollista toteuttaa toimenpiteitä, joilla loukataan vähemmän luonnollisten henkilöiden kyseistä perusoikeutta ja joilla voidaan samalla myötävaikuttaa tehokkaasti julkaisun tavoitteena olevaan avoimuuteen. Esimerkiksi sen sijaan, että julkaistaan

102 EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010, 47–52, 58, 66–67, 75, 86 ja 92 kohta.

103 *Ibid.*, 85 kohta.

yleisesti kaikkien tuensaajien tiedot ja annetaan heidän nimensä ja kunkin saamat tarkat määrät, voitaisiin tehdä ero sellaisten merkityksellisten kriteerien mukaan kuin ajanjaksot, joina kyseiset luonnolliset henkilöt ovat saaneet tällaisia tukia, niiden toistuvuus tai niiden laji ja suuruus[104]. Näin ollen tuomioistuin totesi, että EU:n maatalousrahastojen tuensaajia koskevien tietojen julkaisemisesta annettu EU:n lainsäädäntö oli osittain pätemätöntä.

Esimerkki: Asiassa *Rechnungshof v. Österreichischer Rundfunk ym.*[105] Euroopan unionin tuomioistuin pohti kyseisen Itävallan tietyn lain yhteensoveltuvuutta EU:n tietosuojalainsäädännön kanssa. Lainsäädännössä valtiollinen elin velvoitetaan keräämään ja luovuttamaan edelleen tulotietoja eri julkisyhteisöjen palveluksessa olevien työntekijöiden nimien ja tulojen julkaisemiseksi yleisesti saataville annettavassa vuosiraportissa. Muutamat henkilöt kieltäytyivät antamasta tietojaan tietosuojaan vedoten.

Euroopan unionin tuomioistuin vetosi lausunnossaan perusoikeuksien suojeluun EU:n oikeuden yleisenä periaatteena sekä ihmisoikeussopimuksen 8 artiklaan ja muistutti, että perusoikeuskirja ei ollut tuolloin sitova. Se totesi, että tietojen kerääminen yksityishenkilön ansiotuloista ja erityisesti niiden välittäminen kolmansille osapuolille kuuluu yksityisyyttä koskevan oikeuden soveltamisalaan ja merkitsee puuttumista tähän oikeuteen. Puuttuminen voitaisiin perustella, jos laki sen sallii, jos sillä pyritään lailliseen tavoitteeseen ja jos se on demokraattisessa yhteiskunnassa välttämätön tämän tavoitteen saavuttamiseksi. Euroopan unionin tuomioistuin totesi, että Itävallan lailla oli laillinen tavoite, koska sillä pyrittiin pitämään virkamiesten palkat kohtuullisissa rajoissa. Tähän näkökohtaan liittyy myös maan taloudellinen hyvinvointi. Itävallan intressiä taata julkisten varojen mahdollisimman hyvä käyttö oli kuitenkin punnittava siihen nähden, miten vakavasti asianomaisten henkilöiden oikeutta yksityisyyteen loukataan.

Euroopan unionin tuomioistuin jätti kansallisen tuomioistuimen tarkistettavaksi, onko tällainen yksityishenkilöiden tulotietojen julkistaminen sekä välttämätöntä että oikeassa suhteessa siihen päämäärään, johon lainsäädännöllä pyritään. Se kehotti kansallista tuomioistuinta myös tutkimaan,

104 *Ibid.*, 89 kohta.

105 EUT, hdistetyt asiat C-465/00, C-138/01 ja C-139/09, *Rechnungshof vastaan Österreichischer Rundfunk ym. ja Christa Neukomm ja Joseph Lauermann vastaan Österreichischer Rundfunk*, 20.5.2003.

olisiko tämä tavoite voitu saavuttaa yhtä tehokkaasti lievemmillä toimenpiteillä. Henkilötiedot olisi esimerkiksi voitu toimittaa vain valvontaelimille eikä suurelle yleisölle.

Myöhemmissä asioissa kävi selväksi, että tietosuojan ja asiakirjojen saatavuuden punninta edellyttää tapauskohtaista yksityiskohtaista analyysia. Kumpikaan oikeus ei voi automaattisesti kumota toista. Euroopan unionin tuomioistuimella oli tilaisuus tulkita henkilötietoja sisältävien asiakirjojen saatavuutta koskevaa oikeutta kahdessa asiassa.

Esimerkki: Asiassa *Euroopan komissio v. Bavarian Lager*[106] Euroopan unionin tuomioistuin määritteli henkilötietojen suojan laajuuden EU:n toimielinten asiakirjojen saatavuuden yhteydessä sekä asetusten (EY) N:o 1049/2001 (asiakirjojen saatavuutta koskeva asetus) ja (EY) N:o 45/2001 (EU:n toimielinten tietosuoja-asetus) välisen suhteen. Vuonna 1992 perustettu Bavarian Lager tuo pullotettua saksalaista olutta Yhdistyneeseen kuningaskuntaan, pääasiallisesti pubeihin ja baareihin. Se kuitenkin kohtasi vaikeuksia siksi, että Yhdistyneen kuningaskunnan lainsäädäntö tosiasiallisesti suosii kansallisia valmistajia. Bavarian Lagerin tekemän valituksen seurauksena Euroopan komissio päätti käynnistää Yhdistynyttä kuningaskuntaa vastaan menettelyn velvollisuuksien noudattamatta jättämisen takia. Yhdistynyt kuningaskunta muuttikin kiistanalaisia säännöksiä ja saattoi ne yhdenmukaisiksi EU:n oikeuden kanssa. Tämän jälkeen Bavarian Lager pyysi komissiolta muiden asiakirjojen mukana kopiota komission edustajien, Yhdistyneen kuningaskunnan viranomaisten ja ammattiyhdistyksen *Confédération des Brasseurs du Marché Commun* (CBMC) edustajien välisen kokouksen pöytäkirjasta. Komissio suostui paljastamaan joitakin tapaamiseen liittyneitä asiakirjoja, mutta peitti viisi pöytäkirjassa esiintynyttä nimeä, sillä kaksi henkilöä oli vastustanut henkilöllisyytensä paljastamista eikä komissio ollut onnistunut tavoittamaan kolmea muuta. Komissio hylkäsi 18. maaliskuuta 2004 tekemällään päätöksellä Bavarian Lagerin uuden pyynnön saada kokouksen pöytäkirja kokonaisuudessaan ja vetosi erityisesti asianomaisten yksityiselämän suojeluun sellaisena kuin se taataan EU:n toimielinten tietosuoja-asetuksessa.

106 EUT, C-28/08 P, *Euroopan komissio v. The Bavarian Lager Co. Ltd.* [suuri jaosto], 29.6.2010.

Bavarian Lager ei hyväksynyt komission kantaa vaan nosti kanteen unionin yleisessä tuomioistuimessa. Tuomioistuin kumosi komission päätöksen 8. marraskuuta 2007 tekemällään päätöksellä (asia T-194/04, *The Bavarian Lager Co. Ltd v. Euroopan yhteisöjen komissio*) ja katsoi erityisesti, että pelkkä asianomaisten nimien esiintyminen kokouksen osanottajaluettelossa niiden elinten kohdalla, joita he edustivat, ei vahingoittanut eikä vaarantanut yksityiselämän suojaa.

Komission valitettua Euroopan unionin tuomioistuin kumosi unionin yleisen tuomioistuimen antaman tuomion. Euroopan unionin tuomioistuin katsoi, että asiakirjojen saatavuutta koskevalla asetuksella ”otetaan käyttöön erillinen ja vaativampi järjestely sellaisen henkilön suojaamiseksi, jonka henkilötiedot saatetaan joissain tapauksissa luovuttaa yleisölle”. Euroopan unionin tuomioistuimen mukaan silloin, kun asiakirjojen saatavuutta koskevaan asetukseen perustuvalla hakemuksella pyydetään oikeutta tutustua henkilötietoja sisältävään asiakirjaan, asiakirjojen saatavuutta koskevan asetuksen säännökset tulevat kaikilta osin sovellettaviksi. Tämän jälkeen tuomioistuin totesi, että komissio saattoi perustellusti hylätä hakemuksen saada tutustua lokakuussa 1996 pidetyn kokouksen täydelliseen pöytäkirjaan. Koska viisi kokouksen osanottajaa ei ollut antanut suostumustaan, komissio oli noudattanut riittävällä tavalla avoimuusvelvoitettaan luovuttamalla riidanalaisesta asiakirjasta version, josta kyseisten henkilöiden nimet oli poistettu.

Lisäksi tuomioistuin katsoi seuraavaa: ”Koska Bavarian Lager ei ole esittänyt mitään nimenomaista ja laillista tarkoitusta eikä minkäänlaisia vakuuttavia argumentteja osoittaakseen tarpeen näiden henkilötietojen siirtoon, komissio ei ole voinut vertailla asianosaisten eri intressejä. Se ei ole myöskään voinut selvittää, oliko syytä ajatella, että rekisteröityjen oikeutetut edut voisivat siirron vuoksi vaarantua”, kuten EU:n toimielinten tietosuoja-asetuksessa edellytetään.

Esimerkki: Asiassa *ClientEarth ja PAN Europe v. EFSA*[107] Euroopan unionin tuomioistuin tutki, oli Euroopan elintarviketurvallisuusviranomaisen (EFSA) päätös evätä kantajilta oikeus tutustua kaikkiin asiakirjoihin välttämätöntä niiden henkilöiden yksityiselämän ja henkilötietojen suojaa koskevien oikeuksien suojelemiseksi, joihin asiakirjoissa viitattiin. Asiakirja oli ohjeluonnos, jonka

107 EUT, C-615/13P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. Euroopan elintarviketurvallisuusviranomainen (EFSA), Euroopan komissio*, 16.7.2015.

EFSAn työryhmä laati yhteistyössä ulkopuolisten asiantuntijoiden kanssa kasvinsuojeluaineiden markkinoille saattamisesta. Alun perin EFSA myönsi oikeuden tutustua osaan pyydetyistä asiakirjoista mutta epäsi oikeuden tutustua ohjeluonnoksen valmisteluvaiheen joihinkin versioihin. Myöhemmin se myönsi oikeuden tutustua luonnosversioon, joka sisälsi ulkopuolisten asiantuntijoiden ohjeluonnoksesta esittämiä yksittäisiä huomautuksia. Se kuitenkin poisti kyseisten asiantuntijoiden nimet ja vetosi yksilöiden suojelua yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä koskevan asetuksen (EY) N:o 45/2001 4 artiklan 1 kohdan b alakohtaan ja siihen, että ulkopuolisten asiantuntijoiden yksityisyyttä on suojeltava. Unionin yleinen tuomioistuin piti EFSAn päätöksen voimassa.

Kantajien valitettua Euroopan unionin tuomioistuin kumosi unionin yleisen tuomioistuimen antaman tuomion. Se totesi, että henkilötietojen siirtäminen tässä tapauksessa oli tarpeellista, jotta voitiin varmistua kunkin ulkopuolisen asiantuntijan puolueettomuudesta tämän tieteellisessä tehtävässä EFSAn palveluksessa ja varmistaa EFSAn päätöksentekomenettelyn avoimuus. Euroopan unionin tuomioistuimen mukaan EFSA ei täsmentänyt, miten yksittäisiä huomautuksia ohjeluonnoksesta esittäneiden ulkopuolisten asiantuntijoiden nimien paljastaminen vaarantaisi kyseisten henkilöiden oikeutetut edut. Yleinen väite siitä, että tietojen luovuttaminen todennäköisesti aiheuttaa vaaran yksityiselämän loukkaamisesta, ei riitä, jos kunkin tapauksen tueksi ei ole esitetty mitään näyttöä.

Näiden tuomioiden mukaisesti puuttuminen henkilötietojen suojaa koskevaan oikeuteen asiakirjojen saatavuuden yhteydessä edellyttää erityistä ja perusteltua syytä. Oikeus saada asiakirjoja ei voi automaattisesti kumota oikeutta tietosuojaan.[108]

Tämä lähestymistapa on samanlainen kuin Euroopan ihmisoikeustuomioistuimella yksityisyyden suojasta ja asiakirjojen saatavuudesta, kuten seuraava tuomio osoittaa. Asiassa *Magyar Helsinki* annetussa tuomiossa Euroopan ihmisoikeustuomioistuin totesi, että 10 artikla ei anna yksilölle oikeutta saada viranomaisen hallussa olevaa tietoa eikä se velvoita hallintoa välittämään kyseistä tietoa yksilölle. Tällainen oikeus tai velvollisuus voi kuitenkin aiheutua ensinnäkin silloin, kun tietojen luovuttamisesta määrätään lainvoimaisella oikeuden tuomiolla, ja toiseksi silloin, kun

108 Ks. kuitenkin Euroopan tietosuojavaltuutetun (EDPS) yksityiskohtainen pohdinta asiakirjassa (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bryssel, 24.3.2011.

tietojen saaminen on ratkaisevaa yksilön sananvapauden käyttämiselle – erityisesti vapaudelle vastaanottaa ja välittää tietoja – ja kun sen epääminen merkitsisi puuttumista kyseiseen oikeuteen[109]. Jokaisessa yksittäisessä tapauksessa on arvioitava tapauksen erityisten olosuhteiden perusteella, onko saatavuuden epääminen puuttumista hakijan sananvapauteen ja missä määrin sillä puututaan tähän vapauteen. Arvioitavia olosuhteita ovat muun muassa i) tietopyynnön tarkoitus, ii) haluttujen tietojen laji, iii) hakijan rooli ja iv) se, ovatko tiedot valmiina ja saatavilla.

Esimerkki: Asiassa *Magyar Helsinki Bizottság v. Unkari*[110] kantajana oli ihmisoikeuksia puolustava kansalaisjärjestö, joka pyysi poliisilta tietoa viran puolesta toimivista puolustusasianajajista tutkimukseen, jossa käsiteltiin julkisten oikeusavustajien järjestelmää Unkarissa. Poliisi kieltäytyi antamasta tietoja ja väitti, että niissä oli henkilötietoja, joita ei saanut luovuttaa. Euroopan ihmisoikeustuomioistuin sovelsi edellä mainittuja kriteereitä ja katsoi, että 10 artiklalla suojattuun oikeuteen oli puututtu. Tarkemmin sanottuna kantaja halusi käyttää oikeutta välittää tietoa yleisen edun mukaisesta asiasta, ja se oli pyytänyt siksi tietoja saataville. Tiedot olivat välttämättömiä, jotta kantaja pystyi harjoittamaan sananvapautta. Yleisön intressissä oli saada tietoa julkisten oikeusavustajien nimittämisestä. Ei ollut syytä epäillä, että kyseessä ollut tutkimus sisälsi tietoa, jonka kantaja välitti yleisölle ja joka yleisöllä oli oikeus vastaanottaa. Tuomioistuin katsoi näin ollen, että pyydetyt tiedot oli saatava, jotta kantaja pystyi täyttämään tehtävän. Tiedot olivat myös valmiina ja saatavilla.

Euroopan unionin tuomioistuin totesi, että tässä tapauksessa tietojen saatavuuden epääminen oli vaarantanut tiedonsaantioikeuden keskeisen sisällön. Tähän johtopäätökseen päätymiseksi se tutki erityisesti pyydettyjen tietojen tarkoitusta ja sen panosta merkittävään julkiseen keskusteluun, pyydettyjen tietojen luonnetta ja niiden yleisen edun mukaisuutta sekä asian kantajan asemaa yhteiskunnassa.

Perusteluissaan tuomioistuin pani merkille, että kansalaisjärjestön tekemä tutkimus koski oikeusjärjestelmän toimintaa ja oikeudenmukaista kuulemista koskevaa oikeutta, joka on ihmisoikeussopimuksen mukaan erittäin tärkeä oikeus. Koska pyydetyt tiedot eivät sisältäneet julkisen alan ulkopuolisia tietoja, kyseessä olevien rekisteröityjen (viran puolesta toimivien julkisten

109 EIT, *Magyar Helsinki Bizottság v. Unkari* [suuri jaosto], nro 18030/11, 8.11.2016, 148 kohta.

110 *Ibid.*, 181, 187–200 kohta.

oikeusavustajien) yksityisyyttä koskevat oikeudet eivät olisi vaarantuneet, vaikka poliisi olisi antanut tiedot kantajan saataville. Kantajan pyytämät tiedot olivat tilastotietoja, jotka liittyivät niiden kertojen määrään, jolloin viran puolesta toimiva asianajaja oli nimitetty edustamaan vastaajia julkisissa rikosoikeudenkäynneissä.

Koska tutkimuksen tarkoituksena oli edistää tärkeää keskustelua yleisen edun mukaisesta aiheesta, tuomioistuin katsoi, että kaikki rajoitukset kansalaisjärjestön ehdottamaan julkaisuun olisi tarkastettava erittäin huolellisesti. Kyseessä olevat tiedot olivat yleisen edun mukaisia, koska yleinen etu kattaa asiat, jotka voivat aiheuttaa huomattavaa erimielisyyttä, jotka koskevat tärkeää yhteiskunnallista kysymystä tai jotka koskevat ongelmaa, jonka tietoon saaminen olisi yleisön intressissä[111]. Se koskisi siis ehdottomasti keskustelua oikeuden käyttämisestä ja oikeudenmukaisista oikeudenkäynneistä, jotka olivat kantajan tutkimuksen aiheena. Kyseessä olevia eri oikeuksia punniten ja suhteellisuusperiaatetta soveltaen Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 10 artiklan mukaisia kantajan oikeuksia oli loukattu perusteettomasti.

1.3.2 Vaitiolovelvollisuus

Kansallisen lainsäädännön mukaan tiettyyn viestintään voidaan soveltaa vaitiolovelvollisuutta. Vaitiolovelvollisuus voidaan ymmärtää erityiseksi eettiseksi velvollisuudeksi, joka aiheuttaa tiettyihin luottamukseen perustuviin ammatteihin ja tehtäviin luonnostaan kuuluvan oikeudellisen velvoitteen. Näitä tehtäviä suorittavat henkilöt ja laitokset eivät saa paljastaa tehtäviensä suorittamisessa saamiaan luottamuksellisia tietoja. Vaitiolovelvollisuus koskee erityisesti terveydenhuoltoalan ammatteja ja asianajosalaisuutta. Monilla oikeudenkäyttöalueilla vaitiolovelvollisuus tunnustetaan myös rahoitusalalla. Vaitiolovelvollisuus ei ole perusoikeus, mutta sitä suojataan oikeutena nauttia yksityiselämän kunnioitusta. Euroopan unionin tuomioistuin on esimerkiksi linjannut joissakin asioissa, että ”tiettyjen luottamuksellisiksi määriteltyjen tietojen ilmaisemisen kieltäminen voi olla tarpeen, jotta turvattaisiin yrityksen perusoikeus yksityiselämän suojaan, joka on vahvistettu [ihmisoikeussopimuksen] 8 artiklassa ja perusoikeuskirjan 7 artiklassa”[112]. Myös Euroopan ihmisoikeustuomioistuinta on pyydetty linjaamaan, ovatko vaitiolovelvollisuuden

111 *Ibid.*, 156 kohta.

112 EUT, asia T-462/12 R, *Pilkington Group Ltd v. Euroopan komissio*, unionin yleisen tuomioistuimen presidentin määräys, 11.3.2013, 44 kohta.

rajoitukset puuttumista ihmisoikeussopimuksen 8 artiklaan. Tätä havainnollistetaan esitettävissä esimerkeissä.

Esimerkki: Asiassa *Pruteanu v. Romania*[113] kantaja toimi asianajajana kaupallisessa yrityksessä, jota oli kielletty toteuttamasta pankkitransaktioita petosväitteiden vuoksi. Asian tutkinnan aikana romanialaiset antoivat syyttäjäviranomaisille luvan salakuunnella ja tallentaa yhtiön yhteistyökumppanin puhelinkeskusteluja tietyn ajan. Äänityksiin ja kuuntelutallenteisiin kuului kumppanin viestintää tämän asianajajan kanssa.

Kantaja Pruteanu väitti, että tällä puututtiin hänen oikeuteensa nauttia yksityis- ja perhe-elämään ja kirjeenvaihtoon kohdistuvaa kunnioitusta. Euroopan ihmisoikeustuomioistuin korosti tuomiossaan asianajajan ja tämän asiakkaan välisen suhteen asemaa ja merkitystä. Asianajajan ja tämän asiakkaan keskustelujen salakuuntelu epäilemättä merkitsi puuttumista vaitiolovelvollisuuteen, joka oli näiden kahden henkilön välisen suhteen perusta. Siinä tapauksessa asianajaja voisi myös valittaa puuttumisesta oikeuteensa nauttia yksityiselämään ja kirjeenvaihtoon kohdistuvasta kunnioituksesta. Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Brito Ferrinho Bexiga Villa-Nova v. Portugali*[114] kantaja oli juristi, joka kieltäytyi luovuttamasta omia tiliotteitaan veroviranomaisille ammatillisen luottamuksellisuuden ja pankkisalaisuuden perusteella. Syyttäjänvirasto aloitti tutkimuksen veropetoksesta ja pyysi lupaa ammatillisen vaitiolovelvollisuuden peruuttamiseen. Kansalliset tuomioistuimet määräsivät ammatillisen luottamuksellisuuden ja pankkisalaisuuden peruuttamisesta, koska yleisen edun on oltava tärkeämpi kuin kantajan yksityiset edut.

Kun asia tuli Euroopan ihmisoikeustuomioistuimen käsiteltäväksi, tuomioistuin katsoi, että kantajan tiliotteiden saatavuus merkitsi puuttumista hänen ammatillisen luottamuksellisuuden kunnioittamista koskevaan oikeuteensa, joka kuuluu yksityiselämää koskevan oikeuden soveltamisalaan. Puuttumisella oli oikeusperusta, koska se perustui rikosoikeusmenettelyistä annettuun säädökseen, ja sillä oli laillinen tarkoitus. Tutkiessaan puuttumisen välttämättömyyttä ja oikeasuhteisuutta Euroopan ihmisoikeustuomioistuin kuitenkin

113 EIT, *Pruteanu v. Romania*, nro 30181/05, 3.2.2015.

114 EIT, *Brito Ferrinho Bexiga Villa-Nova v. Portugali*, nro. 69436/10, 1.12.2015.

huomautti, että luottamuksellisuuden poistamista koskeva menettely oli toteutettu ilman, että kantaja osallistui siihen tai tiesi siitä. Kantaja ei näin ollen pystynyt esittämään perusteluitaan. Lisäksi, vaikka kansallisessa lainsäädännössä säädetään, että asianajajaliittoa on kuultava tällaisessa menettelyssä, liittoa ei ollut kuultu. Kantajalle ei myöskään ollut mahdollisuutta tosiasiallisesti riitauttaa luottamuksellisuuden poistamista eikä oikeussuojakeinoa, jolla toimenpiteen olisi voinut riitauttaa. Koska menettelytakeita ei ollut eikä luottamuksellisuusvelvoitteen peruuttavaa toimenpidettä valvottu tosiasiallisesti oikeudellisesti, Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Vaitiolovelvollisuuden ja tietosuojan välinen vuorovaikutus on usein ristiriitaista. Toisaalta tietosuojasäännöt ja lainsäädännössä vahvistetut suojatoimet auttavat varmistamaan vaitiolovelvollisuuden. Esimerkiksi sääntöjen, joiden mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on otettava käyttöön vakaita tietoturvatoimenpiteitä, tavoitteena on estää muun muassa vaitiolovelvollisuudella suojattujen henkilötietojen luottamuksellisuuden menetys. Lisäksi EU:n yleisen tietosuoja-asetuksen mukaan terveystietoja, jotka kuuluvat erityisiin henkilötietoryhmiin, jotka vaativat muita vahvempaa suojaa, voidaan käsitellä, kunhan on olemassa asianmukaiset ja erityiset toimenpiteet rekisteröityjen oikeuksien, erityisesti salassapitovelvollisuuden, suojaamiseksi[115].

Toisaalta rekisterinpitäjille ja henkilötietojen käsittelijöille tiettyjen henkilötietojen osalta määrätyllä vaitiolovelvollisuudella voidaan rajoittaa rekisteröityjen oikeuksia, erityisesti tiedonsaantioikeutta. Vaikka yleisessä tietosuoja-asetuksessa on kattava luettelo tiedoista, jotka on periaatteessa annettava rekisteröidylle, kun henkilötietoja ei ole saatu häneltä, tätä luovuttamisvaatimusta ei sovelleta, kun henkilötiedot on pidettävä luottamuksellisina, koska niitä koskee unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuva vaitiolovelvollisuus[116].

Yleisessä tietosuoja-asetuksessa säädetään jäsenvaltioiden mahdollisuudesta vahvistaa lainsäädännöllä erityiset säännöt, joiden avulla taataan vaitiolovelvollisuus tai muu vastaava velvoite ja sovitetaan yhteen henkilötietojen suojaa koskeva oikeus ja salassapitovelvollisuus[117].

115 Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan h alakohta ja 9 artiklan 3 kohta.

116 *Ibid.*, 14 artiklan 5 kohdan d alakohta.

117 *Ibid.*, johdanto-osan 164 kappale ja 90 artikla.

Yleisessä tietosuoja-asetuksessa säädetään, että jäsenvaltiot voivat antaa erityisiä sääntöjä valvontaviranomaisten valtuuksista niiden rekisterinpitäjien ja henkilötietojen käsittelijöiden osalta, joita salassapitovelvollisuus koskee. Nämä erityissäännöt liittyvät valtuuteen saada pääsy kaikkiin rekisterinpitäjän ja henkilötietojen käsittelijän tiloihin, tietojenkäsittelylaitteisiin ja henkilötietoihin, kun kyseiset henkilötiedot on saatu vaitiolovelvollisuuden kattaman toiminnan yhteydessä. Näin ollen tietosuojasta vastaavien valvontaviranomaisten on noudatettava vaitiolovelvollisuutta, joka sitoo rekisterinpitäjiä ja henkilötietojen käsittelijöitä. Lisäksi vaitiolovelvollisuus sitoo itse valvontaviranomaisten jäseniä toimikauden aikana ja sen jälkeen. Tehtäviään suorittaessaan valvontaviranomaisten jäsenet ja työntekijät voivat saada luottamuksellista tietoa. Asetuksen 54 artiklan 2 kohdassa säädetään selkeästi, että heidän on pidettävä nämä luottamukselliset tiedot salassa.

Yleisen tietosuoja-asetuksen mukaan jäsenvaltioiden on ilmoitettava komissiolle säännöistä, joita ne antavat tietosuojan ja asetuksessa vahvistettujen periaatteiden sovittamiseksi yhteen vaitiolovelvollisuuden kanssa.

1.3.3 Uskonnon ja vakaumuksen vapaus

Uskonnon ja vakaumuksen vapaus on suojattu ihmisoikeussopimuksen 9 artiklalla (ajatuksen-, omantunnon- ja uskonnonvapaus) ja EU:n perusoikeuskirjan 10 artiklalla. Uskonnolliset tai aatteelliset vakaumukset paljastavat henkilötiedot katsotaan ”arkaluonteisiksi tiedoiksi” sekä EU:n että Euroopan neuvoston oikeudessa, ja niiden käsittely ja käyttö vaativat vahvempaa suojaa.

Esimerkki: Asiassa *Sinan Işık v. Turkki*[118] kantaja oli uskonnollisen alawiittiyhteisön jäsen. Yhteisön uskoon ovat vaikuttaneet sufismi ja muut islamia edeltäneet vakaumukset. Jotkut tutkijat pitävät sitä erillisenä uskontona ja toiset islamin uskon osana. Kantaja valitti siitä, että hänen henkilöllisyystodistuksensa uskonnon ilmaisevaan kohtaan oli hänen toiveidensa vastaisesti merkitty ”islam” eikä ”alawiitti”. Kansalliset tuomioistuimet hylkäsivät hänen pyyntönsä muuttaa henkilöllisyystodistukseen uskonnoksi ”alawiitti”, koska sana merkitsee islamin alaryhmää eikä erillistä uskontoa. Kantaja valitti Euroopan ihmisoikeustuomioistuimeen, että hänen oli pitänyt ilman suostumustaan julkistaa uskontonsa, koska henkilöllisyystodistuksessa piti

118 EIT, *Sinan Işık v. Turkki*, nro 21924/05, 2.2.2010.

ilmoittaa uskonto, ja että se oli vastoin hänen uskonnon ja omantunnon vapautta koskevaa oikeuttaan etenkin, kun henkilöllisyystodistuksen mainin ta ”islam” oli virheellinen.

EIT toisti, että uskonnonvapaus sisältää vapauden tunnustaa uskontoaan joko yksin tai yhdessä muiden kanssa julkisesti tai yksityisesti. Käsittelyn aikaan sovellettavan kansallisen lainsäädännön mukaan yksilöillä piti olla mukanaan henkilöllisyystodistus eli asiakirja, joka piti esittää viranomaisen tai yksityisen yrityksen pyynnöstä ja josta kävi ilmi henkilön uskonto. Tällaisessa velvollisuudessa ei otettu huomioon, että oikeus tunnustaa uskontoaan päti myös päinvastoin eli vakaumuksiaan ei tarvitse paljastaa. Vaikka hallitus perusteli, että kansallista lainsäädäntöä oli muutettu siten, että ihmiset voisivat pyytää henkilöllisyystodistuksen uskontokohdan jättämistä tyhjäksi, tuomioistuimen mielestä pelkästään se, että uskonnon poistamista pitäisi hakea, voisi paljastaa tietoa ihmisten asenteista uskontoon. Lisäksi, kun henkilöllisyystodistuksissa on uskontokohta, sen tyhjäksi jättäminen saa aikaan tietyn mielleyhtymän, koska ihmiset, joiden henkilöllisyystodistuksessa ei ole tietoa uskonnosta, erottautuisivat niistä, joiden todistukseen vakaumus on merkitty. Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 9 artiklaa oli rikottu.

Kirkkojen tai uskonnollisten yhdistysten tai yhteisöjen toiminta voi kuitenkin edellyttää jäsenten henkilötietojen käsittelyä, jotta seurakunnassa voidaan pitää yhteyttä ja järjestää toimintaa. Kirkot ja uskonnolliset yhdistykset ovat näin ollen usein laatineet sääntöjä henkilötietojen käsittelystä. Tällaiset säännöt voivat yleisen tietosuoja-asetuksen 91 artiklan mukaan olla edelleen päteviä, jos ne ovat kattavia, edellyttäen, että ne saatetaan asetuksen mukaisiksi. Tällaisia kattavia sääntöjä soveltavien kirkkojen ja uskonnollisten yhteisöjen on oltava sellaisen riippumattoman valvontaviranomaisen valvonnassa, joka voi olla erityisviranomainen edellyttäen, että se täyttää yleisessä tietosuoja-asetuksessa kyseisille viranomaisille vahvistetut edellytykset[119].

Uskonnolliset järjestöt voivat käsitellä henkilötietoja useista syistä, esimerkiksi pitääkseen yhteyttä seurakuntaan tai tiedottaakseen järjestettävistä uskonnollisista tapahtumista tai hyväntekeväisyystapahtumista tai juhlista. Joissakin maissa kirkkojen on pidettävä jäsenistään rekisteriä verotusta varten, koska uskonnollisten

119 Yleinen tietosuoja-asetus, 91 artiklan 2 kohta.

laitosten jäsenyys voi vaikuttaa henkilöiden verotukseen. Eurooppalaisen lainsäädännön mukaisesti uskonnolliset vakaumukset paljastavat tiedot ovat arkaluonteista tietoa, ja kirkkojen on oltava niiden hallinnoinnista ja käsittelystä osoitusvelvollisia etenkin, koska uskonnollisten järjestöjen käsittelemät tiedot koskevat usein lapsia, iäkkäitä ihmisiä tai muita yhteiskunnan heikommassa asemassa olevia jäseniä.

1.3.4 Taiteen ja tutkimuksen vapaus

Yksi oikeus, jota on punnittava suhteessa yksityiselämän ja henkilötietojen suojaa koskeviin oikeuksiin, on taiteen ja tutkimuksen vapaus, joka on nimenomaisesti turvattu perusoikeuskirjan 13 artiklassa. Tämä oikeus on johdettu pääasiallisesti oikeudesta ajatuksen- ja ilmaisunvapauteen ja sen käytössä on otettava huomioon perusoikeuskirjan 1 artikla (ihmisarvo). Euroopan ihmisoikeustuomioistuin katsoo, että taiteen vapaus on turvattu ihmisoikeussopimuksen 10 artiklalla[120]. Perusoikeuskirjan 13 artiklassa taattuun oikeuteen voidaan soveltaa myös perusoikeuskirjan 52 artiklan 1 kohdan mukaisia rajoituksia, ja sitä voidaan tulkita myös ihmisoikeussopimuksen 10 artiklan 2 kohdan perusteella[121].

Esimerkki: Asiassa *Vereinigung bildender Künstler v. Itävalta*[122] itävaltalaiset tuomioistuimet kielsivät kantajana ollutta yhdistystä jatkamasta sellaisen taulun näyttämistä, jossa oli valokuvia julkisuuden henkilöistä seksiasennoissa. Itävallan parlamentin jäsen, jonka valokuvaa oli käytetty maalauksessa, nosti kantajana ollutta yhdistystä vastaan kanteen, jolla se haki kieltomääräystä taulun näyttämiselle. Kansallinen tuomioistuin hyväksyi pyynnön ja antoi kieltomääräyksen. Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 10 artiklaa sovelletaan sellaisten ajatusten esittämiseen, jotka loukkaavat, järkyttävät tai häiritsevät valtiota tai jotain väestön osaa. Taideteoksia luovat, esittävät tai näyttävät henkilöt osallistuvat ajatusten ja näkemysten vaihtoon, ja valtiolla on velvollisuus olla rajoittamatta perusteettomasti heidän ilmaisunvapauttaan. Kun otetaan huomioon, että kyseinen taulu oli kollaasi, jossa käytettiin valokuvia ainoastaan henkilöiden päistä ja heidän vartalonsa oli maalattu epärealistisesti ja liioitellusti tavalla, jonka ei selvästi ollut tarkoitus heijastaa todellisuutta tai edes viitata todellisuuteen, EIT katsoi, ettei taulun voitu ymmärtää käsittelevän esitetyn

120 EIT, *Müller ym. v. Sveitsi*, nro 10737/84, 24.5.1988.

121 Euroopan unionin perusoikeuskirjan selitykset, EUVL 2007, C 303.

122 EIT, *Vereinigung bildender Künstler v. Itävalta*, nro 68345/01, 25.1.2007, 26 ja 34 kohta.

henkilön yksityiselämää, vaan sen oli pikemminkin ymmärrettävä liittyvän taiteilijan näkemykseen poliitikoista, ja että esitetyn henkilön oli asemansa puolesta suvaittava kritiikkiä tavallista laajemmin. Punnittuaan asiaan liittyviä erilaisia etuja EIT päätyi siihen, että taulun esittämisen rajoittamaton kielto oli suhteeton. Tuomioistuin totesi, että ihmisoikeussopimuksen 10 artiklaa oli rikottu.

Euroopan tietosuojalainsäädännössä on otettu huomioon tieteen erityinen merkitys yhteiskunnalle. Yleisessä tietosuoja-asetuksessa ja uudistetussa yleissopimuksessa 108 sallitaan tietojen säilyttäminen pidempään, kunhan henkilötietoja käsitellään ainoastaan tieteellisiä tai historiallisia tutkimustarkoituksia varten. Lisäksi, ja riippumatta tietyn käsittelytoimen alkuperäisestä tarkoituksesta, myöhempää henkilötietojen käyttöä tieteellisiä tutkimustarkoituksia varten ei saa katsoa yhteensopimattomaksi alkuperäisten tarkoitusten kanssa[123]. Samalla kyseistä käsittelyä varten on otettava käyttöön asianmukaiset suojatoimenpiteet rekisteröityjen oikeuksien ja vapauksien suojelemiseksi. EU:n tai jäsenvaltioiden lainsäädännössä voidaan säätää poikkeuksia rekisteröidyn oikeuksista, esimerkiksi oikeudesta tietoihin tutustumiseen, niiden oikaisuun ja käsittelyn rajoittamiseen ja oikeudesta vastustaa, kun kyse on rekisteröityjen henkilötietojen käsittelystä tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten (ks. myös 6.1 kohta ja 9.4 kohta).

1.3.5 Henkisen omaisuuden suoja

Oikeus omaisuudensuojaan on vahvistettu ihmisoikeussopimuksen ensimmäisen lisäpöytäkirjan 1 artiklassa ja perusoikeuskirjan 17 artiklan 1 kohdassa. Tietosuojan kannalta yksi omaisuudensuojaa koskevan oikeuden tärkeä näkökohta on oikeus teollis- ja tekijänoikeuksien turvaan, joka mainitaan erikseen perusoikeuskirjan 17 artiklan 2 kohdassa. EU:n oikeusjärjestykseen kuuluu useita direktiivejä, joilla pyritään turvaamaan tehokkaasti henkinen omaisuus, erityisesti tekijänoikeudet. Henkinen omaisuus kattaa kirjallisen ja taiteellisen omaisuuden lisäksi patentti- ja tavaramerkkioikeudet sekä niihin liittyvät oikeudet.

Kuten Euroopan unionin tuomioistuimen oikeuskäytännössä on tehty selväksi, perusoikeutta omaisuudensuojaan on punnittava suhteessa muihin perusoikeuksiin,

123 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan b alakohta, ja uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta.

erityisesti suhteessa tietosuojaa koskevaan oikeuteen[124]. Tekijänoikeusjärjestöt ovat joissakin tapauksissa vaatineet internetpalvelujen tarjoajia paljastamaan internetissä olevien tiedostojenjako-ohjelmien käyttäjien henkilöllisyyden. Tällaiset ohjelmat antavat internetin käyttäjille usein mahdollisuuden ladata musiikkikappaleita ilmaiseksi, vaikka kappaleet olisi suojattu tekijänoikeuksilla.

Esimerkki: Asiassa *Promusicae v. Telefónica de España*[125] espanjalainen internetyhteyspalvelujen tarjoaja, Telefónica, oli kieltäytynyt luovuttamasta musiikkitallenteiden ja audiovisuaalisten tallenteiden tuottajien ja julkaisijoiden voittoa tavoittelemattomalle yhdistykselle, Promusicaelle, tiettyjen sellaisten henkilöiden tietoja, joille se tarjosi internetyhteyspalveluja. Promusicae tarvitsi tietoja voidakseen panna vireille siviiliprosessit niitä henkilöitä vastaan, jotka olivat sen mukaan käyttäneet tiedostojenjako-ohjelmaa, jonka avulla oli mahdollista saada äänitteitä, joiden käyttöön liittyvät taloudelliset oikeudet kuuluivat Promusicaen jäsenille.

Espanjalainen tuomioistuin saattoi asian Euroopan unionin tuomioistuimen käsiteltäväksi ja kysyi, velvoittaako yhteisön oikeus luovuttamaan henkilötietoja siviiliprosessin yhteydessä tekijänoikeuden tehokkaan suojan varmistamiseksi. Espanjalainen tuomioistuin viittasi direktiiveihin 2000/31/EY, 2001/29/EY ja 2004/48/EY, kun niitä luetaan myös perusoikeuskirjan 17 ja 47 artiklan valossa. Euroopan unionin tuomioistuin totesi, että kyseisissä kolmessa direktiivissä sen enempää kuin sähköisen viestinnän tietosuojadirektiivissäkään (direktiivi 2002/58/EY) ei suljeta pois jäsenvaltioiden mahdollisuutta säätää velvollisuudesta paljastaa henkilötietoja siviiliprosessin yhteydessä tekijänoikeuden tehokkaan suojan varmistamiseksi.

Tuomioistuin esitti, että asiassa tuli esiin kysymys eri perusoikeuksien eli yhtäältä yksityisyyden kunnioittamista koskevan oikeuden ja toisaalta omaisuudensuojaa ja tehokkaita oikeussuojakeinoja koskevien oikeuksien suojaan liittyvien vaatimusten välttämättömästä yhteensovittamisesta.

Se totesi, että ”jäsenvaltioiden on pannessaan täytäntöön edellä mainittuja direktiivejä huolehdittava siitä, että ne nojautuvat sellaiseen kyseisten direktiivien tulkintaan, jolla voidaan varmistaa yhteisön oikeusjärjestyksessä

124 EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 29.1.2008, 62–68 kohta.

125 *Ibid.*, 54 ja 60 kohta.

suojattujen eri perusoikeuksien välinen asianmukainen tasapaino. Jäsenvaltioiden viranomaisten ja tuomioistuinten on pannessaan täytäntöön kyseisten direktiivien noudattamisen edellyttämiä toimenpiteitä tulkittava kansallista oikeuttaan mainittujen direktiivien mukaisesti, ja niiden on tämän lisäksi myös varottava nojautumasta sellaiseen kyseisten direktiivien tulkintaan, joka johtaisi ristiriitaan mainittujen perusoikeuksien kanssa tai muiden yhteisön oikeuden yleisten periaatteiden, kuten suhteellisuusperiaatteen, kanssa."[126]

Esimerkki: Asiassa *Bonnier Audio AB ym. v. Perfect Communication Sweden AB*[127] punnittiin teollis- ja tekijänoikeuksia suhteessa henkilötietojen suojaan. Kantajina oli viisi kustantamoa, joilla oli tekijänoikeudet 27 äänikirjaan. Ne veivät asian ruotsalaiseen tuomioistuimeen, koska ne katsoivat, että näitä tekijänoikeuksia oli loukattu käyttäen FTP-palvelinta (tiedonsiirtoprotokolla, joka mahdollistaa tiedostojen jakamisen ja tietojen siirron internetissä). Kantajat pyysivät internetyhteyden tarjoajaa ilmoittamaan sen henkilön nimen ja osoitteen, joka käyttää IP-osoitetta, jonka kautta kyseiset tiedostot lähetettiin. Internetyhteyden tarjoaja ePhone riitautti kanteen ja väitti, että se on direktiivin 2006/24/EY (tietojen säilyttämistä koskeva direktiivi – tullut pätemättömäksi vuonna 2014) vastainen.

Ruotsalainen tuomioistuin vei asian Euroopan unionin tuomioistuimen käsiteltäväksi ja kysyi, onko direktiivi 2006/24/EY esteenä sellaisen kansallisen säännöksen soveltamiselle, joka on annettu direktiivin 2004/48/EY (teollis- ja tekijänoikeuksien noudattamisen varmistamisesta annettu direktiivi) 8 artiklan nojalla ja jonka mukaan internetyhteyden tarjoaja voidaan määrätä antamaan tekijänoikeuden haltijalle tieto tilaajista, joiden IP-osoitteita on väitetysti käytetty rikkomuksiin. Kysymys perustui olettamaan, jonka mukaan kantaja on esittänyt selkeät todisteet tietyn tekijänoikeuden rikkomisesta ja että toimenpide on oikeasuhteinen.

Euroopan unionin tuomioistuin huomautti, että direktiivi 2006/24/EY koskee yksinomaan sähköisten viestintäpalvelujen tarjoajien tuottamien tietojen käsittelemistä ja säilyttämistä vakavan rikollisuuden tutkintaa, selvittämistä ja syyteharkintaa varten sekä niiden toimittamista toimivaltaisille kansallisille

126 *Ibid.*, 65 ja 68 kohta; ks. myös EUT, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vastaan Netlog NV*, 16.2.2012.

127 EUT, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB v. Perfect Communication Sweden AB*, 19.4.2012.

viranomaisille. Näin ollen kansallinen säännös, jolla saatetaan teollis- ja tekijänoikeuksien noudattamisen varmistamisesta annettu direktiivi osaksi kansallista lainsäädäntöä, ei kuulu direktiivin 2006/24/EY soveltamisalaan, eikä kyseinen direktiivi ole siten esteenä sen soveltamiselle.[128]

Kyseessä olevan nimen ja osoitteen luovuttamisen osalta Euroopan unionin tuomioistuin totesi, että tällainen toiminta on henkilötietojen käsittelyä ja kuuluu siis direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi) soveltamisalaan. Se totesi myös, että näiden tietojen luovuttamista vaadittiin riita-asian oikeudenkäynnissä tekijänoikeuden haltijalle, jotta voidaan varmistaa tekijänoikeuksien tehokas suojaaminen. Näin ollen se kuuluu kohteensa vuoksi myös direktiivin 2004/48/EY soveltamisalaan.[129]

Euroopan unionin tuomioistuin totesi, että direktiivejä 2002/58/EY ja 2004/48/EY on tulkittava siten, ettei pääasiassa kyseessä olevan kaltainen kansallinen lainsäädäntö ole niiden kanssa ristiriidassa, koska kansallinen tuomioistuin, jonka käsiteltäväksi on saatettu asiavaltuuden omaavan henkilön vaatimus henkilötietojen antamista koskevasta määräyksestä, voi tämän lainsäädännön nojalla punnita asiaan liittyviä vastakkaisia etuja jokaisen yksittäistapauksen olosuhteiden mukaan ja ottaen asianmukaisesti huomioon suhteellisuusperiaatteesta johtuvat vaatimukset.

1.3.6 Tietosuoja ja taloudelliset edut

Digitaaliajalla tai massadatan aikakaudella tietoa on kuvattu talouden ”uudeksi öljyksi”, joka vauhdittaa innovointia ja luovuutta[130]. Monet yritykset ovat laatineet tietojenkäsittelystä kokonaisvaltaisia liiketoimintamalleja, ja kyseiseen käsittelyyn kuuluu usein henkilötietoja. Tietyt yritykset voivat katsoa, että henkilötietojen suojaan liittyvät erityiset säännöt voivat käytännössä johtaa liian rasittaviin velvoitteisiin, jotka voivat vaikuttaa niiden taloudellisiin etuihin. Se herättää kysymyksen, voidaanko rekisterinpitäjien ja henkilötietojen käsittelijöiden tai suuren yleisön taloudellisilla eduilla perustella tietosuojaa koskevan oikeuden rajoittaminen.

128 *Ibid.*, 40–41 kohta.

129 *Ibid.*, 52–54 kohta. Ks. myös EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 29.1.2008, 58 kohta.

130 Ks. esim., *Financial Times* (2016), ”Data is the new oil… who’s going to own it?”, 16.11.2016.

Esimerkki: Asiassa *Google Spain*[131] Euroopan unionin tuomioistuin totesi, että tietyissä olosuhteissa yksilöillä on oikeus pyytää hakukoneita poistamaan hakutuloksia hakuluettelostaan. Perusteluissaan tuomioistuin kiinnitti huomiota siihen, että hakukoneiden käytön ja lueteltujen hakutulosten avulla voidaan laatia yksityiskohtainen profiili henkilöstä. Nämä tiedot voivat koskea useita eri seikkoja henkilön yksityiselämässä, ja niitä olisi ilman hakukonetta ollut hyvin hankala löytää tai yhdistää toisiinsa. Ne voivat näin ollen merkitä vakavaa puuttumista rekisteröityjen yksityisyydensuojaa ja henkilötietojen suojaa koskeviin perusoikeuksiin.

Tuomioistuin tutki, voidaanko puuttuminen perustella. Euroopan unionin tuomioistuin totesi hakukoneen ylläpitäjän tekemää käsittelyä koskevan taloudellisen edun osalta, ”ettei [puuttumista] voida perustella hakukoneen ylläpitäjällä tällaiseen käsittelyyn olevalla pelkällä taloudellisella intressillä”, ja että ”lähtökohtaisesti” perusoikeuskirjan 7 ja 8 artiklan mukaiset oikeudet syrjäyttävät kyseisen intressin sekä suurella yleisöllä olevan intressin löytää mainitut tiedot tehdessään haun rekisteröidyn nimellä[132].

Yksi EU:n tietosuojalainsäädännön keskeisistä kohdista on lisätä valtaa, jota yksilöillä on henkilötietoihinsa. Etenkin digitaaliajalla liiketoimintayhteisöillä, jotka käsittelevät ja pitävät hallussaan valtavia määriä henkilötietoja, ja henkilöillä, joille kyseiset henkilötiedot kuuluvat, on hyvin erilaiset valtuudet hallita tietojaan. Euroopan unionin tuomioistuin punnitsee tietosuojaa ja taloudellisia etuja tapauskohtaisesti. Niihin kuuluvat muun muassa kolmansien osapuolten edut osakeyhtiöissä ja rajavastuuyhtiöissä, kuten asiassa *Manni* annettu tuomio havainnollistaa.

Esimerkki: Asiassa *Manni*[133] oli kyse yksilön henkilötietojen sisällyttämisestä julkiseen kaupalliseen rekisteriin. Salvatore Manni oli pyytänyt Leccen kauppakamaria poistamaan hänen henkilötietonsa kyseisestä rekisteristä, kun hän oli havainnut, että mahdolliset asiakkaat tutustuisivat rekisteriin ja näkisivät, että hän oli ollut konkurssipesän hoitaja yhtiössä, joka oli julistettu

131 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014.

132 *Ibid.*, 81 ja 97 kohta.

133 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9.3.2017.

konkurssiin yli kymmenen vuotta sitten. Nämä tiedot vaikuttivat hänen mahdollisiin asiakkaisiinsa, ja niillä voisi olla kielteinen vaikutus hänen kaupallisiin etuihinsa.

Euroopan unionin tuomioistuinta pyydettiin määrittämään, tunnustetaanko EU:n oikeudessa tässä tapauksessa oikeus poistamiseen. Johtopäätöksen aikaansaamiseksi se punnitsi EU:n tietosuojasääntöjä ja kantaja Mannin kaupallista intressiä poistaa tiedot entisen yhtiönsä konkurssista suhteessa yleiseen intressiin saada tietoa. Se otti asianmukaisesti huomioon, että tietojen julkistamisesta julkiseen yhtiörekisteriin säädettiin lailla ja erityisesti EU:n direktiivillä, jonka tavoitteena on edesauttaa yhtiöitä koskevien tietojen saamista ulkopuolisten henkilöiden saataville helpommin. Tietojen julkistaminen oli tärkeää sellaisten ulkopuolisten henkilöiden etujen suojaamiseksi, jotka ehkä haluavat harjoittaa liiketoimintaa tietyn yhtiön kanssa, koska osakeyhtiöiden ja rajavastuuyhtiöiden ainoana takeena ulkopuolisille henkilöille on niiden yhtiövarallisuus. Näin ollen ”tärkeimmät yhtiötä koskevat asiakirjat olisi julkistettava tätä tarkoitusta varten, jotta ulkopuoliset henkilöt voivat tutustua niihin ja saada tietoja yhtiöstä ja erityisesti siitä, keillä on oikeus edustaa yhtiötä”.[134]

Rekisterin laillisen tavoitteen merkityksen vuoksi Euroopan unionin tuomioistuin totesi, että kantaja Mannilla ei ollut oikeutta saada henkilötietojaan poistetuksi, koska tarve suojata ulkopuolisten henkilöiden etuja suhteessa osakeyhtiöihin ja rajavastuuyhtiöihin ja turvata oikeusvarmuus, rehellinen kaupankäynti ja siten sisämarkkinoiden moitteeton toiminta olivat ensisijaisia suhteessa hänen tietosuojalainsäädännön mukaisiin oikeuksiinsa. Tämä päti erityisesti sen vuoksi, että luonnolliset henkilöt, jotka päättävät osallistua liiketoimintaan osakeyhtiön tai rajavastuuyhtiön avulla, ovat tietoisia velvollisuudestaan julkistaa tietoja, jotka koskevat heidän henkilötietojaan ja tehtäviään yhtiössä.

Vaikka Euroopan unionin tuomioistuin katsoi, että tässä asiassa ei ollut perusteita saada tietoja poistetuksi, se tunnusti, että käsittelyä voi vastustaa ja totesi seuraavaa: ”ei voida [...] sulkea pois sitä, että saattaa olla erityisiä tilanteita, joissa kyseisen henkilön konkreettiseen tilanteeseen liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi on poikkeuksellisesti

134 *Ibid.*, 49 kohta.

oikeutettua, että oikeus saada yhtiörekisteriin merkittyjä häntä koskevia henkilötietoja annetaan riittävän pitkän ajan kuluttua [...] käytettäviksi vain ulkopuolisille, joilla on erityinen intressi tutustua niihin"[135].

Euroopan unionin tuomioistuin totesi, että kansallisten tuomioistuinten asiana on arvioida kukin tapaus ja arvioida kaikkien yksilön kannalta merkityksellisten seikkojen perusteella, onko mahdollisesti olemassa sellaisia huomattavan tärkeitä ja perusteltuja syitä, joiden vuoksi voi olla poikkeuksellisesti oikeutettua rajoittaa ulkopuolisten oikeutta saada yhtiörekisteriin merkittyjä tietoja. Se selvensi kuitenkin, että kantaja Mannin tapauksessa pelkästään se seikka, että on väitetty, että hänen henkilötietojensa julkistaminen rekisterissä vaikutti hänen asiakaskuntaansa, ei voi riittää tällaiseksi huomattavan tärkeäksi ja perustelluksi syyksi. Kantaja Mannin mahdollisilla asiakkailla on oikeutettu intressi hänen entisen yhtiönsä konkurssia koskevien tietojen saamiseen.

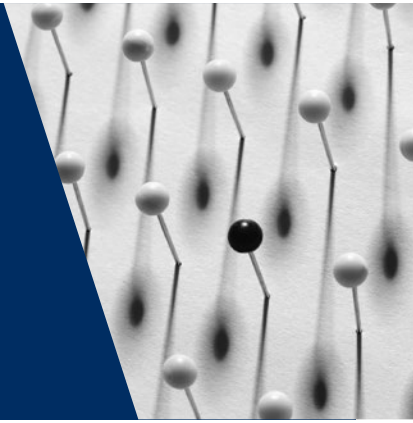
Puuttumisella kantaja Mannin ja muiden rekisterissä olevien henkilöiden perusoikeuskirjan 7 ja 8 artiklassa vahvistettuihin yksityiselämän kunnioittamista ja henkilötietojen suojaa koskeviin perusoikeuksiin oli yleisen edun mukainen tavoite, ja se oli välttämätöntä ja oikeasuhteista.

Näin ollen Euroopan unionin tuomioistuin totesi asiassa *Manni*, että tietosuojaa ja yksityisyydensuojaa koskevat oikeudet eivät olleet tärkeämpiä kuin kolmansien osapuolten intressi saada yhtiörekisterin tietoja osakeyhtiöistä ja rajavastuuyhtiöistä.

135 *Ibid.*, 60 kohta.

2

Tietosuojaan liittyvä terminologia



EU	Käsiteltävät asiat	EN
Henkilötiedot		
Yleinen tietosuoja-asetus, 4 artiklan 1 kohta Yleinen tietosuoja-asetus, 4 artiklan 5 kohta ja 5 artiklan 1 kohdan e alakohta Yleinen tietosuoja-asetus, 9 artikla EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 2010 EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 2008 EUT, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 EUT, C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 2016 EUT, yhdistetyt asiat C-141/12 ja C-372/12, YS v. *Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel v. M ja S*, 2014	**Tietosuojan oikeudellinen määritelmä**	Uudistettu yleissopimus 108, 2 artiklan a alakohta EIT, *Bernh Larsen Holding AS ym. v. Norja*, nro 24117/08, 2013 EIT, *Uzun v. Saksa*, nro 35623/05, 2010 EIT, *Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 2000
EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 2003	**Erityiset tietoryhmät (arkaluonteiset tiedot)**	Uudistettu yleissopimus 108, 6 artiklan 1 kohta

EU	Käsiteltävät asiat	EN
EUT, C-434/16, *Peter Nowak v. Data Protection Commissioner*, 2017	**Anonyymit ja pseudo-nymisoidut tiedot**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan e alakohta Uudistettu yleissopimus 108, selitysmuistio, 50 artikla
Tietojenkäsittely		
Yleinen tietosuoja-asetus, 4 artiklan 2 kohta EUT, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 2014 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 2003 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 2014	**Määritelmät**	Uudistettu yleissopimus 108, 2 artiklan b ja c alakohta
Tietojen käyttäjät		
Yleinen tietosuoja-asetus, 4 artiklan 7 kohta EUT, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 2014 EUT, C-1318/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 2014	**Rekisterinpitäjä**	Uudistettu yleissopimus 108, 2 artiklan d alakohta Profilointia koskeva suositus, 1 artiklan g alakohta*
Yleinen tietosuoja-asetus, 4 artiklan 8 kohta	**Henkilötietojen käsittelijä**	Uudistettu yleissopimus 108, 2 artiklan f alakohta Profilointia koskeva suositus, 1 artiklan h alakohta
Yleinen tietosuoja-asetus, 4 artiklan 9 kohta	**Vastaanottaja**	Uudistettu yleissopimus 108, 2 kohdan e alakohta
Yleinen tietosuoja-asetus, 4 artiklan 10 kohta	**Kolmas osapuoli**	

EU	Käsiteltävät asiat	EN
Suostumus		
Yleinen tietosuoja-asetus, 4 artiklan 11 kohta ja 7 artikla EUT, C-543/09, *Deutsche Telekom AG vastaan Bundesrepublik Deutschland*, 2011 EUT, C-536/15, *Tele2 (Netherlands) BV ym. vastaan Autoriteit Consument en Markt (AMC)*, 2017	Pätevän suostumuksen määritelmä ja edellytykset	Uudistettu yleissopimus 108, 5 artiklan 2 kohta Potilastietoja koskeva suositus, 6 artikla, ja erilaisia muita suosituksia EIT, *Elberte v. Latvia*, nro 61243/08, 13.1.2015

*Huom. * Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä (profilointia koskeva suositus), 23. marraskuuta 2010.*

2.1 Henkilötiedot

Keskeiset kohdat

- Tiedot ovat henkilötietoja, jos ne koskevat tunnistettua tai tunnistettavissa olevaa henkilöä, eli rekisteröityä.
- Jotta voidaan määrittää, onko luonnollinen henkilö tunnistettavissa, olisi otettava huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuullisen todennäköisesti käyttää mainitun luonnollisen henkilön tunnistamiseen suoraan tai välillisesti, kuten kyseisen henkilön erottaminen muista.
- Todentaminen tarkoittaa sen todistamista, että tietyllä henkilöllä on tietty henkilöllisyys ja/tai lupa toteuttaa tiettyjä toimintoja.
- Uudistetussa yleissopimuksessa 108 ja EU:n tietosuojalainsäädännössä on lueteltu erityisiä tietoryhmiä, niin kutsuttuja arkaluonteisia tietoja, jotka vaativat vahvempaa suojaa ja joihin siksi sovelletaan erityistä oikeudellista järjestelmää.
- Tiedot on tehty anonyymeiksi, jos ne eivät enää liity tunnistettuun tai tunnistettavissa olevaan henkilöön.
- Pseudonymisointi on toimenpide, jossa henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, jotka säilytetään erillään. ”Avain”, jolla rekisteröidyt voidaan tunnistaa uudelleen, on säilytettävä erillään ja suojassa. Pseudonymisoidut tiedot ovat edelleen henkilötietoja. EU:n lainsäädännössä ei ole ”pseudonymisoitujen tietojen” käsitettä.
- Tietosuojan periaatteita ja sääntöjä ei sovelleta anonyymeihin tietoihin. Pseudonymisoituihin tietoihin niitä kuitenkin sovelletaan.

2.1.1 Henkilötietojen käsitteen tärkeimmät näkökohdat

EU:n oikeudessa samoin kuin **Euroopan neuvoston oikeudessa** henkilötiedot määritellään tiedoiksi, jotka koskevat tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä[136]. Ne ovat tietoja henkilöstä, jonka henkilöllisyys joko on ilmeisen selvä tai se voidaan saada selville lisätiedoista. Jotta voidaan määrittää, onko henkilö tunnistettavissa, on otettava huomioon kaikki keinot, joita joko rekisterinpitäjä tai muu henkilö voi kohtuullisen todennäköisesti käyttää mainitun luonnollisen henkilön tunnistamiseen suoraan tai välillisesti, kuten kyseisen henkilön erottaminen muista[137].

Jos tällaista henkilöä koskevia tietoja käsitellään, henkilöstä käytetään nimitystä ”rekisteröity”.

Rekisteröity

EU:n oikeuden mukaan tietosuojaa sovelletaan vain luonnollisiin henkilöihin[138] ja EU:n tietosuojalainsäädäntö suojelee vain eläviä olentoja[139]. Yleisessä tietosuoja-asetuksessa henkilötiedot määritellään kaikiksi tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviksi tiedoiksi.

Euroopan neuvoston oikeudessa, erityisesti uudistetussa yleissopimuksessa 108, viitataan myös yksilöiden suojeluun heidän henkilötietojensa käsittelyssä. Myös siinä henkilötiedot tarkoittavat kaikkia tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön liittyviä tietoja. Tämä henkilö, johon yleisessä tietosuoja-asetuksessa viitataan luonnollisena henkilönä ja uudistetussa yleissopimuksessa 108 yksilönä, tunnetaan tietosuojalainsäädännössä rekisteröitynä.

Myös oikeushenkilöillä on jonkin verran suojaa. Euroopan ihmisoikeustuomioistuin on oikeuskäytännössään ratkaissut asioita, joissa oikeushenkilöt ovat kanteessaan väittäneet, että niiden ihmisoikeussopimuksen 8 artiklan mukaista oikeutta yksityiselämän suojaan on rikottu. Ihmisoikeussopimuksen 8 artikla kattaa oikeuden nauttia sekä yksityis- ja perhe-elämään että kotiin ja kirjeenvaihtoon kohdistuvaa

136 Yleinen tietosuoja-asetus, 4 artiklan 1 kohta, uudistettu yleissopimus 108, 2 artiklan a alakohta.

137 Yleinen tietosuoja-asetus, johdanto-osan 26 kappale.

138 *Ibid.*, 1 artikla

139 *Ibid.*, johdanto-osan 27 kappale. Ks. myös tietosuojatyöryhmä *(2007), lausunto 4/2007 henkilötietojen käsitteestä*, WP 136, 20.6.2007, s. 22.

kunnioitusta. Tuomioistuin voi siksi tutkia asioita kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta muttei yksityiselämän kunnioitusta koskevan oikeuden nojalla.

Esimerkki: Asiassa *Bernh Larsen Holding AS ym. v. Norja*[140] kolme norjalaista yritystä oli tehnyt valituksen veroviranomaisen päätöksestä, jolla ne määrättiin toimittamaan verotarkastajille jäljennös kaikista niiden yhteisessä käytössä olleella palvelimella olleista tiedoista.

Euroopan ihmisoikeustuomioistuin totesi, että tällainen kantajina olleille yrityksille määrätty velvollisuus rikkoi ihmisoikeussopimuksen 8 artiklassa tarkoitettua oikeutta nauttia ”kotiin” ja ”kirjeenvaihtoon” kohdistuvaa kunnioitusta. Tuomioistuin kuitenkin katsoi, että veroviranomaisilla oli tehokkaat ja riittävät suojatoimet väärinkäytöksiä vastaan: kantajina olleille yrityksille oli ilmoitettu asiasta hyvissä ajoin; ne olivat läsnä ja saivat esittää huomioita, kun paikalla tehty tarkastus toteutettiin; ja aineisto oli määrä tuhota sen jälkeen, kun verotarkastus olisi saatettu päätökseen. Näissä olosuhteissa kantajina olleiden yritysten oikeus nauttia kotiin ja kirjeenvaihtoon kohdistuvaa kunnioitusta oli saatettu asianmukaisesti tasapainoon yhtäältä sen intressin kanssa, joka yrityksillä on työntekijöiden yksityisyyden suojaamisessa, ja toisaalta sen yleisen intressin kanssa, joka on verojen arviointiin tarvittavan tehokkaan tarkastuksen varmistaminen. Tuomioistuin katsoi näin ollen, ettei ihmisoikeussopimuksen 8 artiklaa ollut rikottu.

Uudistetun yleissopimuksen 108 mukaan tietosuoja koskee ensisijaisesti luonnollisia henkilöitä; sopimuspuolet voivat kuitenkin kansallisessa lainsäädännössään ulottaa tietosuojan oikeushenkilöihin, kuten yrityksiin ja yhdistyksiin. Uudistetun yleissopimuksen selitysmuistiossa todetaan, että kansallisella lainsäädännöllä voidaan suojata oikeushenkilöiden oikeutettuja etuja laajentamalla yleissopimuksen soveltamisala kyseisiin toimijoihin[141]. **EU:n tietosuojalainsäädäntö** ei koske oikeushenkilöiden ja erityisesti oikeushenkilön muodossa perustettujen yritysten henkilötietojen käsittelyä, kuten oikeushenkilön nimeä, oikeudellista muotoa ja yhteystietoja[142]. Sähköisen viestinnän tietosuojadirektiivillä kuitenkin suojataan viestinnän luottamuksellisuutta ja oikeushenkilöiden oikeutettuja etuja tilaajia ja käyttäjiä koskevien

140 EIT, *Bernh Larsen Holding AS ym. v. Norja*, No. 24117/08, 14.3.2013. Ks. kuitenkin myös EIT, *Liberty ym. v. Yhdistynyt kuningaskunta*, nro 58243/00, 1.7.2008.

141 Uudistettu yleissopimus 108, selitysmuistio, 30 kohta.

142 Yleinen tietosuoja-asetus, johdanto-osan 14 kappale.

tietojen automaattisen tallennus- ja käsittelykapasiteetin lisääntymisen osalta[143]. Myös sähköisen viestinnän tietosuoja-asetusta koskevassa ehdotuksessa suoja ulotetaan oikeushenkilöihin.

Esimerkki: Yhdistetyissä asioissa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*[144] Euroopan unionin tuomioistuin totesi maatalousrahastojen tuensaajien henkilötietojen julkaisemisen osalta, että ”oikeushenkilöt voivat vedota tällaisen yksilöinnin kannalta perusoikeuskirjan 7 ja 8 artiklan mukaiseen suojaan vain siltä osin kuin oikeushenkilön virallisessa nimessä yksilöidään yksi tai usea luonnollinen henkilö. […] Perusoikeuskirjan 7 ja 8 artiklassa tunnustettu oikeus yksityiselämän kunnioittamiseen henkilötietojen käsittelyssä koskee kaikenlaisia tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevia tietoja […].”[145]

Punnitessaan toisaalta EU:n intressiä taata toimiensa avoimuus tuen osoittamisessa ja toisaalta tuensaajien perusoikeuksia yksityisyyden suojaan ja tietosuojaan Euroopan unionin katsoi, että puuttuminen kyseisiin perusoikeuksiin oli suhteetonta. Se katsoi, että avoimuustavoite olisi tosiasiallisesti voitu saavuttaa toimenpiteillä, joilla loukattaisiin vähemmän kyseisten yksilöiden oikeuksia. Tutkiessaan tukea saaneita oikeushenkilöitä koskevien tietojen julkaisemisen oikeasuhteisuutta Euroopan unionin tuomioistuin päätyi kuitenkin erilaiseen johtopäätökseen ja totesi, että kyseinen julkaisu ei ylittänyt suhteellisuusperiaatteen rajoja. Se totesi, että ”henkilötietojen suojaa koskevan oikeuden loukkauksen vakavuus ei nimittäin ole oikeushenkilöiden osalta sama kuin luonnollisten henkilöiden osalta”[146]. Oikeushenkilöitä koskee laajennettu velvollisuus julkaista itseään koskevia tietoja. Euroopan unionin tuomioistuin totesi, että kansallisten viranomaisten velvollisuus tutkia, yksilöidäänkö kunkin tukea saavan oikeushenkilön tiedoissa asiaan liittyviä luonnollisia henkilöitä ennen kyseessä olevien tietojen julkaisemista, aiheuttaisi näille viranomaisille kohtuuttoman hallinnollisen rasituksen. Näin ollen säännöksissä, joissa edellytetään oikeushenkilöihin liittyvien tietojen yleistä julkistamista, on löydetty oikea tasapaino kyseessä olevien intressien välillä.

143 Sähköisen viestinnän tietosuojadirektiivi, johdanto-osan 7 kappale ja 1 artiklan 2 kohta.

144 EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010, 53 kohta.

145 *Ibid.*, 52–53 kohta.

146 *Ibid.*, 87 kohta.

Tietojen luonne

Kaikenlaiset tiedot voivat olla henkilötietoja, jos ne liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön.

Esimerkki: Työntekijän henkilökansioon tallennettu esimiehen arvio työntekijän työsuorituksesta on työntekijää koskeva henkilötieto, vaikka se vain kuvastaisi osittain tai kokonaisuudessaan esimiehen henkilökohtaista näkemystä, esimerkiksi näin: ”työntekijä ei ole omistautunut työlleen” – eikä paljastaisi tosiseikkoja, esimerkiksi näin: ”työntekijä on ollut viimeisen puolen vuoden aikana viisi viikkoa poissa töistä”.

Henkilötietoihin kuuluvat tiedot, jotka liittyvät henkilön yksityiselämään, samoin kuin tiedot hänen työelämästään tai julkisesta elämästään.

Asiassa *Amann*[147] Euroopan ihmisoikeustuomioistuin tulkitsi henkilötietojen käsitettä siten, että se ei rajoittunut henkilön yksityisasioihin. Tämä termin ”henkilötiedot” merkitys on olennainen myös yleisen tietosuoja-asetuksen näkökulmasta:

Esimerkki: Yhdistetyissä asioissa *Volker und Markus Schecke ja Hartmut Eifert v. Land Hessen*[148] Euroopan unionin tuomioistuin totesi seuraavaa: ”Tässä on merkityksetöntä, että julkaistavat tiedot liittyvät ammattitoimintaan […]. Euroopan ihmisoikeustuomioistuin on tältä osin todennut Euroopan ihmisoikeussopimuksen 8 artiklan tulkinnasta, ettei ilmaisua ’yksityiselämä’ pidä tulkita suppeasti ja ettei mikään periaatteellinen syy salli sitä, että ammattitoiminta jätettäisiin […] ’yksityiselämän’ käsitteen ulkopuolelle.”

Esimerkki: Yhdistetyissä asioissa *YS v. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel v. M ja S*[149] Euroopan unionin tuomioistuin totesi, että oleskelulupahakemuksia käsittelevän maahanmuutto- ja kansalaisuusviraston päätösluonnokseen sisältyvä oikeudellinen arviointi ei itsessään ole henkilötieto, vaikka siihen voi sisältyä henkilötietoja.

147 Ks. EIT, *Amann v. Sveitsi*, nro 27798/95, 16.2.2000, 65 kohta.

148 EUT, yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010, 59 kohta.

149 EUT, yhdistetyt asiat C-141/12 ja C-372/12, *YS v. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel v. M ja S*, 17.7.2014, 39 kohta.

Ihmisoikeussopimuksen 8 artiklaa koskevasta Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä ilmenee, että yksityis- ja työelämää voi toisinaan olla vaikea erottaa selkeästi toisistaan[150].

Esimerkki: Asiassa *Bărbulescu v. Romania*[151] kantaja oli irtisanottu, koska hän oli käyttänyt työnantajansa verkkoyhteyttä työaikana sisäisten määräysten vastaisesti. Työnantaja oli seurannut hänen viestintäänsä, ja kansallisessa oikeudenkäynnissä esitettiin asiakirjoja täysin yksityisistä viesteistä. Euroopan ihmisoikeustuomioistuin katsoi, että 8 artiklaa voidaan soveltaa, mutta jätti avoimeksi kysymyksen siitä, jättivätkö työnantajan rajoittavat määräykset kantajalle kohtuullisen odotuksen yksityisyydestä. Joka tapauksessa se totesi, että yksityistä sosiaalista elämää työpaikalla ei voida työnantajan ohjeilla vähentää olemattomaan. Pääasian osalta sopimuspuolille piti antaa laaja harkintavalta sen arvioimiseksi, onko laadittava oikeudellinen kehys ehdoille, joiden mukaan työnantaja voisi säännellä työntekijöidensä sähköistä ja muuta työhön kuulumatonta viestintää työpaikalla. Kansallisten viranomaisten piti joka tapauksessa varmistaa, että jos työnantaja ottaa käyttöön toimenpiteitä, joilla valvotaan kirjeenvaihtoa ja muuta viestintää, toimenpiteisiin on niiden laajuudesta ja kestosta riippumatta kuuluttava asianmukaiset ja riittävät takeet väärinkäyttöä vastaan. Suhteellisuus ja menettelytakeet mielivaltaisuudelta olivat olennaisen tärkeitä, ja Euroopan ihmisoikeustuomioistuin yksilöi useita olosuhteiden kannalta merkityksellisiä tekijöitä. Tällaisia tekijöitä olivat esimerkiksi se, miten kattavasti työnantaja valvoo työntekijöitä ja miten paljon työntekijän yksityisyyteen puututaan, ja lisäksi seuraukset työntekijälle sekä se, onko riittävät suojatoimet otettu käyttöön. Kansallisten viranomaisten piti lisäksi varmistaa, että työntekijällä, jonka viestintää oli valvottu, oli saatavillaan oikeussuojakeinoja oikeusviranomaisessa, jonka valtuuksiin kuului määrittää, ainakin pääkohdiltaan, miten annettuja kriteereitä noudatettiin ja olivatko kiistanalaiset toimenpiteet lainmukaisia. Tässä tapauksessa Euroopan ihmisoikeustuomioistuin totesi, että 8 artiklaa oli rikottu, koska kansalliset viranomaiset eivät olleet taanneet riittävää suojaa kantajan oikeudelle nauttia yksityis- ja perhe-elämään ja kirjeenvaihtoon kohdistuvaa kunnioitusta eivätkä siksi olleet pystyneet löytämään oikeaa tasapainoa kyseessä olevien intressien välille.

150 Ks. esim. EIT, *Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000, 43 kohta; EIT, *Niemietz v. Saksa*, nro 13710/88, 16.12.1992, 29 kohta.

151 EIT, *Bărbulescu v. Romania* [suuri jaosto], nro 61496/08, 5.9.2017, 121 kohta.

Sekä **EU:n oikeudessa** että **Euroopan neuvoston oikeudessa** tieto sisältää henkilötietoja, jos

- henkilö on tunnistettu tai hänet voidaan tunnistaa näiden tietojen nojalla tai
- henkilöä ei ole tunnistettu, mutta hänet voidaan erottaa näiden tietojen perusteella siten, että rekisteröidyn selville saaminen on mahdollista tiettyjen lisätoimenpiteiden avulla.

Molemmat näistä tiedon muodoista on suojattu Euroopan tietosuojaa koskevissa säädöksissä. Yksilöiden suora tai välillinen tunnistettavuus edellyttää jatkuvaa arviointia, jossa olisi otettava huomioon ”käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys”[152]. Euroopan ihmisoikeustuomioistuin on useasti todennut, että henkilötietojen käsite on yleissopimuksessa 108 sama kuin ihmisoikeussopimuksessa, erityisesti siltä osin, kuin niiden edellytetään viittaavan tunnistettuihin tai tunnistettaviin henkilöihin[153].

Yleisen tietosuoja-asetuksen mukaan ”tunnistettavissa olevana pidetään luonnollista henkilöä, joka voidaan suoraan tai epäsuorasti tunnistaa erityisesti tunnistetietojen, kuten nimen, henkilötunnuksen, sijaintitiedon, verkkotunnistetietojen taikka yhden tai useamman hänelle tunnusomaisen fyysisen, fysiologisen, geneettisen, psyykkisen, taloudellisen, kulttuurillisen tai sosiaalisen tekijän perusteella”[154]. Tunnistaminen edellyttää näin ollen henkilön kuvaamista tavalla, joka erottaa hänet kaikista muista henkilöistä ja mahdollistaa hänen yksilöimisensä. Henkilön nimi on hyvä esimerkki tällä tavalla kuvaavasta tiedosta. Sen perusteella henkilö voidaan tunnistaa suoraan. Joissakin tapauksissa muilla tunnisteilla voi olla samanlainen vaikutus kuin nimellä. Silloin henkilö tunnistetaan välillisesti. Henkilö voidaan tunnistaa esimerkiksi puhelinnumeron, sosiaaliturvanumeron ja rekisterinumeron perusteella. Tietokoneen tiedostojen, evästeiden ja verkkoliikenteen valvontavälineiden kaltaisten ominaisuuksien avulla yksilöitä voidaan erottaa, kun tunnistetaan heidän käytöksensä ja tapansa. Tietosuojatyöryhmän lausunnossa selitetään seuraavasti: ”Edes kysymättä henkilön nimeä ja osoitetta hänet voidaan luokitella sosioekonomisin, psykologisin, filosofisin tai muin perustein ja hänen voidaan katsoa tekevän tietynlaisia päätöksiä, koska henkilön yhteydenottoväline (tietokone) ei enää

152 Yleinen tietosuoja-asetus, johdanto-osan 26 kappale.

153 Ks. EIT, *Amann v. Sveitsi* [suuri jaosto], nro 27798/95, 16.2.2000, 65 kohta.

154 Yleinen tietosuoja-asetus, 4 artiklan 1 kohta.

välttämättä edellytä henkilöllisyyden paljastamista suppeassa mielessä."[155] Sekä Euroopan neuvoston että EU:n määritelmä henkilötiedoista on riittävän laaja kattamaan kaikki tunnistamismahdollisuudet (ja siten kaikki tunnistettavuuden tasot).

Esimerkki: Asiassa *Promusicae v. Telefónica de España*[156] Euroopan unionin tuomioistuin totesi, että "on kiistatonta, että Promusicaen vaatima [tietyn tiedostojen jako-ohjelman] tiettyjen käyttäjien nimien ja osoitteiden luovuttaminen merkitsee henkilötietojen eli direktiivin 95/46 2 artiklan a alakohdassa [tällä hetkellä yleisen tietosuoja-asetuksen 4 artiklan 1 kohdassa] olevan määritelmän mukaisesti tunnistettua tai tunnistettavissa olevaa luonnollista henkilöä koskevien tietojen käyttöön antamista. Niiden tietojen luovuttaminen, jotka Telefónica on Promusicaen mukaan tallentanut – mitä Telefónica ei ole kiistänyt – on [...] henkilötietojen käsittelyä."[157]

Esimerkki: Asiassa *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] oli kyse siitä, että internetyhteyden tarjoaja Scarlet oli kieltäytynyt asentamasta järjestelmää, jolla suodatetaan tiedostonjako-ohjelmistoa käyttävää sähköistä viestintää, jotta voidaan estää tiedostonjako, joka loukkaa musiikkiteosten tekijöitä, säveltäjiä ja tuottajia edustavan tekijänoikeusjärjestön suojaamaa tekijänoikeutta. Euroopan unionin tuomioistuin totesi, että IP-osoitteet "ovat suojattuja henkilötietoja, koska niiden avulla mainitut käyttäjät on mahdollista tunnistaa täsmällisesti".

Monet nimet eivät ole ainutlaatuisia ja siksi voidaan tarvita muita tunnisteita, jotta varmistettaisiin, ettei henkilöllisyyksissä tapahdu sekaannuksia. Joskus on ehkä yhdistettävä suoria ja välillisiä tunnisteita, jotta voidaan tunnistaa yksilö, jota tiedot koskevat. Syntymäaikaa ja -paikkaa käytetään usein. Lisäksi joissakin maissa on otettu käyttöön yksilölliset numerot helpottamaan kansalaisten yksilöimistä. Siirretyt verotiedot[159], hallinnolliseen asiakirjaan sisältyvät oleskeluluvan hakijaa koskevat

155 Tietosuojatyöryhmä (2007), *lausunto 4/2007 henkilötietojen käsitteestä*, WP 136, 20.6.2007, s. 14.

156 EUT, C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 29.1.2008, 45 kohta.

157 Entinen direktiivi 95/46, 2 artiklan b alakohta, nyt yleinen tietosuoja-asetus, 4 artiklan 2 kohta.

158 EUT, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24.11.2011, 51 kohta.

159 EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 1.10.2015.

tiedot[160] ja pankki- ja varainhoitosuhteita koskevat asiakirjat[161] voivat olla henkilötietoja. Biometrisiä tietoja, kuten sormenjälkiä, digitaalisia valokuvia tai iiriksen kuvaa, paikkatietoja ja verkkotunnisteita, käytetään tekniikan aikakaudella yhä useammin henkilöiden tunnistamiseen.

Euroopan tietosuojasäännösten soveltaminen ei kuitenkaan edellytä rekisteröidyn tarkkaa tunnistamista vaan riittää, että asianomainen henkilö on tunnistettavissa. Henkilöä pidetään tunnistettavissa olevana, jos tieto sisältää riittävästi tunnisteita, joiden avulla henkilö voidaan tunnistaa suoraan tai välillisesti[162]. Yleisen tietosuoja-asetuksen johdanto-osan 26 kappaleen mukaan vertailukohtana on sen todennäköisyys, onko tietojen ennakoitavissa olevien käyttäjien saatavilla ja käytössä kohtuullisia tunnistamiskeinoja. Tähän kuuluvat myös ulkopuolisten vastaanottajien hallussa olevat tiedot (ks. 2.3.2 kohta).

Esimerkki: Paikallisviranomainen päättää kerätä tietoa alueen teillä ylinopeutta ajavista autoista. Se valokuvaa autot tallentaen automaattisesti aika- ja paikkatiedot, jotta toimivaltainen viranomainen voisi sakottaa niitä henkilöitä, jotka rikkovat nopeusrajoituksia. Rekisteröity tekee valituksen ja väittää, ettei paikallisviranomaisella ole lain mukaista oikeudellista perustetta tällaiselle tiedonkeruulle. Paikallisviranomainen katsoo, että se ei kerää henkilötietoja. Sen mielestä rekisterikilvet ovat anonyymien henkilöiden tietoja. Paikallisviranomaisella ei ole laillista toimivaltaa käyttää yleistä ajoneuvorekisteriä auton omistajan tai kuljettajan henkilöllisyyden selvittämiseksi.

Tämä perustelu ei ole yhdenmukainen tietosuojadirektiivin johdanto-osan 26 kappaleen kanssa. Kun otetaan huomioon, että tiedonkeruun tarkoituksena selkeästi on ylinopeutta ajavien henkilöiden tunnistaminen ja sakottaminen, on ennakoitavissa, että henkilöitä pyritään tunnistamaan. Vaikka paikallisviranomaisella ei ole suoraan käytettävissään tunnistuskeinoja, se välittää tiedot toimivaltaiselle viranomaiselle, poliisille, jolla on tällaiset keinot. Johdanto-osan 26 kappaleessa on myös erikseen mainittu tilanne, jossa tulevat tiedon vastaanottajat, muut kuin välitön tiedon käyttäjä, voivat

160 EUT, *YS v. Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel v. M ja S*, 17.7.2014.

161 EIT, *M.N. ym. v. San Marino*, nro 28005/12, 7.7.2015.

162 Yleinen tietosuoja-asetus, 4 artiklan 1 kohta.

yrittää tunnistaa henkilön. Johdanto-osan 26 kappaleen valossa paikallisviranomaisen toiminta vastaa tiedon keräämistä tunnistettavissa olevista henkilöistä ja siksi sillä tulisi olla lain mukainen oikeudellinen peruste.

”Jotta voidaan varmistaa, voidaanko keinoja kohtuullisen todennäköisesti käyttää luonnollisen henkilön tunnistamiseen, olisi otettava huomioon kaikki objektiiviset tekijät, kuten tunnistamisesta aiheutuvat kulut ja tunnistamiseen tarvittava aika sekä käsittelyajankohtana käytettävissä oleva teknologia ja tekninen kehitys.”[163]

Esimerkki: Asiassa *Breyer v. Saksan liittotasavalta*[164] Euroopan unionin tuomioistuin pohti välillistä tunnistettavuutta. Asiassa oli kyse dynaamisista IP-osoitteista, jotka vaihtuvat jokaisen uuden internetyhteyden ottamisen myötä. Saksan liittovaltion laitosten verkkosivustoilla rekisteröitiin ja tallennettiin dynaamisia IP-osoitteita verkkohyökkäyksiltä suojautumista ja tarvittaessa hyökkääjien rikosoikeudelliseen vastuuseen saattamista varten. Vain Breyerin käyttämällä internetyhteyden tarjoajalla oli lisätietoja, jotka mahdollistivat hänen tunnistamisensa.

Euroopan unionin tuomioistuin katsoi, että dynaaminen IP-osoite, jonka verkkomediapalvelujen tarjoaja tallentaa henkilön käydessä tämän palveluntarjoajan yleisön saataville asettamalla internetsivustolla, on henkilötieto siitä huolimatta, että vain kolmannella osapuolella eli tässä tapauksessa internetyhteyden tarjoajalla on lisätietoja, joiden perusteella henkilö voidaan tunnistaa[165]. Se totesi, että jotta tietoa voitaisiin pitää henkilötietona, se ”ei edellytetä, että kaikki tiedot, joiden perusteella rekisteröity voidaan tunnistaa, ovat yhden ainoan tahon hallussa”. Internetyhteyden tarjoajien rekisteröimät dynaamiset IP-osoitteet voidaan tunnistaa tietyissä tilanteissa, esimerkiksi kyberhyökkäystilannetta koskevan rikosoikeudellisen menettelyn yhteydessä, muiden henkilöiden avulla[166]. Kun ”palveluntarjoajalla on käytettävissään oikeudelliset keinot, joiden perusteella se voi tunnistaa kyseisen henkilön sellaisten lisätietojen avulla, jotka ovat tämän henkilön

163 *Ibid.*, johdanto-osan 26 kappale.

164 EUT, C-582/14, *Patrick Breyer v. Saksan liittotasavalta*, 19.10.2016, 47-48 kohta.

165 Entinen Euroopan parlamentin ja neuvoston direktiivi 95/46/EY, annettu 24 päivänä lokakuuta 1995, yksilöiden suojelusta henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, 2 artiklan a alakohta.

166 EUT, C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24.11.2011, 47–48 kohta.

internetyhteyden tarjoajan käytettävissä", se on Euroopan unionin tuomioistuimen mukaan "rekisteröidyn tunnistamiseksi kohtuullisesti toteutettavissa oleva keino". Siksi tällaiset tiedot katsotaan henkilötiedoiksi.

Euroopan neuvoston oikeudessa tunnistettavuus ymmärretään samankaltaisesti. Uudistetun yleissopimuksen 108 selitysmuistiossa on samankaltainen kuvaus. Sen mukaan tunnistettavissa olevan käsitteellä ei viitata pelkästään yksilön henkilöllisyyteen tai oikeudelliseen identiteettiin sellaisenaan vaan myös siihen, minkä perusteella henkilö voidaan "yksilöllistää" tai erottaa muista ja sen tuloksena mahdollisesti kohdella tätä eri tavalla. Tämä "yksilöllistäminen" voitaisiin tehdä esimerkiksi viittaamalla nimenomaisesti häneen tai laitteeseen tai laitteiden (tietokone, matkapuhelin, kamera, pelilaite jne.) yhdistelmään, joka liittyy henkilönumeroon, pseudonyymiin, biometrisiin tai geneettisiin tietoihin, paikkatietoihin, IP-osoitteeseen tai muuhun tunnisteeseen.[167] Henkilöä ei pidetä tunnistettavissa olevana, jos tunnistaminen vaatii kohtuuttoman paljon aikaa, kustannuksia tai työtä. Tästä on kyse esimerkiksi silloin, kun rekisteröidyn tunnistaminen edellyttäisi liian monimutkaisia, pitkiä ja kalliita toimia. Ajan, kustannusten tai työn kohtuuttomuutta on arvioitava tapauskohtaisesti ja otettava huomioon eri tekijöitä, kuten käsittelyn tarkoitus, tunnistamisen kustannukset ja siitä saatavat hyödyt, rekisterinpitäjän laji ja käytetty teknologia.[168]

Muoto, jossa henkilötietoja säilytetään ja käytetään, ei vaikuta tietosuojaa koskevien säännösten sovellettavuuteen. Henkilötietoja voi sisältyä yhtä lailla kirjalliseen kuin puheviestintään samoin kuin kuvamateriaaliin[169], kuten kameravalvontatallenteisiin[170], tai äänimateriaaliin[171]. Sähköisesti tallennettu tieto voi olla henkilötietoa siinä missä paperillakin oleva tieto. Jopa ihmiskudoksen solunäytteet voivat olla biometristen tietojen lähteitä, sillä niihin on tallentunut henkilön dna[172], kunhan tiedot koskevat luonnollisen henkilön perittyjä tai hankittuja geneettisiä ominaisuuksia, joista

167 Uudistettu yleissopimus 108, selitysmuistio, 18 kohta.

168 *Ibid.*, 17 kohta.

169 EIT, *Von Hannover v. Saksa*, nro 59320/00, 24.6.2004; EIT, *Sciacca v. Italia*, nro 50774/99, 11.1.2005; EUT, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014.

170 EIT, *Peck v. Yhdistynyt kuningaskunta*, nro 44647/98, 28.1.2003; EIT, *Köpke v. Saksa* (päätös), nro 420/07, 5.10.2010; EDPS (2010), *The EDPS video-surveillance guidelines*, 17.3.2010.

171 EIT, *P.G. ja J.H. v. Yhdistynyt kuningaskunta*, nro 44787/98, 25.9.2001, 59–60 kohta; EIT, *Wisse v. Ranska*, nro 71611/01, 20.12.005 (ranskankielinen versio).

172 Ks. tietosuojatyöryhmä (2007), *lausunto 4/2007 henkilötietojen käsitteestä*, WP136, 20.6.2007, s. 9; Euroopan neuvosto, ministerikomitean suositus Rec(2006)4 jäsenvaltioille ihmisperäisten biologisten materiaalien tutkimisesta, 15.3.2006.

selviää yksilöllistä tietoa kyseisen luonnollisen henkilön fysiologiasta tai terveydentilasta ja jotka on saatu erityisesti kyseisen luonnollisen henkilön biologisesta näytteestä analysoimalla[173].

Anonymisointi

Yleisen tietosuoja-asetuksen ja uudistetun yleissopimuksen 108 mukainen tietojen säilytyksen rajoittamisen periaate (jota käsitellään tarkemmin 3 luvussa) edellyttää, että tietoja säilytetään "muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten".[174] Tämä tarkoittaa, että tiedot tulee poistaa, tai jos rekisterinpitäjä haluaisi säilyttää tietoja sen jälkeen, kun niitä ei enää tarvita eivätkä ne enää palvele alkuperäistä tarkoitustaan, tiedot pitäisi anonymisoida.

Tietojen anonymisointi tarkoittaa, että henkilötiedoista on poistettu kaikki tunnistettavuus siten, ettei rekisteröidyn tunnistaminen ole enää mahdollista[175]. Tietosuojatyöryhmä analysoi lausunnossaan 5/2014 eri anonymisointitekniikkojen tehokkuutta ja rajoituksia[176]. Tietosuojatyöryhmä myöntää kyseisten tekniikoiden mahdollisen arvon mutta korostaa, että tietyt tekniikat eivät välttämättä toimi kaikissa tapauksissa. Parhaan mahdollisen ratkaisun löytämiseksi kuhunkin tilanteeseen soveltuva anonymisointiprosessi olisi valittava tapauskohtaisesti. Käytettävästä tekniikasta riippumatta tunnistaminen on estettävä peruuttamattomasti. Se tarkoittaa, että tietojen anonymisoinnissa niihin ei saa jäädä mitään tekijää, jonka perusteella kyseessä oleva henkilö (kyseessä olevat henkilöt) voitaisiin tunnistaa uudelleen kohtuullisesti toteutettavissa olevan keinon avulla.[177] Uudelleentunnistamisen riskiä voidaan arvioida ottamalla huomioon tietojen luonteen vuoksi tarvittavat aika, työ ja kustannukset, tietojen käytön tausta, käytettävissä olevat uudelleentunnistamistekniikat ja niihin liittyvät kustannukset[178].

Kun tiedot on tehty anonyymeiksi, niitä ei enää pidetä henkilötietoina eikä tietosuojasäännöksiä enää sovelleta.

173 Yleinen tietosuoja-asetus, 4 artiklan 13 kohta.

174 *Ibid.*, 5 artiklan 1 kohdan e alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan e alakohta.

175 Yleinen tietosuoja-asetus, johdanto-osan 26 kappale.

176 Tietosuojatyöryhmä (2014), *lausunto 5/2014 anonymisointitekniikoista*, WP216, 10.4.2014.

177 Yleinen tietosuoja-asetus, johdanto-osan 26 kappale.

178 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23.1.2017, 6.2. kohta.

Yleisessä tietosuoja-asetuksessa säädetään, että henkilötietojen käsittelyä valvovalla henkilöllä tai organisaatiolla ei ole velvollisuutta säilyttää, hankkia tai käsitellä lisätietoja rekisteröidyn tunnistamista varten, jos tämä olisi tarpeen vain asetuksen noudattamiseksi. Tähän sääntöön on kuitenkin merkittävä poikkeus: jos rekisteröity käyttääkseen oikeuksiaan, jotka koskevat tietoihin tutustumista, niiden oikaisua tai poistamista, käsittelyn rajoittamista ja tietojen siirtämistä, antaa rekisterinpitäjälle lisätietoja, joiden avulla hänet voidaan tunnistaa, aiemmin anonymisoiduista tiedoista tulee jälleen henkilötietoja.[179]

Pseudonymisointi

Henkilötiedot sisältävät tunnisteita, kuten nimen, syntymäajan, sukupuolen, osoitteen tai muita tekijöitä, joista henkilö voidaan tunnistaa. Henkilötiedot käsitellään pseudonyymeiksi siten, että tunnisteet korvataan ns. salanimellä, pseudonyymillä.

EU:n lainsäädännössä pseudonymisoinnilla tarkoitetaan ”henkilötietojen käsittelemistä siten, että henkilötietoja ei voida enää yhdistää tiettyyn rekisteröityyn käyttämättä lisätietoja, edellyttäen että tällaiset lisätiedot säilytetään erillään ja niihin sovelletaan teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, ettei henkilötietojen yhdistämistä tunnistettuun tai tunnistettavissa olevaan luonnolliseen henkilöön tapahdu”[180]. Anonyymeista tiedoista poiketen pseudonymisoidut tiedot ovat edelleen henkilötietoja, ja niihin sovelletaan tietosuojalainsäädäntöä. Vaikka pseudonymisoinnilla voidaan vähentää rekisteröityjen riskejä, se kuuluu kuitenkin yleisen tietosuoja-asetuksen soveltamisalaan.

Yleisessä tietosuoja-asetuksessa pseudonymisointi tunnustetaan asianmukaiseksi tekniseksi toimenpiteeksi tietosuojan edistämistä varten, ja se mainitaan nimenomaisesti tietojenkäsittelyn suunnittelun ja turvallisuuden osalta[181]. Se on myös asianmukainen suojatoimi, jota voidaan käyttää henkilötietojen käsittelyyn muita tarkoituksia varten kuin niitä tarkoituksia, joita varten henkilötiedot on alun perin kerätty[182].

Pseudonymisointia ei mainita nimenomaisesti **Euroopan neuvoston** uudistetun yleissopimuksen 108 oikeudellisessa määritelmässä. Uudistetun

179 Yleinen tietosuoja-asetus, 11 artikla.

180 *Ibid.*, 4 artiklan 5 kohta.

181 *Ibid.*, 25 artiklan 1 kohta.

182 *Ibid.*, 6 artiklan 4 kohta.

yleissopimuksen 108 selitysmuistiossa kuitenkin todetaan selkeästi, että pseudonyymin tai muun digitaalisen tunnisteen / digitaalisen identiteetin käyttö ei tarkoita tietojen anonymisointia, koska rekisteröity on edelleen tunnistettavissa tai yksilöitävissä[183]. Tiedot voidaan pseudonymisoida esimerkiksi tietojen salauksella. Kun tiedot on pseudonymisoitu, tiedot on yhdistetty henkilöön salanimen ja salauksen avaimen avulla. Ilman avainta pseudonymisoitujen tietojen tunnistaminen on hankalaa. Niille, joilla on oikeus käyttää salauksen avainta, henkilöiden uudelleentunnistaminen on kuitenkin vaivatta mahdollista. Salauksen avaimien luvattoman käytön estämisestä on huolehdittava erityisillä suojatoimilla. Näin ollen pseudonymisoidut tiedot on katsottava uudistetun yleissopimuksen 108 soveltamisalaan kuuluviksi henkilötiedoiksi.[184]

Todentaminen

Todentaminen on menettely, jonka kautta henkilö voi todistaa, että hänellä on tietty henkilöllisyys ja/tai lupa tehdä tiettyjä asioita, kuten päästä suljetulle alueelle tai nostaa rahaa pankkitililtä. Todentaminen voidaan toteuttaa vertaamalla biometrisiä tietoja (kuten passissa olevaa valokuvaa tai sormenjälkeä) esimerkiksi maahanmuuton valvonnassa rajalle saapuvan henkilön tietoihin[185], tai kysymällä tietoja, jotka voi tietää vain henkilö, jolla on tietty henkilöllisyys tai lupa (kuten henkilökohtainen tunnusluku tai salasana), tai vaatimalla henkilöä esittämään tietty merkki, jonka pitäisi olla vain sellaisen henkilön hallussa, jolla on tietty henkilöllisyys tai lupa (kuten erityinen sirukortti tai tallelokeron avain). Paitsi salasanojen ja sirukorttien avulla, yhdistettyinä toisinaan henkilökohtaiseen tunnuslukuun, henkilö voidaan sähköisessä viestinnässä tunnistaa ja todentaa erityisesti sähköisellä allekirjoituksella.

2.1.2 Erityiset tietoryhmät

EU:n oikeudessa ja **Euroopan neuvoston oikeudessa** on erityisiä henkilötietoryhmiä, jotka saattavat luonteensa takia aiheuttaa rekisteröidyille riskin, kun niitä käsitellään, ja jotka tarvitsevat siksi vahvempaa suojaa. Näihin tietoihin sovelletaan kieltoperiaatetta, ja niiden käsittely on lainmukaista vain rajatuin ehdoin.

183 Uudistettu yleissopimus 108, selitysmuistio, 18 kohta.

184 *Ibid.*

185 *Ibid.*, 56–57 kohta.

Uudistetussa yleissopimuksessa 108 (6 artikla) ja yleisessä tietosuoja-asetuksessa (9 artikla) arkaluonteisiksi tiedoiksi katsotaan seuraavat tietoryhmät:

- henkilötiedot, joista ilmenee rotu tai etninen alkuperä
- henkilötiedot, joista ilmenee poliittisia mielipiteitä, uskonnollinen tai muu vakaumus, muun muassa filosofinen vakaumus
- henkilötiedot, joista ilmenee ammattiliiton jäsenyys
- geneettiset tai biometriset tiedot, joita käsitellään henkilön yksiselitteistä tunnistamista varten
- henkilötiedot, jotka koskevat terveyttä tai seksuaalista käyttäytymistä tai suuntautumista.

Esimerkki: Asiassa *Bodil Lindqvist*[186] oli kyse siitä, että internetsivulla mainittiin eri henkilöiden nimiä tai muita tietoja, kuten heidän puhelinnumeronsa tai heidän harrastuksiaan koskevia tietoja. Euroopan unionin tuomioistuin totesi, että ”mainintaa siitä, että henkilö on loukannut jalkansa ja on osa-aikaisella sairaslomalla, on pidettävä [...] terveyteen liittyvänä henkilötietona”[187].

Rikostuomioihin ja rikkomuksiin liittyvät henkilötiedot

Uudistetun yleissopimuksen 108 mukaan rikkomuksiin, rikosoikeudenkäynteihin ja rikostuomioihin ja niihin liittyviin turvatoimenpiteisiin liittyvät henkilötiedot sisältyvät erityisten tietoryhmien luetteloon[188]. Yleisessä tietosuoja-asetuksessa rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja ei mainita sellaisenaan erityisten henkilötietoryhmien luettelossa, vaan niitä käsitellään erillisessä artiklassa. Yleisen tietosuoja-asetuksen 10 artiklan mukaan tällainen käsittely voidaan suorittaa vain ”viranomaisen valvonnassa tai silloin, kun se sallitaan unionin oikeudessa tai jäsenvaltion lainsäädännössä, jossa säädetään asianmukaisista suojatoimista rekisteröidyn oikeuksien ja vapauksien suojelemiseksi”. Kattavaa rikosrekisteriä voidaan

186 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003, 51 kohta.

187 Entinen direktiivi 95/46, 8 artiklan 1 kohta, nyt yleinen tietosuoja-asetus, 9 artiklan 1 kohta.

188 Uudistettu yleissopimus 108, 6 artiklan 1 kohta.

puolestaan pitää vain julkisen viranomaisen valvonnassa.[189] EU:ssa henkilötietojen käsittelyä lainvalvonnan yhteydessä säännellään erityisellä säädöksellä, direktiivillä (EU) 2016/680[190]. Direktiivissä säädetään erityisistä tietosuojasäännöistä, jotka sitovat toimivaltaisia viranomaisia, kun ne käsittelevät henkilötietoja nimenomaisesti rikosten ennalta estämistä, tutkimista, paljastamista ja rikoksiin liittyviä syytetoimia varten (ks. 8.2.1 kohta).

2.2 Tietojenkäsittely

Keskeiset kohdat

- ”Tietojenkäsittely” koskee mitä tahansa henkilötiedoilla tehtyä toimea.
- ”Käsittely” kattaa sekä automaattisen että muun kuin automaattisen käsittelyn.
- EU:n oikeudessa ”käsittelyllä” viitataan lisäksi jäsennetyissä rekistereissä olevien tietojen manuaaliseen käsittelyyn.
- Euroopan neuvoston oikeudessa ”käsittelyn” merkitystä voidaan laajentaa kansallisessa lainsäädännössä niin, että se kattaa manuaalisen käsittelyn.

2.2.1 Tietojenkäsittelyn käsite

Tietojenkäsittelyn käsite on **sekä EU:n että Euroopan neuvoston oikeudessa** kattava: ”käsittelyllä” [tarkoitetaan] [...] toimintoja, [joita kohdistetaan henkilötietoihin,] kuten tietojen keräämistä, tallentamista, järjestämistä, jäsentämistä, säilyttämistä, muokkaamista tai muuttamista, hakua, kyselyä, käyttöä, tietojen luovuttamista siirtämällä, levittämällä tai asettamalla ne muutoin saataville, tietojen yhteensovittamista tai yhdistämistä, rajoittamista, poistamista tai tuhoamista”[191]. Uudistetussa yleissopimuksessa 108 määritelmään lisätään henkilötietojen suojelu (preservation)[192].

189 Yleinen tietosuoja-asetus, 10 artikla.

190 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta (EUVL 2016, L 119).

191 Yleinen tietosuoja-asetus, 4 artiklan 2 kohta. Ks. myös uudistettu yleissopimus 108, 2 artiklan b alakohta.

192 Uudistettu yleissopimus 108, 2 artiklan b alakohta.

Esimerkki: Asiassa *František Ryneš*[193] kantaja Ryneš sai kiinteistölleen asentamansa videovalvontajärjestelmän avulla kuvan kahdesta henkilöstä, jotka rikkoivat hänen kotinsa ikkunoita. Euroopan unionin tuomioistuin totesi, että valvonta, johon kuuluu henkilötietojen tallentamista ja säilyttämistä, on EU:n tietosuojalainsäädännön soveltamisalaan kuuluvaa automatisoitua henkilötietojen käsittelyä.

Esimerkki: Asiassa *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*[194] kantaja Manni pyysi poistamaan henkilötietonsa luokitusyhtiön rekisteristä, jossa hänet oli liitetty kiinteistöyhtiön realisointiin, mikä vaikutti kielteisesti hänen maineeseensa. Euroopan unionin tuomioistuin totesi, että ”merkitessään mainitut tiedot rekisteriin ja säilyttäessään niitä rekisterissä sekä luovuttaessaan niitä mahdollisesti ulkopuolisten henkilöiden pyynnöstä, yhtiörekisteriä pitävä viranomainen suorittaa ’rekisterinpitäjän’ asemassa ’henkilötietojen käsittelyä’”.

Esimerkki: Työnantajat keräävät ja käsittelevät työntekijöitään koskevia tietoja, myös palkkaa koskevia tietoja. Tällaisen toiminnan oikeudellisena perusteena on työsopimus.

Työnantajien on toimitettava työntekijöidensä palkkatiedot veroviranomaisille. Tällainen tietojen luovuttaminen on uudistetussa yleissopimuksessa 108 ja yleisessä tietosuoja-asetuksessa tarkoitettua tietojenkäsittelyä. Tietojen luovuttamisen oikeudellinen peruste ei kuitenkaan ole työsopimus. Tarvitaan toinen oikeudellinen peruste niille käsittelytoimille, jotka johtavat palkkatietojen siirtoon työnantajalta veroviranomaisille. Tämä oikeudellinen peruste sisältyy yleensä kansalliseen verolainsäädäntöön. Ilman näitä säännöksiä – ja jos käsittelylle ei ole muuta oikeutettua perustetta – tietojen luovuttaminen olisi laitonta käsittelyä.

2.2.2 Automaattinen tietojenkäsittely

Uudistetun yleissopimuksen 108 ja yleisen tietosuoja-asetuksen mukainen tietosuoja koskee täysimääräisesti automaattista tietojenkäsittelyä.

193 EUT, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, 25 kohta.

194 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9.3.2017, 35 kohta.

EU:n oikeuden mukaan automaattinen tietojenkäsittely koskee henkilötietojen käsittelyä, ”joka on osittain tai kokonaan automaattista”[195]. Uudistetussa yleissopimuksessa 108 on samankaltainen määritelmä[196]. Käytännössä tämä tarkoittaa, että kaikki henkilötietojen käsittely, joka tehdään automaattisesti esimerkiksi tietokoneen, mobiililaitteen tai reitittimen avulla, kuuluu sekä EU:n että Euroopan neuvoston tietosuojasääntöjen soveltamisalaan.

Esimerkki: Asiassa *Bodil Lindqvist*[197] oli kyse siitä, että internetsivulla mainittiin eri henkilöiden nimiä tai muita tietoja, kuten heidän puhelinnumeronsa tai heidän harrastuksiaan koskevia tietoja. Euroopan unionin tuomioistuin totesi seuraavaa: ”sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin, kuten ilmoittamalla heidän puhelinnumeronsa tai antamalla tietoja heidän työsuhteestaan ja harrastuksistaan, on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä”[198].

Esimerkki: Asiassa *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González*[199] kantaja González pyysi poistamaan Googlen hakukoneesta hänen nimellään tulevat linkit kahdelle sanomalehden sivulle, joilla oli ilmoitus sosiaaliturvasaatavien perimiseksi suoritettuun takavarikkoon liittyvästä kiinteän omaisuuden huutokaupasta, tai muuttamaan linkkejä. Euroopan unionin tuomioistuin totesi, että ”kun hakukoneen ylläpitäjä selaa automaattisesti, jatkuvasti ja järjestelmällisesti internetiä internetissä julkaistuja tietoja hakeakseen, se ’kerää’ tällaisia tietoja, jotka se tämän jälkeen ’hakee’, ’tallentaa’ ja ’järjestää’ indeksointiohjelmiensa yhteydessä, ’säilyttää’ palvelimillaan ja tarvittaessa ’luovuttaa’ käyttäjilleen ja ’asettaa [niiden] saataville’ niiden hakujen tulosten luetteloiden muodossa”[200]. Tuomioistuin totesi, että tällaiset toimet ovat

195 Yleinen tietosuoja-asetus, 2 artiklan 1 kohta ja 4 artiklan 2 kohta.

196 Uudistettu yleissopimus 108, 2 artiklan b ja c alakohta, uudistettu yleissopimus 108, selitysmuistio, 21 kohta.

197 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003, 27 kohta.

198 Yleinen tietosuoja-asetus, 2 artiklan 1 kohta.

199 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014.

200 *Ibid.*, 28 kohta.

”käsittelyä” ”ilman, että merkitystä olisi sillä, että hakukoneen ylläpitäjä soveltaa samoja toimia myös muun tyyppisiin tietoihin eikä tee eroa tällaisten tietojen ja henkilötietojen välillä”.

2.2.3 Muu kuin automaattinen tietojenkäsittely

Myös manuaalinen tietojenkäsittely tarvitsee tietosuojaa.

EU:n oikeudessa tietosuojaa ei ole mitenkään rajoitettu automaattiseen tietojenkäsittelyyn. Näin ollen EU:n oikeudessa tietosuojaa sovelletaan manuaalisessa rekisterissä, eli jäsennetyssä paperiarkistossa, olevien henkilötietojen käsittelyyn[201]. Jäsennetyssä paperiarkistossa luokitellaan eri henkilötietoja, jolloin ne ovat saatavilla tiettyjen kriteerien mukaan. Jos esimerkiksi työnantaja pitää paperiarkistoa, jonka nimi on ”työntekijöiden vapaat” ja joka sisältää aakkosjärjestyksessä kaikki tiedot työntekijöiden kahden edellisen vuoden vapaista, arkisto on manuaalinen rekisteri, joka kuuluu EU:n tietosuojasääntöjen soveltamisalaan. Tietosuoja on haluttu ulottaa näihin seuraavista syistä:

- paperiarkistot voidaan jäsentää niin, että tiedot löytyvät niistä helposti ja nopeasti; ja

- automaattista tietojenkäsittelyä varten lainsäädännössä asetettuja rajoituksia on helppo kiertää säilyttämällä henkilötiedot jäsennetyissä paperiarkistoissa[202].

Euroopan neuvoston oikeudessa automaattisen tietojenkäsittelyn määritelmässä tunnustetaan, että joitakin manuaalisen tietojenkäsittelyn vaiheita voidaan tarvita automaattisten toimien välillä[203]. Uudistetun yleissopimuksen 108 2 artiklan c alakohdassa todetaan, että kun automaattista käsittelyä ei käytetä, tietojenkäsittely tarkoittaa operaatiota tai operaatioita, joissa käsitellään henkilötietoja kyseisten tietojen jäsennellyssä kokonaisuudessa, johon voi tutustua tai jonka voi hakea tiettyjen kriteerien mukaan.

201 Yleinen tietosuoja-asetus, 2 artiklan 1 kohta.

202 Yleinen tietosuoja-asetus, johdanto-osan 15 kappale.

203 Uudistettu yleissopimus 108, 2 artiklan b ja c alakohta.

2.3 Henkilötietojen käyttäjät

Keskeiset kohdat

- ”Rekisterinpitäjä” on taho, joka määrittelee muiden ihmisten henkilötietojen käsittelyn keinot ja tarkoitukset. Jos monta tahoa tekee yhdessä kyseisen päätöksen, voidaan heitä nimittää ”yhteisrekisterinpitäjäksi”.
- ”Henkilötietojen käsittelijä” on luonnollinen henkilö tai oikeushenkilö, joka käsittelee henkilötietoja rekisterinpitäjän lukuun.
- Henkilötietojen käsittelijästä tulee rekisterinpitäjä, jos hän määrittää itse tietojenkäsittelyn keinot ja tarkoitukset.
- Jokainen, jolle henkilötietoja luovutetaan, on ”vastaanottaja”.
- ”Kolmas osapuoli” on muu luonnollinen henkilö tai oikeushenkilö kuin rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä ja henkilö, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena.
- Suostumuksen, joka on henkilötietojen käsittelyn oikeusperusta, on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilötietojen käsittely hyväksytään toteuttamalla selkeästi suostumusta ilmaiseva toimi.
- Suostumukseen perustuva erityisten henkilötietoryhmien käsittely edellyttää nimenomaista suostumusta.

2.3.1 Rekisterinpitäjät ja henkilötietojen käsittelijät

Rekisterinpitäjänä tai henkilötietojen käsittelijänä olemisen tärkein seuraus on oikeudellinen vastuu tietosuojasäännöksissä asetettujen velvollisuuksien noudattamisesta. Yksityissektorilla kyseisiä tehtäviä hoitaa yleensä luonnollinen henkilö tai oikeushenkilö; julkisella sektorilla se on yleensä viranomainen. Rekisterinpitäjän ja henkilötietojen käsittelijän välillä on huomattava ero: rekisterinpitäjä on luonnollinen henkilö tai oikeushenkilö, joka määrittelee henkilötietojen tarkoitukset ja keinot, ja henkilötietojen käsittelijä on luonnollinen henkilö tai oikeushenkilö, joka käsittelee tietoja rekisterinpitäjän lukuun tiukkojen ohjeiden mukaisesti. Periaatteessa juuri rekisterinpitäjän on valvottava käsittelyä, ja rekisterinpitäjällä on tästä vastuu, myös oikeudellinen vastuu. Tietosuojasääntöjen uudistuksen myötä henkilötietojen käsittelijöiden on nyt kuitenkin noudatettava monia rekisterinpitäjiin sovellettavia vaatimuksia. Yleisen tietosuoja-asetuksen mukaan henkilötietojen käsittelijöiden on esimerkiksi ylläpidettävä selostetta kaikista käsittelytoimista

osoittaakseen noudattavansa asetuksessa asetettuja velvollisuuksia[204]. Henkilötietojen käsittelijöiden on myös toteutettava käsittelyn turvallisuuden varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet[205], nimitettävä tietosuojavastaava tietyissä tilanteissa[206] ja ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle[207].

Se, pystyykö henkilö päättämään käsittelyn tarkoituksesta ja keinoista ja määrittelemään ne, riippuu asian tosiseikoista tai olosuhteista. Yleisen tietosuoja-asetuksen rekisterinpitäjän määritelmän mukaan rekisterinpitäjä voi olla luonnollinen henkilö, oikeushenkilö tai mikä tahansa muu elin. Tietosuojatyöryhmä on kuitenkin korostanut, että jotta rekisteröidyille esitettäisiin vakaampi viiteyhteisö oikeuksien käyttämiseksi, ”rekisterinpitäjäksi olisi mieluimmin katsottava yritys tai yhteisö sellaisenaan eikä ketään tiettyä henkilöä tässä yrityksessä tai yhteisössä”[208]. Esimerkiksi yritys, joka myy terveydenhuollon välineitä alan toimijoille, on rekisterinpitäjä, joka laatii ja pitää yllä jakeluluetteloa kaikista tietyn alueen toimijoista, eikä myyntipäällikkö, joka tosiasiallisesti käyttää ja ylläpitää luetteloa.

Esimerkki: Kun Sunshine-yhtiön markkinointiosasto suunnittelee tietojen käsittelemistä markkinatutkimusta varten, rekisterinpitäjäksi katsotaan Sunshine-yhtiö, ei sen markkinointiosaston työntekijöitä. Markkinointiosasto ei voi olla rekisterinpitäjä, koska sillä ei ole erillistä oikeushenkilöyttä.

Luonnolliset henkilöt voivat olla rekisterinpitäjiä sekä EU:n että Euroopan neuvoston oikeuden mukaan. Kun kuitenkin muiden henkilöiden henkilötietojen käsittely on yksinomaan henkilökohtaista tai kotitaloutta koskevaa toimintaa, yksityishenkilöt eivät kuulu yleisen tietosuoja-asetuksen ja uudistetun yleissopimuksen 108 soveltamisalaan eikä heitä katsota rekisterinpitäjiksi[209]. Henkilö, joka käy kirjeenvaihtoa, pitää henkilökohtaista päiväkirjaa, jossa kuvataan tapahtumia ystävien ja työtovereiden kanssa, ja kirjaa perheen terveystietoja, voidaan vapauttaa tietosuojasäännöistä, koska nämä toimet voivat olla yksinomaan henkilökohtaista tai kotitaloutta

204 Yleinen tietosuoja-asetus, 30 artiklan 2 kohta.

205 *Ibid.*, 32 artikla.

206 *Ibid.*, 37 artikla.

207 *Ibid.*, 33 artiklan 2 kohta.

208 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010.

209 Yleinen tietosuoja-asetus, johdanto-osan 18 kappale ja 2 artiklan 2 kohdan c alakohta; uudistettu yleissopimus 108, 3 artiklan 2 kohta.

koskevaa toimintaa. Yleisessä tietosuoja-asetuksessa täsmennetään lisäksi, että henkilökohtaista tai kotitaloutta koskevaa toimintaa voi olla myös sosiaalinen verkostoituminen ja verkkotoiminta, joita harjoitetaan tällaisen toiminnan yhteydessä[210]. Sitä vastoin tietosuojasääntöjä sovelletaan täysimääräisesti rekisterinpitäjiin ja henkilötietojen käsittelijöihin, jotka tarjoavat keinot tällaiseen henkilökohtaiseen tai kotitaloutta koskevaan henkilötietojen käsittelyyn (esimerkiksi sosiaalisen verkostoitumisen alustat).[211]

Henkilökohtaista toimintaa koskevaa käsittelyä on koko ajan vaikeampi erottaa muusta kuin henkilökohtaisesta käsittelystä, koska kansalaiset pääsevät internetiin ja voivat käyttää verkkokauppa-alustoja, sosiaalisen median verkostoja ja bloggaussivustoja jakamaan tietoja itsestään ja muista henkilöstä[212]. Olosuhteet määrittävät, onko kyse yksinomaan henkilökohtaisesta tai kotitaloutta koskevasta toiminnasta[213]. Ammatillisia tai kaupallisia näkökohtia sisältävään toimintaan ei voida soveltaa kotitalouksia koskevaa poikkeusta[214]. Kun tietojenkäsittelyn laajuuden ja tiheyden perusteella voidaan päätellä, että kyse on ammatillisesta tai kokopäiväisestä toiminnasta, yksityishenkilö voidaan katsoa rekisterinpitäjäksi. Käsittelyn ammatillisuuden tai kaupallisuuden lisäksi toinen huomioon otettava tekijä on se, annetaanko henkilötiedot sellaisen suuren ihmismäärän saataville, joka ei selkeästi kuulu henkilön yksityiselämän piiriin. Tietosuojadirektiivin mukaisessa oikeuskäytännössä on todettu, että tietosuojalakeja sovelletaan, kun yksityishenkilö julkaisee internetin käytön yhteydessä tietoja muista julkisella verkkosivustolla. Euroopan unionin tuomioistuin ei ole vielä antanut yleisen tietosuoja-asetuksen nojalla tuomioita samankaltaisista tosiseikoista. Asetuksessa annetaan direktiiviä enemmän ohjeita aiheista, joiden voitaisiin katsoa olevan tietosuojalainsäädännön soveltamisalan ulkopuolella ”kotitalouspoikkeuksen” nojalla. Niihin kuuluu esimerkiksi sosiaalisen median henkilökohtainen käyttö.

210 Yleinen tietosuoja-asetus, johdanto-osan 18 kappale.

211 *Ibid.*, johdanto-osan 18 kappale; uudistettu yleissopimus 108, selitysmuistio, 29 kohta.

212 Ks. tietosuojatyöryhmän lausunto tietosuojan uudistuspakettia koskevista keskusteluista (2013), *Liite 2: Ehdotukset ja muutokset henkilökohtaista tai kotitaloutta koskevaan toimintaan liittyvästä poikkeuksesta*, 27.2.2013.

213 Uudistettu yleissopimus 108, selitysmuistio, 28 kohta.

214 Ks. yleinen tietosuoja-asetus, johdanto-osan 18 kappale, ja uudistettu yleissopimus 108, selitysmuistio, 27 kohta.

Esimerkki: Asiassa *Bodil Lindqvist*[215] oli kyse siitä, että internetsivulla mainittiin eri henkilöiden nimiä tai muita tietoja, kuten heidän puhelinnumeronsa tai heidän harrastuksiaan koskevia tietoja. Euroopan unionin tuomioistuin totesi seuraavaa: ”sitä, että Internet-kotisivulla viitataan henkilöihin ja yksilöidään heidät joko nimeltä tai muulla tavoin […] on pidettävä direktiivin 95/46/EY 3 artiklan 1 kohdassa tarkoitettuna kokonaan tai osittain automatisoituna henkilötietojen käsittelynä”[216].

Tällainen henkilötietojen käsittely ei kuulu yksinomaan henkilökohtaiseen tai kotitaloutta koskevaan toimintaan, joka on EU:n tietosuojasääntöjen soveltamisalan ulkopuolella, koska ”tätä poikkeusta on […] tulkittava niin, että se kohdistuu ainoastaan toimintaan, joka kuuluu yksityisen henkilön yksityis- tai perhe-elämään, mistä ei ilmeisestikään ole kysymys sellaisessa henkilötietojen käsittelyssä, jossa tiedot julkaistaan Internet-sivulla siten, että ne saatetaan ennalta määrittelemättömän henkilöryhmän saataville”[217].

Euroopan unionin tuomioistuimen mukaan yksityisesti asennetun turvakameran kuvatallenteen voivat myös tietyissä olosuhteissa kuulua EU:n tietosuojalainsäädännön soveltamisalaan.

Esimerkki: Asiassa *František Ryneš*[218] kantaja Ryneš sai kiinteistölleen asentamansa videovalvontajärjestelmän avulla kuvan kahdesta henkilöstä, jotka rikkoivat hänen kotinsa ikkunoita. Kuva luovutettiin sitten poliisille, ja sitä käytettiin rikosoikeudenkäynnissä.

Euroopan unionin tuomioistuin totesi, että ”[s]iltä osin kuin […] videovalvonta ulottuu vaikka osittainkin julkiseen tilaan ja kohdistuu tämän vuoksi tietoja tällä tavoin käsittelevän tahon yksityisen piirin ulkopuolelle, sitä ei voida pitää yksinomaan ’henkilökohtaisena tai kotitaloutta koskevana’ toimintana”[219].

215 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003.

216 *Ibid.*, 27 kohta; entinen direktiivi 95/46/EY, 3 artiklan 1 kohta, nyt yleinen tietosuoja-asetus, 2 artiklan 1 kohta.

217 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003, 47 kohta.

218 EUT, C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014, 33 kohta.

219 Entinen direktiivi 95/46/EY, 3 artiklan 2 kohdan toinen luetelmakohta, nyt yleinen tietosuoja-asetus, 2 artiklan 2 kohdan c alakohta.

Rekisterinpitäjä

EU:n oikeudessa rekisterinpitäjällä tarkoitetaan jotakuta, joka ”yksin tai yhdessä toisten kanssa määrittelee henkilötietojen käsittelyn tarkoitukset ja keinot”[220]. Rekisterinpitäjä päättää, miksi ja miten tietoja käsitellään.

Euroopan neuvoston oikeudessa, uudistetussa yleissopimuksessa 108 rekisterinpitäjällä tarkoitetaan luonnollista henkilöä tai oikeushenkilöä, julkista viranomaista, yksikköä tai virastoa tai muuta yhteisöä, joka on yksin tai yhdessä muiden kanssa toimivaltainen päättämään tietojenkäsittelystä[221]. Tämä päätöksentekoa koskeva toimivalta koskee käsittelyn tarkoituksia ja keinoja sekä käsiteltäviä tietoryhmiä ja tietojen saatavuutta[222]. Tapauskohtaisesti on päätettävä, perustuuko toimivalta oikeudelliseen nimitykseen vai tosiasiallisiin olosuhteisiin[223].

Esimerkki: Asiassa *Google Spain*[224] kantajana oli Espanjan kansalainen, joka halusi, että Googlesta poistetaan hänen aiempia taloudellisia tietojaan koskeva vanha sanomalehti-ilmoitus.

Euroopan unionin tuomioistuimelta kysyttiin, onko hakukoneen ylläpitäjä Google tietosuojadirektiivin 2 artiklan d alakohdassa tarkoitettu rekisterinpitäjä[225]. Tuomioistuin käytti rekisterinpitäjän laajaa määritelmää, jotta voidaan ”varmistaa rekisteröityjen tehokas ja kattava suojelu”[226]. Tuomioistuin totesi, että hakukoneen ylläpitäjä määrittelee käsittelyn tarkoitukset ja keinot ja antaa verkkosivustojen julkaisijoiden internetsivuille sisällyttämät tiedot jokaisen rekisteröidyn nimellä haun tekevän internetin käyttäjän saataville[227]. Näin ollen tuomioistuin totesi, että Google voidaan katsoa ”rekisterinpitäjäksi”[228].

220 Yleinen tietosuoja-asetus, 4 artiklan 7 kohta.

221 Uudistettu yleissopimus 108, 2 artiklan d alakohta.

222 Uudistettu yleissopimus 108, selitysmuistio, 22 kohta.

223 *Ibid.*

224 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014.

225 Yleinen tietosuoja-asetus, 4 artiklan 7 kohta; EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 21 kohta.

226 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 34 kohta.

227 *Ibid.*, 35–40 kohta.

228 *Ibid.*, 41 kohta.

Kun rekisterinpitäjä tai henkilötietojen käsittelijä on sijoittautunut EU:n ulkopuolelle, kyseisen yrityksen on nimettävä kirjallisesti edustaja unionin aluetta varten[229]. Yleisessä tietosuoja-asetuksessa korostetaan, että edustajan on oltava sijoittautunut ”johonkin jäsenvaltioista, joissa ovat ne rekisteröidyt, joiden henkilötietoja käsitellään heille tarjottavien tavaroiden tai palvelujen yhteydessä tai joiden käyttäytymistä seurataan”[230]. Vaikka edustajaa ei nimitetä, itse rekisterinpitäjää tai henkilötietojen käsittelijää vastaan voidaan kuitenkin käynnistää oikeustoimia[231].

Yhteisrekisterinpitäjät

Yleisessä tietosuoja-asetuksessa säädetään, että jos vähintään kaksi rekisterinpitäjää määrittää yhdessä käsittelyn tarkoitukset ja keinot, ne ovat yhteisrekisterinpitäjiä. Tällöin ne päättävät yhdessä käsitellä tietoja yhteiseen tarkoitukseen.[232] Uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että myös **Euroopan neuvoston oikeudellisessa kehyksessä** sallitaan useita rekisterinpitäjiä tai yhteinen rekisterinpito[233].

Tietosuojatyöryhmä panee merkille, että yhteinen rekisterinpito voi saada eri muotoja ja että eri rekisterinpitäjät eivät välttämättä osallistu rekisterinpitoon samassa määrin[234]. Tällaisen joustavuuden ansiosta pystytään kattamaan tietojen käsittelyn lisääntyvä mutkikkuus[235]. Asetuksen velvollisuuksien noudattamiseksi yhteisrekisterinpitäjien on näin ollen määritettävä omat vastuualueensa nimenomaisessa sopimuksessa[236].

Yhteisrekisterinpitäjillä on yhteisvastuu käsittelytoimista[237]. **EU:n oikeudessa** tämä tarkoittaa, että kutakin rekisterinpitäjää tai henkilötietojen käsittelijää voidaan pitää vastuussa koko vahingosta, joka johtuu käsittelystä, johon osallistuu useampi rekisterinpitäjä. Näin voidaan varmistaa, että rekisteröity saa tosiasiallisen korvauksen[238].

229 Yleinen tietosuoja-asetus, 27 artiklan 1 kohta.

230 *Ibid.*, 27 artiklan 3 kohta.

231 *Ibid.*, 27 artiklan 5 kohta.

232 *Ibid.*, 4 artiklan 7 kohta ja 26 artikla.

233 Uudistettu yleissopimus 108, 2 artiklan d alakohta, uudistettu yleissopimus 108, selitysmuistio, 22 kohta.

234 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010, s. 21.

235 *Ibid.*

236 Yleinen tietosuoja-asetus, johdanto-osan 79 kappale.

237 *Ibid.*, 21 kohta.

238 *Ibid.*, 82 artiklan 4 kohta.

Esimerkki: Usean luottolaitoksen yhteisesti ylläpitämä tietokanta asiakkaista, joilla on maksuhäiriöitä, on tavallinen esimerkki yhteisestä rekisterinpidosta. Kun henkilö hakee luottoa pankista, joka on yksi yhteisistä rekisterinpitäjistä, pankki tarkistaa tietokannasta hakijan luottokelpoisuuden tietoon perustuvan päätöksen tekemiseksi.

Säännöksistä ei käy yksiselitteisesti ilmi, onko yhteistä rekisterinpitoa varten yhteisen tarkoituksen oltava kaikille sama vai riittääkö, että tarkoitukset ovat osittain päällekkäisiä. Euroopan tasolla ei ole vielä asiaa koskevaa oikeuskäytäntöä. Tietosuojatyöryhmä toteaa vuonna 2010 rekisterinpitäjistä ja henkilötietojen käsittelijöistä antamassaan lausunnossa, että yhteisrekisterinpitäjien kaikki käsittelyn tarkoitukset ja keinot voivat olla samat tai niillä voi olla yhteiset tarkoitus ja keinot, tai vain osa niistä voi olla yhteisiä[239]. Kun kaikki tarkoitukset ja keinot ovat samat, eri toimijoiden suhde on erittäin tiivis, ja kun ne ovat vain osittain samoja, suhde on löyhempi.

Tietosuojatyöryhmä kannattaa yhteisen rekisterinpidon laajaa tulkintaa, joka mahdollistaisi tietyn joustavuuden yhä monimuotoisemman tietojen käsittelyn kattamiseksi[240]. Tietosuojatyöryhmän kantaa kuvastaa tapaus, jossa Society for Worldwide Interbank Financial Telecommunication (SWIFT) oli osallisena.

Esimerkki: Niin kutsutussa SWIFT-asiassa eurooppalaiset pankit käyttivät SWIFTiä alun perin tietojen käsittelijänä tietojen siirtämiseen pankkitapahtumien yhteydessä. Tietoja säilytettiin Yhdysvalloissa sijaitsevassa tietojenkäsittelykeskuksessa. SWIFT paljasti nämä pankkitapahtumia koskevat tiedot Yhdysvaltain valtiovarainministeriölle ilman, että sen asiakkaina olleet eurooppalaiset pankit olisivat nimenomaisesti määränneet sen tekemään niin. Tietosuojatyöryhmä arvioi tilanteen lainmukaisuutta ja tuli siihen johtopäätökseen, että SWIFTin kanssa sopimuksen tehneet eurooppalaiset pankit ja SWIFT olivat yhteisiä rekisterinpitäjiä, jotka olivat vastuussa eurooppalaisille asiakkaille näiden tietojen paljastamisesta Yhdysvaltojen viranomaisille[241].

239 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010, s. 21.

240 *Ibid.*

241 Tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22.11.2006.

Henkilötietojen käsittelijä

EU:n oikeudessa henkilötietojen käsittelijä määritellään tahoksi, joka käsittelee henkilötietoja rekisterinpitäjän lukuun[242]. Henkilötietojen käsittelijän toiminta saattaa rajoittua tarkoin määriteltyyn tehtävään tai tilanteeseen tai se voi olla melko yleistä ja kattavaa.

Euroopan neuvoston oikeudessa henkilötietojen käsittelijällä tarkoitetaan samaa asiaa kuin EU:n oikeudessa[243].

Sen lisäksi, että henkilötietojen käsittelijät käsittelevät tietoja muiden lukuun, ne ovat itse rekisterinpitäjiä, kun ne käsittelevät tietoja omiin tarkoituksiinsa, esimerkiksi omien työntekijöidensä, myyntinsä ja tiliensä hallinnoinnissa.

Esimerkki: Everready-yhtiö on erikoistunut tietojenkäsittelyyn muiden yritysten henkilöstöhallinnon hoitamisen yhteydessä. Tässä tehtävässä Everready on henkilötietojen käsittelijä. Kun Everready käsittelee omien työntekijöidensä henkilötietoja, se on kuitenkin rekisterinpitäjä niissä tietojenkäsittelytoimissa, jotka se toteuttaa täyttääkseen velvollisuutensa työnantajana.

Rekisterinpitäjän ja henkilötietojen käsittelijän välinen suhde

Kuten olemme todenneet, rekisterinpitäjä on se, joka määrittelee käsittelyn tarkoitukset ja keinot. Yleisessä tietosuoja-asetuksessa todetaan selkeästi, että henkilötietojen käsittelijä saa käsitellä henkilötietoja vain rekisterinpitäjän ohjeiden mukaisesti, ellei unionin oikeudessa tai jäsenvaltion lainsäädännössä toisin vaadita[244]. Rekisterinpitäjän ja henkilötietojen käsittelijän välisen suhteen olennainen osa on niiden välinen sopimus, joka on lakisääteinen vaatimus[245].

242 Yleinen tietosuoja-asetus, 4 artiklan 8 kohta.

243 Uudistettu yleissopimus 108, 2 artiklan f alakohta.

244 Yleinen tietosuoja-asetus, 29 artikla.

245 *Ibid.*, 28 artiklan 3 kohta.

Esimerkki: Sunshine-yhtiön johtaja päättää, että pilvipohjaiseen tietojen tallentamiseen erikoistuneen Cloudy-yhtiön pitäisi hallinnoida Sunshinen asiakastietoja. Sunshine säilyy rekisterinpitäjänä ja Cloudy on vain henkilötietojen käsittelijä, sillä sopimuksen mukaan Cloudy saa käyttää Sunshinen asiakastietoja yksinomaan Sunshinen määrittelemiin tarkoituksiin.

Vaikka henkilötietojen käsittelijälle annettaisiinkin valtuudet määritellä käsittelyn keinot, rekisterinpitäjän on voitava vaikuttaa henkilötietojen käsittelijän päätöksiin käsittelyn keinoista. Kokonaisvastuu henkilötietojen käsittelyn lainmukaisuudesta säilyy rekisterinpitäjällä, jonka on valvottava henkilötietojen käsittelijöitä ja varmistettava, että niiden päätökset noudattavat tietosuojalainsäädäntöä.

Jos henkilötietojen käsittelijä ei noudattaisi rajoituksia, jotka rekisterinpitäjä on asettanut tietojen käsittelylle, henkilötietojen käsittelijästä tulisi rekisterinpitäjä ainakin siinä määrin, kuin se olisi rikkonut rekisterinpitäjän ohjeita. Henkilötietojen käsittelijää pidettäisiin todennäköisesti laittomasti toimivana rekisterinpitäjänä. Alkuperäisen rekisterinpitäjän pitäisi vuorostaan selittää, miten henkilötietojen käsittelijä onnistui ylittämään valtuutensa[246]. Tietosuojatyöryhmä vaikuttaa tosiaan lähtevän siitä, että tällaisissa tapauksissa on kyse yhteisestä rekisterinpidosta, koska näin turvataan parhaiten rekisteröityjen edut[247].

Vastuun jakautuminen saattaa olla epäselvää myös silloin, kun rekisterinpitäjä on pieni yritys ja henkilötietojen käsittelijä on suuri yhtymä, jolla on valta sanella palvelujensa ehdot. Tietosuojatyöryhmä kuitenkin katsoo, ettei tällaisessa tilanteessa tulisi madaltaa vastuun kynnystä taloudellisen eriarvoisuuden perusteella, vaan rekisterinpitäjän käsite tulisi ymmärtää edelleen samalla tavalla.[248]

Selkeyden ja avoimuuden vuoksi rekisterinpitäjän ja henkilötietojen käsittelijän välisen suhteen yksityiskohdista on sovittava kirjallisesti[249]. Sopimukseen täytyy sisältyä erityisesti käsittelyn aihe, luonne, tarkoitus ja kesto, henkilötietojen laji ja rekisteröityjen ryhmät. Siinä määrätään myös rekisterinpitäjän ja henkilötietojen

246 *Ibid.*, 82 artiklan 2 kohta.

247 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010, s. 25; tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22.11.2006.

248 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010, s. 21.

249 Yleinen tietosuoja-asetus, 28 artiklan 3 ja 9 kohta.

käsittelijän velvollisuuksista ja oikeuksista, kuten luottamuksellisuutta ja turvallisuutta koskevista vaatimuksista. Tällaisen sopimuksen puuttuminen rikkoo rekisterinpitäjän velvollisuutta pystyä osoittamaan asiakirjojen avulla osapuolten vastuut, ja se voi johtaa seuraamuksiin. Kun rekisterinpitäjän lainmukaisten ohjeiden vastaisesti toimimisesta tai niiden noudattamatta jättämisestä aiheutuu vahinko, rekisterinpitäjän lisäksi myös henkilötietojen käsittelijä voi joutua vastuuseen[250]. Henkilötietojen käsittelijän on ylläpidettävä selostetta kaikista rekisterinpitäjän lukuun suoritettavista käsittelytoimista[251]. Seloste on pyydettäessä saatettava valvontaviranomaisen saataville, koska sekä rekisterinpitäjän että henkilötietojen käsittelijän on tehtävä yhteistyötä valvontaviranomaisen kanssa sen tehtävien suorittamiseksi[252]. Rekisterinpitäjät ja henkilötietojen käsittelijät voivat osoittaa yleisen tietosuoja-asetuksen vaatimusten noudattamisen myös noudattamalla hyväksyttyjä käytännesääntöjä tai sertifiointimekanismia[253].

Henkilötietojen käsittelijät saattavat haluta delegoida joitakin tietojenkäsittelytehtäviä edelleen muille käsittelijöille. Se on lainsäädännön näkökulmasta mahdollista edellyttäen, että asiasta sovitaan rekisterinpitäjän ja henkilötietojen käsittelijän välisessä asianmukaisessa sopimuksessa, jossa tulee myös määrätä muun muassa siitä, onko rekisterinpitäjältä pyydettävä joka kerta erikseen lupa vai riittääkö, että sille tiedotetaan asiasta. Yleisen tietosuoja-asetuksen mukaan alkuperäinen henkilötietojen käsittelijä on edelleen täysimääräisesti vastuussa, kun alihankkijana toimiva henkilötietojen käsittelijä ei täytä tietosuojavelvoitteitaan[254].

Euroopan neuvoston oikeudessa rekisterinpitäjän ja henkilötietojen käsittelijän käsitteitä tulkitaan, kuten edellä selitettiin, täydessä laajuudessaan[255].

2.3.2 Vastaanottajat ja kolmannet osapuolet

Merkittävin ero näiden kahden tietosuojadirektiivissä määritellyn henkilö- tai yksikköryhmän välillä liittyy niiden suhteeseen rekisterinpitäjään ja siten niiden mahdollisuuteen saada rekisterinpitäjän hallussa olevia henkilötietoja.

250 *Ibid.*, 82 artiklan 2 kohta.

251 *Ibid.*, 30 artiklan 2 kohta.

252 *Ibid.*, 30 artiklan 4 kohta ja 31 artikla.

253 *Ibid.*, 28 artiklan 5 kohta ja 42 artiklan 4 kohta.

254 *Ibid.*, 28 artiklan 4 kohta.

255 Ks. esim. uudistettu yleissopimus 108, 2 artiklan b alakohta; profilointia koskeva suositus, 1 artikla.

”Kolmas osapuoli” on taho, joka ei ole rekisterinpitäjä eikä henkilötietojen käsittelijä. Yleisen tietosuoja-asetuksen 4 artiklan 10 kohdan mukaan kolmannella osapuolella tarkoitetaan ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta toimielintä kuin rekisteröityä, rekisterinpitäjää, henkilötietojen käsittelijää ja henkilöä, joilla on oikeus käsitellä henkilötietoja suoraan rekisterinpitäjän tai henkilötietojen käsittelijän välittömän vastuun alaisena”. Tämä tarkoittaa, että toisen yhtiön kuin rekisterinpitäjän lukuun toimivat henkilöt ovat yleensä kolmansia osapuolia, vaikka yhtiö kuuluisi samaan yhtymään tai holdingyhtiöön. Toisaalta taas asiakkaiden tilejä käsittelevät pankin sivukonttorit, jotka toimivat pääkonttorin suoraan valtuuttamina, eivät ole kolmansia osapuolia.[256]

”Vastaanottaja” on laajempi käsite kuin ”kolmas osapuoli”. Yleisen tietosuoja-asetuksen 4 artiklan 9 kohdan mukaan vastaanottajalla tarkoitetaan ”luonnollista henkilöä tai oikeushenkilöä, viranomaista, virastoa tai muuta elintä, jolle luovutetaan henkilötietoja, oli kyseessä kolmas osapuoli tai ei”. Vastaanottaja voi olla taho, joka ei kuulu rekisterinpitäjän eikä henkilötietojen käsittelijän organisaatioon – silloin kyseessä on kolmas osapuoli –, tai taho, joka kuuluu rekisterinpitäjän tai henkilötietojen käsittelijän organisaatioon, kuten työntekijä tai toinen saman yrityksen tai viranomaisen alainen osasto.

Vastaanottajien ja kolmansien osapuolien erottaminen toisistaan on tärkeää vain arvioitaessa henkilötietojen luovutuksen laillisuuden edellytyksiä. Rekisterinpitäjän tai henkilötietojen käsittelijän työntekijän ei tarvitse täyttää muita oikeudellisia vaatimuksia voidakseen olla henkilötietojen vastaanottaja, jos hän osallistuu rekisterinpitäjän tai henkilötietojen käsittelijän suorittamiin käsittelytoimiin. Sen sijaan kolmas osapuoli, joka on oikeudellisesti erillinen rekisterinpitäjästä tai henkilötietojen käsittelijästä, ei saa käyttää henkilötietojen käsittelijän käsittelemiä henkilötietoja ilman, että tapausta varten on erityinen oikeudellinen peruste.

Esimerkki: Henkilötietojen käsittelijän työntekijä, joka käyttää henkilötietoja niiden tehtävien suorittamiseen, jotka työnantaja on hänelle osoittanut, on henkilötietojen vastaanottaja muttei kolmas osapuoli, sillä hän käyttää henkilötietoja henkilötietojen käsittelijän nimissä ja alaisuudessa. Jos työnantaja esimerkiksi luovuttaa työntekijöidensä henkilötietoja henkilöstöosastolleen

256 Tietosuojatyöryhmä (2010), *lausunto 1/2010 rekisterinpitäjän ja henkilötietojen käsittelijän käsitteistä*, WP 169, Bryssel, 16.2.2010, s. 30.

tulevia tuloksellisuusarviointeja varten, henkilöstöosasto on henkilötietojen vastaanottaja, koska tiedot on luovutettu sille, kun henkilötietoja on käsitelty rekisterinpitäjää varten.

Jos taas organisaatio antaa työntekijöistään tietoa koulutusyritykselle, joka käyttää niitä työntekijöiden koulutusohjelman laatimiseen, koulutusyritys on kolmas osapuoli. Tämä johtuu siitä, että koulutusyrityksellä ei ole erityistä oikeutusta tai lupaa (joka henkilöstöosaston tapauksessa perustuu työsuhteeseen rekisterinpitäjän kanssa), käsitellä kyseisiä henkilötietoja. Se ei toisin sanoen ole saanut tietoja työsuhteessa rekisterinpitäjän kanssa.

2.4 Suostumus

Keskeiset kohdat

- Suostumuksen, joka on henkilötietojen käsittelyn oikeusperusta, on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla henkilötietojen käsittely hyväksytään toteuttamalla selkeästi suostumusta ilmaiseva toimi.
- Erityisten henkilötietoryhmien käsittely edellyttää nimenomaista suostumusta.

Suostumus on yksi kuudesta laillisen tietojenkäsittelyn oikeudellisesta perusteesta. Tätä käsitellään yksityiskohtaisesti luvussa 4. Suostumuksella tarkoitetaan ”mitä tahansa vapaaehtoista, yksilöityä, tietoista ja yksiselitteistä tahdonilmaisua”[257].

EU:n oikeudessa asetetaan useita edellytyksiä sille, että suostumusta voidaan pitää pätevänä. Niillä pyritään takaamaan, että rekisteröidyt ovat todella tarkoittaneet suostua henkilötietojensa käsittelyyn:[258]

- Suostumus on annettava selkeästi suostumusta ilmaisevalla toimella, josta käy ilmi rekisteröidyn vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen tahdonilmaisu, jolla hän hyväksyy henkilötietojensa käsittelyn. Suostumus voi olla toimi tai lausuma.

- Rekisteröidyllä on oltava oikeus peruuttaa suostumuksensa milloin tahansa.

257 Yleinen tietosuoja-asetus, 4 artiklan 11 kohta. Ks. myös uudistettu yleissopimus 108, 5 artiklan 2 kohta.

258 Yleinen tietosuoja-asetus, 7 artikla.

- Jos rekisteröity antaa suostumuksensa kirjallisessa ilmoituksessa, joka koskee myös muita asioita, esimerkiksi palveluehtoja, suostumuksen antamista koskeva pyyntö on esitettävä selvästi erillään muista asioista helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Jos jokin ilmoituksen osa rikkoo yleistä tietosuoja-asetusta, se ei ole sitova.

Vain jos kaikki nämä vaatimukset täyttyvät, suostumusta voidaan pitää pätevänä tietosuojasäännöksissä tarkoitetulla tavalla. Rekisterinpitäjän vastuulla on osoittaa, että rekisteröity on antanut suostumuksen henkilötietojensa käsittelyyn[259]. Pätevän suostumuksen edellytyksiä käsitellään lisää 4.1.1 kohdassa, joka koskee henkilötietojen käsittelyn lainmukaisia perusteita.

Yleissopimuksessa 108 ei ole määritelty suostumusta, vaan asia on jätetty kansallisen lainsäädännön piiriin. **Euroopan neuvoston oikeudessa** pätevän suostumuksen edellytykset kuitenkin vastaavat edellä esitettyjä[260].

Muita siviilioikeuden mukaisia pätevän suostumuksen edellytyksiä, kuten oikeuskelpoisuutta, sovelletaan perustavanlaatuisina oikeudellisina ennakkoedellytyksinä luonnollisesti myös tietosuojan alalla. Oikeustoimikelvottoman henkilön antama suostumus on mitätön, eikä tällaisen henkilön henkilötietojen käsittelylle ole oikeudellista perustetta. Yleisessä tietosuoja-asetuksessa säädetään alaikäisten sopimusten tekemistä koskevasta oikeustoimikelpoisuudesta, että sen säännöt pätevän suostumuksen hankkimista koskevasta vähimmäisiästä eivät vaikuta jäsenvaltioiden yleiseen sopimusoikeuteen[261].

Suostumus on annettava selkeästi, jottei jää epäselvyyttä siitä, onko rekisteröity suostunut tietojensa käsittelyyn[262]. Suostumuksen on oltava yksiselitteinen, kun se koskee arkaluonteisten tietojen käsittelyä, ja se voidaan antaa suullisesti tai kirjallisesti[263]. Kirjallinen suostumus voidaan antaa sähköisesti[264]. Sekä **EU:n** että **Euroopan neuvoston oikeudessa** henkilötietojen käsittely on hyväksyttävä antamalla suostumusta ilmaiseva lausuma tai toteuttamalla selkeästi suostumusta ilmaiseva toimi[265].

259 *Ibid.*, 7 artiklan 1 kohta.

260 Uudistettu yleissopimus 108, 5 artiklan 2 kohta, uudistettu yleissopimus 108, selitysmuistio, 42–45 kohta.

261 Yleinen tietosuoja-asetus, 8 artiklan 3 kohta.

262 *Ibid.*, 6 artiklan 1 kohdan a alakohta ja 9 artiklan 2 kohdan a alakohta.

263 *Ibid.*, johdanto-osan 32 kappale.

264 *Ibid.*

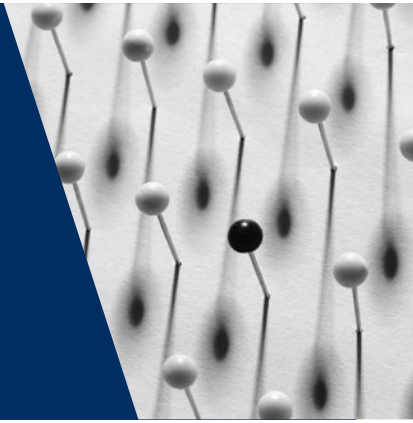
265 *Ibid.*, 4 artiklan 11 kohta; uudistetun yleissopimuksen 108 selitysmuistio, 42 kohta.

Suostumusta ei sen vuoksi pitäisi voida antaa vaikenemalla, valmiiksi rastitetuilla ruuduilla, valmiiksi täytetyillä lomakkeilla tai jättämällä jokin toimi toteuttamatta[266].

266 Yleinen tietosuoja-asetus, johdanto-osan 32 kappale; uudistettu yleissopimus 108, selitysmuistio, 42 kohta.

3

Euroopan tietosuojaoikeuden pääperiaatteet



EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta	**Lainmukaisuuden periaate**	Uudistettu yleissopimus 108, 5 artiklan 3 kohta
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta	**Kohtuullisuuden periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan a alakohta EIT, *K.H. ym. v. Slovakia*, nro 32881/04, 2009
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 2015	**Läpinäkyvyyden periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan a alakohta ja 8 artikla EIT, *Haralambie v. Romania*, nro 21737/03, 2009
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan b alakohta	**Käyttötarkoitus-sidonnaisuuden periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan c alakohta EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland* ja *Kärntner Landesregierung ym.* [suuri jaosto], 2014	**Tietojen minimoinnin periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan c alakohta
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan d alakohta EUT, C-553/07, *College van burgemeester en wethouders van Rotterdam vastaan E. E. Rijkeboer*, 2009	**Tietojen täsmällisyyden periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan d alakohta

EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan e alakohta EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland ja Kärntner Landesregierung ym.* [suuri jaosto], 2014	**Säilytyksen rajoittamisen periaate**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan e alakohta EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 2008
Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan f alakohta ja 32 artikla	**Tietojen turvallisuuden (eheyden ja luottamuksellisuuden) periaate**	Uudistettu yleissopimus 108, 7 artikla
Yleinen tietosuoja-asetus, 5 artiklan 2 kohta	**Osoitusvelvollisuuden periaate**	Uudistettu yleissopimus 108, 10 artikla

Yleisen tietosuoja-asetuksen 5 artiklassa esitetään henkilötietojen käsittelyn periaatteet. Ne ovat

- lainmukaisuus, kohtuullisuus ja läpinäkyvyys
- käyttötarkoitussidonnaisuus
- tietojen minimointi
- tietojen täsmällisyys
- säilytyksen rajoittaminen
- eheys ja luottamuksellisuus.

Periaatteet ovat lähtökohtana asetuksen seuraavissa artikloissa säädetyille yksityiskohtaisemmille säännöksille. Ne esitetään myös uudistetun yleissopimuksen 108 5, 7, 8 ja 10 artiklassa. Euroopan neuvoston ja EU:n myöhempää tietosuojalainsäädäntöä laadittaessa ja tulkittaessa on aina noudatettava näitä periaatteita. EU:n oikeudessa poikkeukset käsittelyn periaatteisin ovat sallittuja vain, jos ne vastaavat 12–22 artiklassa säädettyjä oikeuksia ja velvollisuuksia ja niissä noudatetaan perusoikeuksien ja -vapauksien keskeistä sisältöä. Näihin pääperiaatteisiin voidaan säätää poikkeuksia ja rajoituksia unionin oikeudessa ja kansallisessa lainsäädännössä[267]. Poikkeuksista ja rajoituksista on säädettävä laissa, niillä on oltava laillinen tarkoitus

267 Uudistettu yleissopimus 108, 11 artiklan 1 kohta; yleinen tietosuoja-asetus, 23 artiklan 1 kohta.

ja niiden on oltava välttämättömiä demokraattisessa yhteiskunnassa.[268] Kaikkien kolmen ehdon on täytyttävä.

3.1 Käsittelyn lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaatteet

Keskeiset kohdat

- Lainmukaisuuden, kohtuullisuuden ja läpinäkyvyyden periaatteet koskevat kaikkea henkilötietojen käsittelyä.
- Yleisen tietosuoja-asetuksen mukaan lainmukaisuus edellyttää jotakin seuraavista:
  - rekisteröity on antanut suostumuksensa
  - on tehtävä sopimus
  - on noudatettava lakisääteistä velvoitetta
  - on suojeltava rekisteröidyn tai toisen luonnollisen henkilön elintärkeitä etuja
  - on suoritettava yleistä etua koskeva tehtävä
  - on toteutettava rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut, jos rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä niitä.
- Henkilötietojen käsittelyn on oltava asianmukaista.
  - Rekisteröidylle on ilmoitettava riskistä, jotta voidaan varmistaa, että käsittelyllä ei ole ennakoimattomia kielteisiä vaikutuksia.
- Henkilötietojen käsittelyn on oltava läpinäkyvää.
  - Rekisterinpitäjien on ilmoitettava rekisteröidyille ennen näiden tietojen käsittelemistä muun muassa käsittelyn tarkoitus ja rekisterinpitäjän identiteetti ja osoite.
  - Käsittelytoimia koskevat tiedot on annettava selkeällä ja yksinkertaisella kielellä, jotta rekisteröidyt pystyvät ymmärtämään helposti käsittelyyn liittyvät säännöt, riskit, suojatoimet ja oikeudet.
  - Rekisteröidyillä on oikeus saada pääsy tietoihinsa riippumatta siitä, missä niitä käsitellään.

268 Yleinen tietosuoja-asetus, 23 artiklan 1 kohta.

3.1.1 Käsittelyn lainmukaisuus

EU:n ja Euroopan neuvoston tietosuojalakien mukaan henkilötietoja on käsiteltävä lainmukaisesti[269]. Lainmukainen käsittely edellyttää asianomaisen rekisteröidyn suostumusta tai muuta oikeutettua perustetta, josta säädetään tietosuojalainsäädännössä[270]. Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdassa on suostumuksen lisäksi viisi muuta lainmukaista perustetta eli käsittely on tarpeen sopimuksen täytäntöön panemiseksi, julkisen vallan käyttämiseksi, lakisääteisen velvoitteen noudattamiseksi, rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi tai rekisteröidyn elintärkeiden etujen suojaamiseksi. Tätä käsitellään tarkemmin 4.1 kohdassa.

3.1.2 Käsittelyn kohtuullisuus

EU:n ja Euroopan neuvoston tietosuojalakien mukaan henkilötietojen käsittelyn on lainmukaisuuden lisäksi oltava kohtuullista[271]. Kohtuullisuuden periaate koskee pääasiassa rekisterinpitäjän ja rekisteröidyn välistä suhdetta.

Rekisterinpitäjän on ilmoitettava rekisteröidyille ja suurelle yleisölle käsittelevänsä tietoja lainmukaisesti ja asianmukaisesti, ja sen on pystyttävä osoittamaan, että käsittelytoimet ovat yleisen tietosuoja-asetuksen mukaisia. Käsittelytoimia ei saa toteuttaa salaa, ja rekisteröityjen on oltava tietoisia mahdollisista riskeistä. Lisäksi rekisterinpitäjien tulisi mahdollisuuksien mukaan noudattaa rekisteröityjen toiveita, erityisesti silloin, kun rekisteröidyn suostumus on tietojenkäsittelyn oikeudellinen peruste.

Esimerkki: Asiassa *K.H. ym. v. Slovakia*[272] kantajina oli romanisyntyperää olevia naisia, joita oli hoidettu kahdessa itäisen Slovakian sairaalassa heidän raskautensa ja synnytyksensä aikana. Yksikään heistä ei pystynyt enää sen jälkeen saamaan lasta lukuisista yrityksistä huolimatta. Kansalliset tuomioistuimet määräsivät sairaalat sallimaan kantajien ja heidän edustajiensa

269 Uudistettu yleissopimus 108, 5 artiklan 3 kohta; yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta.

270 Euroopan unionin perusoikeuskirja, 8 artiklan 2 kohta, yleinen tietosuoja-asetus, johdanto-osan 40 kappale ja 6–9 artikla, uudistettu yleissopimus 108, 5 artiklan 2 kohta, uudistettu yleissopimus 108, selitysmuistio, 41 kohta.

271 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan a alakohta.

272 EIT, *K.H. ym. v. Slovakia*, nro 32881/04, 28.4.2009.

tutustua potilaskertomuksiin ja kirjata niistä otteita käsin mutta hylkäsivät pyynnön ottaa asiakirjoista valokopioita vedoten väärinkäytösten ehkäisemiseen. Valtion ihmisoikeussopimuksen 8 artiklan mukaisiin positiivisiin velvoitteisiin kuului selvästi velvollisuus saattaa rekisteröityjen saataville kopiot heitä koskevista tiedoista. Valtion tehtävänä oli määritellä, miten henkilötiedot kopioitaisiin, tai tarvittaessa esittää pakottavat syyt tästä kieltäytymiselle. Kantajien tapauksessa kansalliset tuomioistuimet perustelivat potilaskertomusten kopioinnin kieltämisen pääasiallisesti tarpeella suojata tietoja väärinkäytöiltä. Ihmisoikeustuomioistuin ei kuitenkaan voinut nähdä, miten kantajat, joille oli annettu mahdollisuus tutustua omiin potilaskertomuksiinsa, olisivat voineet käyttää väärin itseään koskevia tietoja. Lisäksi tällainen riski olisi voitu ehkäistä muilla keinoin kuin kieltämällä kertomusten kopiointi kantajilta, esimerkiksi rajoittamalla niiden henkilöiden määrää, joille annettiin oikeus tutustua asiakirjoihin. Valtio ei ollut osoittanut riittävän pakottavia syitä sille, miksi se ei ollut antanut kantajille asianmukaista mahdollisuutta tutustua omaa terveyttään koskeviin tietoihin. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Internetpalvelujen yhteydessä tietojenkäsittelyjärjestelmien on oltava ominaisuuksiltaan sellaisia, että rekisteröidyt voivat ymmärtää kunnolla, mitä heidän tiedoilleen tapahtuu. Kohtuullisuuden periaate menee joka tapauksessa avoimuusvelvoitteita pidemmälle, ja se voi liittyä myös henkilötietojen eettiseen käsittelyyn.

Esimerkki: Yliopiston tutkimusyksikkö tekee kokeen, jossa analysoidaan 50 henkilön mielialan vaihteluita. Tutkittavien on kirjattava ajatuksensa sähköiseen tiedostoon joka tunti tiettyyn aikaan. Nämä 50 henkilöä ovat antaneet suostumuksensa tähän tiettyyn projektiin ja tähän nimenomaiseen yliopiston toteuttamaan tietojen käyttöön. Tutkimusyksikössä huomataan pian, että ajatusten sähköinen kirjaaminen olisi erittäin hyödyllistä toisessa mielenterveyteen keskittyvässä projektissa, jota koordinoi toinen ryhmä. Yliopisto olisi rekisterinpitäjänä voinut käyttää samoja tietoja toisen ryhmän työhön ilman muita toimenpiteitä, joilla varmistetaan kyseisten tietojen käsittelyn lainmukaisuus, olettaen että tarkoitukset ovat yhteensopivia. Se kuitenkin ilmoitti tästä rekisteröidyille ja pyysi uutta suostumusta tutkimusta koskevien eettisten käytännesääntöjensä ja kohtuullisen käsittelyn periaatteiden mukaisesti.

3.1.3 Käsittelyn läpinäkyvyys

EU:n ja Euroopan neuvoston tietosuojalakien mukaan henkilötietoja on ”käsiteltävä [...] rekisteröidyn kannalta läpinäkyvästi”[273].

Tämän periaatteen mukaan rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet toimittaakseen rekisteröidylle – joka voi olla käyttäjä, kuluttaja tai asiakas – kaikki tiedot siitä, miten tämän tietoja käytetään[274]. Läpinäkyvyys voi koskea tietoja, jotka annetaan henkilölle ennen käsittelyn alkua[275], tietoja, joiden pitäisi olla vaivatta rekisteröityjen saatavilla käsittelyn aikana[276], sekä tietoja, joita annetaan rekisteröidyille, kun nämä ovat pyytäneet pääsyä omiin tietoihinsa[277].

Esimerkki: Asiassa *Haralambie v. Romania*[278] kantaja oli pyytänyt nähdä tiedot, joita salaisen palvelun organisaatio säilytti hänestä, mutta hänen pyyntönsä hyväksyttiin vasta viisi vuotta myöhemmin. Euroopan ihmisoikeustuomioistuin totesi, että henkilöiden, joiden tietoja viranomaiset säilyttivät, oli erittäin tärkeää voida tutustua tietoihinsa. Viranomaisilla oli velvollisuus tarjota tehokas menettely tällaisten tietojen saantiin. Tuomioistuin katsoi, ettei viiden vuoden viivettä kantajan tietopyynnön täyttämisessä voitu perustella sen enempää tiedostojen määrällä kuin arkistointijärjestelmän heikkouksillakaan. Viranomaiset eivät olleet tarjonneet kantajalle tehokasta ja toimivaa menettelyä henkilötietojen saamiseksi kohtuullisessa ajassa. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Käsittelytoimet on selitettävä rekisteröidyille helposti saatavilla olevalla tavalla niin, että he varmasti ymmärtävät, mitä heidän tiedoilleen tapahtuu. Tämä tarkoittaa, että rekisteröidyn on tiedettävä henkilötietojen käsittelyn nimenomainen tarkoitus henkilötietojen keruun yhteydessä[279]. Käsittelyn läpinäkyvyys edellyttää selkeän ja

273 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan a alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan a alakohta ja 8 kohta.

274 Yleinen tietosuoja-asetus, 12 artikla.

275 *Ibid.*, 13 ja 14 artikla.

276 Tietosuojatyöryhmä, *lausunto 2/2017 tietojenkäsittelystä työpaikalla*, s. 23.

277 Yleinen tietosuoja-asetus, 15 artikla.

278 EIT, *Haralambie v. Romania*, nro 21737/03, 27.10.2009.

279 Yleinen tietosuoja-asetus, johdanto-osan 39 kappale.

yksinkertaisen kielen käyttämistä[280]. Henkilötietojen käsittelyyn liittyvien riskien, sääntöjen, suojatoimien ja oikeuksien on oltava selkeitä asianomaisille henkilöille[281].

Euroopan neuvoston oikeudessa täsmennetään myös, että rekisterinpitäjän on annettava tietyt olennaiset tiedot rekisteröidyille ennakoivasti. Tiedot rekisterinpitäjän (tai yhteisrekisterinpitäjien) nimestä ja osoitteesta, tietojenkäsittelyn oikeusperustasta ja tarkoituksista, käsiteltävien tietojen ja vastaanottajien ryhmistä sekä keinoista käyttää oikeuksia voidaan antaa missä tahansa soveltuvassa muodossa (verkkosivustolla, henkilökohtaisten laitteiden teknologisilla välineillä jne.), kunhan tiedot esitetään asianmukaisesti ja tehokkaasti rekisteröidyille. Tiedot on esitettävä helposti saatavilla olevalla, luettavissa olevalla, ymmärrettävällä ja asianomaisten rekisteröityjen mukaan mukautetulla tavalla (esimerkiksi tarvittaessa lapsille soveltuvalla tavalla). Lisäksi on annettava kaikki lisätiedot, joita tarvitaan varmistamaan asianmukainen tietojenkäsittely tai jotka ovat siinä hyödyllisiä, kuten säilytysaika, tieto tietojenkäsittelyn taustalla olevista syistä, tai tiedot tietojen siirroista vastaanottajalle sopimuspuolessa tai muussa kuin sopimuspuolessa (myös siitä, takaako kyseinen muu kuin sopimuspuoli asianmukaisen suojan tason, tai toimenpiteistä, jotka rekisterinpitäjä on toteuttanut kyseisen asianmukaisen suojan tason takaamiseksi). [282]

Tietoihin pääsyä koskevan oikeuden[283] nojalla rekisteröidyllä on oikeus pyynnöstä saada tietää rekisterinpitäjältä, käsitelläänkö hänen tietojaan ja, jos käsitellään, mitä tietoja käsitellään[284]. Informoimista koskevan oikeuden[285] mukaan rekisterinpitäjien tai henkilötietojen käsittelijöiden on ilmoitettava henkilöille, joiden tietoja käsitellään, muun muassa käsittelyn tarkoitus, kesto ja keinot ennakoivasti eli lähtökohtaisesti ennen käsittelytoiminnan alkamista.

Esimerkki: Asiassa *Smaranda Bara ym. vastaan Preşidentele Casei Naţionale de Asigurări de Sănătate, Casa Naţională de Administrare Fiscală (ANAF)*[286] oli kyse siitä, että Romaniassa siirrettiin kansalliselta verohallinnolta

280 *Ibid.*

281 *Ibid.*

282 Uudistettu yleissopimus 108, selitysmuistio, 68 kohta.

283 Yleinen tietosuoja-asetus, 15 artikla.

284 Uudistettu yleissopimus 108, 8 artikla ja 9 artiklan 1 kohdan b alakohta.

285 Yleinen tietosuoja-asetus, 13 ja 14 artikla.

286 EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Naţională de Asigurări de Sănătate ym.*, 1.10.2015, 28–46 kohta.

kansalliselle sairausvakuutuskassalle itsenäisten ammatinharjoittajien tuloihin liittyviä verotietoja, joiden perusteella vaadittiin suorittamaan maksamattomat sairausvakuutusmaksut. Euroopan unionin tuomioistuinta pyydettiin määrittämään, olisiko rekisteröidylle pitänyt antaa etukäteen tietoa rekisterinpitäjän henkilöllisyydestä ja tietojen siirtämisen tarkoituksesta ennen kuin kansallinen sairausvakuutuskassa käsitteli tietoja. Tuomioistuin totesi, että kun jäsenvaltion viranomainen siirtää henkilötietoja toiselle viranomaiselle tietojen käsittelemistä varten, rekisteröidyille on ilmoitettava kyseisestä siirtämisestä tai käsittelystä.

Tietyissä tilanteissa sallitaan poikkeukset velvollisuudesta ilmoittaa rekisteröidyille tietojenkäsittelystä. Niitä käsitellään yksityiskohtaisemmin rekisteröidyn oikeuksia koskevassa 6.1 kohdassa.

3.2 Käyttötarkoitussidonnaisuuden periaate

Keskeiset kohdat

- Henkilötietojen käsittelyn tarkoitus on määriteltävä ennen käsittelyn aloittamista.
- Henkilötietoja ei saa käsitellä myöhemmin, jos uusi käsittelytarkoitus on yhteensopimaton alkuperäisen tarkoituksen kanssa. Yleisessä tietosuoja-asetuksessa tosin säädetään, että sääntöön ovat poikkeuksena yleisen edun mukaiset arkistointitarkoitukset, tieteelliset ja historialliset tutkimustarkoitukset ja tilastolliset tarkoitukset.
- Lähtökohtaisesti käyttötarkoitussidonnaisuuden periaate tarkoittaa, että kaikki henkilötietojen käsittely on tehtävä tiettyä hyvin määriteltyä tarkoitusta varten ja ainoastaan alkuperäisen tarkoituksen kanssa yhteensopivia määritettyjä lisätarkoituksia varten.

Käyttötarkoitussidonnaisuuden periaate on yksi Euroopan tietosuojalainsäädännön perusperiaatteista. Se liittyy tiiviisti läpinäkyvyyteen, ennakoitavuuteen ja käyttäjävalvontaan: jos käsittelyn tarkoitus on riittävän täsmällinen ja selkeä, henkilöt tietävät, mitä siltä voi odottaa, ja se edistää läpinäkyvyyttä ja oikeusvarmuutta. Tarkoituksen selkeä rajaaminen on myös tärkeää, jotta rekisteröidyt pystyvät käyttämään tehokkaasti oikeuksiaan, kuten oikeutta vastustaa käsittelyä.[287]

287 Tietosuojatyöryhmä (2013), *Opinion 3/2013 on purpose limitation*, WP 203, 2.4.2013.

Periaate edellyttää, että kaikki henkilötietojen käsittely on tehtävä tiettyä hyvin määriteltyä tarkoitusta varten ja ainoastaan alkuperäisen tarkoituksen kanssa yhteensopivia lisätarkoituksia varten.[288] Henkilötietojen käsittely määrittelemättömiin ja/tai rajoittamattomiin tarkoituksiin on siten lainvastaista. Henkilötietojen käsittely ilman tiettyä tarkoitusta ainoastaan sen perusteella, että tiedot voivat olla hyödyllisiä tulevaisuudessa, ei myöskään ole lainmukaista. Henkilötietojen käsittelyn lainmukaisuus riippuu käsittelyn tarkoituksesta, jonka on oltava yksiselitteinen, nimenomainen ja laillinen.

Jokaisella uudella henkilötietojen käsittelytarkoituksella, joka ei ole yhteensopiva alkuperäisen tarkoituksen kanssa, on oltava oma oikeudellinen peruste eikä käsittelyssä voida lähteä siitä, että tiedot on alun perin kerätty tai niitä on käsitelty toiseen lailliseen tarkoitukseen. Laillinen käsittely puolestaan rajoittuu alun perin määriteltyyn tarkoitukseen ja jokaiselle uudelle käsittelytarkoitukselle on oltava uusi erillinen oikeudellinen peruste. Esimerkiksi henkilötietojen luovuttamista kolmansille osapuolille on harkittava erityisen tarkasti, sillä luovutus vaatii todennäköisesti toisen oikeudellisen perusteen kuin tietojen kerääminen.

Esimerkki: Lentoyhtiö kerää asiakkaistaan tietoja varauksia varten, jotta lento voitaisiin suorittaa asianmukaisesti. Lentoyhtiö tarvitsee seuraavat tiedot: matkustajien paikkanumerot; erityiset liikuntarajoitukset, kuten pyörätuolin tarve; ja erityiset ruokavaatimukset, kuten kosher- tai halal-sääntöjen mukainen ruoka. Jos lentoyhtiötä pyydetään luovuttamaan nämä matkustajarekisterin tiedot kohdemaan maahanmuuttoviranomaiselle, tietoja käytetään myöhemmin maahanmuuton valvontaan, joka on eri tarkoitus kuin se, johon tiedot on kerätty. Näin ollen tietojen luovuttamiselle maahanmuuttoviranomaiselle tarvitaan uusi erillinen oikeudellinen peruste.

Tarkoituksen laajuuden ja rajojen määrittelyä varten uudistetussa yleissopimuksessa 108 ja yleisessä tietosuoja-asetuksessa viitataan yhteensopivuuden käsitteeseen: Tietoja voidaan käyttää alkuperäisen tarkoituksen kanssa yhteensopiviin tarkoituksiin alkuperäisen oikeudellisen perusteen nojalla. Tietoja ei voida näin ollen käsitellä myöhemmin tavalla, joka on rekisteröidyn kannalta odottamatonta, epäasianmukaista tai vastustettavaa.[289] Rekisterinpitäjän on otettava (muun muassa) seuraavat asiat huomioon arvioidessaan, voidaanko myöhempi käsittely katsoa yhteensopivaksi:

288 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan b alakohta.

289 Uudistettu yleissopimus 108, selitysmuistio, 49 kohta.

- ”henkilötietojen keruun tarkoitusten ja aiotun myöhemmän käsittelyn tarkoitusten väliset yhteydet;

- tilanne, jossa henkilötiedot on kerätty, erityisesti myöhempään käsittelyyn liittyvät rekisteröidyn kohtuulliset odotukset, jotka perustuvat hänen ja rekisterinpitäjän väliseen suhteeseen;

- henkilötietojen luonne;

- suunnitellun myöhemmän käsittelyn seuraukset rekisteröidyille; ja

- asianomaisten suojatoimien olemassaolo sekä alkuperäisessä että suunnitellussa käsittelyssä”.[290] Tämä voidaan tehdä esimerkiksi salauksen tai pseudonymisoinnin avulla.

Esimerkki: Sunshine-yhtiö saa asiakastietoja asiakkuudenhallintansa kautta. Se siirtää tiedot suoramarkkinointia harjoittavalle Moonlight-yhtiölle, joka haluaa käyttää näitä tietoja kolmansien osapuolien markkinointikampanjoissa. Tietojen siirtäminen Sunshine-yhtiöstä muiden yhtiöiden markkinointia varten on tietojen myöhempää käyttöä uuteen tarkoitukseen, joka on yhteensopimaton asiakkuudenhallinnan, eli Sunshine-yhtiön alkuperäisen asiakastietojen keräämisen tarkoituksen, kanssa. Tietojen siirtäminen Moonlight-yhtiölle tarvitsee näin ollen oman oikeudellisen perusteen.

Sen sijaan sitä, että Sunshine-yhtiö käyttää asiakashallintajärjestelmänsä tietoja omiin markkinointitarkoituksiinsa eli omia tuotteitaan koskevien markkinointiviestien lähettämiseen asiakkailleen, pidetään yleensä yhteensopivana tarkoituksena.

Yleisen tietosuoja-asetuksen ja uudistetun yleissopimuksen 108 mukaan myöhempi käsittely ”yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten” katsotaan lähtökohtaisesti yhteensopivaksi alkuperäisen tarkoituksen kanssa[291]. Kun tietoja käsitellään

290 Yleinen tietosuoja-asetus, johdanto-osan 50 kappale ja 6 artiklan 4 kohta; uudistettu yleissopimus 108, selitysmuistio, 49 kohta.

291 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan b alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta. Esimerkki vastaavasta kansallisesta säännöksestä on Itävallan tietosuojalaki (*Datenschutzgesetz*), Itävallan virallinen lehti I nro 165/1999, 46 kohta.

myöhemmin, on kuitenkin otettava käyttöön asianmukaiset suojatoimet, kuten tietojen anonymisointi, salaus tai pseudonymisointi sekä tietoihin pääsyn rajoitukset[292]. Yleisessä tietosuoja-asetuksessa lisätään, että ”[j]os rekisteröity on antanut suostumuksensa tai käsittely perustuu unionin oikeuteen tai jäsenvaltion lainsäädäntöön, joka muodostaa demokraattisessa yhteiskunnassa välttämättömän ja oikeasuhteisen toimenpiteen, jolla pyritään turvaamaan erityisesti yleiseen julkiseen etuun liittyviä tärkeitä tavoitteita, rekisterinpitäjälle olisi sallittava henkilötietojen myöhempi käsittely riippumatta tarkoitusten yhteensopivuudesta”.[293] Myöhemmässä käsittelyssä rekisteröidylle olisi näin ollen ilmoitettava näistä muista tarkoituksista ja hänen oikeuksistaan, kuten oikeudesta vastustaa henkilötietojen käsittelyä[294].

Esimerkki: Sunshine-yhtiö on kerännyt ja säilyttänyt asiakkuudenhallintatietoja asiakkaistaan. Se, että Sunshine-yhtiö käyttää samoja tietoja asiakkaidensa ostokäyttäytymisen tilastoanalyysiin, on sallittua, koska tilastointi on yhteensopiva tarkoitus. Tällöin ei tarvita muuta oikeudellista perustetta, kuten rekisteröityjen suostumusta. Sunshine-yhtiön on tilastotarkoituksiin tehtävässä myöhemmässä henkilötietojen käsittelyssä kuitenkin otettava käyttöön asianmukaiset suojatoimet rekisteröidyn oikeuksien ja vapauksien takaamiseksi. Esimerkiksi pseudonymisointi voi kuulua Sunshine-yhtiön käyttöön ottamiin teknisiin ja organisatorisiin toimenpiteisiin.

3.3 Tietojen minimoinnin periaate

Keskeiset kohdat

- Tietojenkäsittelyn on rajoituttava siihen, mikä on välttämätöntä laillisen tarkoituksen saavuttamiseksi.
- Henkilötietoja pitäisi käsitellä vain, kun käsittelyn tarkoitusta ei voida kohtuullisesti saavuttaa muilla keinoin.
- Tietojenkäsittelyllä ei saa kohtuuttomasti puuttua kyseessä oleviin etuihin, oikeuksiin ja vapauksiin.

292 Yleinen tietosuoja-asetus, 6 artiklan 4 kohta; uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta; uudistettu yleissopimus 108, selitysmuistio, 50 kohta.

293 Yleinen tietosuoja-asetus, johdanto-osan 50 kappale.

294 *Ibid.*

Vain sellaisia henkilötietoja voidaan käsitellä, jotka ovat ”asianmukaisia, olennaisia eivätkä liian laajoja siihen tarkoitukseen, mihin ne on kerätty ja missä niitä myöhemmin käsitellään”[295]. Käsiteltäväksi valittujen tietoryhmien on oltava välttämättömiä käsittelytoimille ilmoitetun tarkoituksen saavuttamiseksi, ja rekisterinpitäjän tulisi tiukasti rajata kerättävät henkilötiedot niihin tietoihin, jotka liittyvät suoraan käsittelyn nimenomaiseen tarkoitukseen.

Esimerkki: Asiassa *Digital Rights Ireland*[296] Euroopan unionin tuomioistuin pohti tietojen säilyttämistä koskevan direktiivin pätevyyttä. Sen tarkoituksena on yhdenmukaistaa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien henkilötietojen säilyttämistä koskevia kansallisia säännöksiä, jotta tietoja voidaan mahdollisesti siirtää toimivaltaisille viranomaisille vakavan rikollisuuden, kuten järjestäytyneen rikollisuuden ja terrorismin torjumiseksi. Vaikka tämä katsottiin tarkoitukseksi, joka todella vastaa yleisen edun mukaista tavoitetta, yleinen tapa, jolla direktiivi kattaa ”kaikki henkilöt ja kaikki sähköiset viestintävälineet sekä kaikki liikennetiedot ilman, että tehtäisiin mitään erottelua, rajoituksia tai poikkeuksia vakavan rikollisuuden torjunnan tavoitteen perusteella”, katsottiin ongelmalliseksi[297].

Erityisen yksityisyyttä suojaavan tekniikan avulla voidaan lisäksi toisinaan välttyä kokonaan henkilötietojen käytöltä tai käyttää toimenpiteitä, joilla vähennetään mahdollisuuksia yhdistää tiedot rekisteröityyn (esimerkiksi pseudonymisointia käyttämällä). Näin saadaan aikaan yksityisyyden kannalta suotuisa ratkaisu. Tämä on erityisen merkityksellistä laajoissa käsittelyjärjestelmissä.

Esimerkki: Kaupunginvaltuusto tarjoaa kaupungin julkisen liikenteen säännöllisille käyttäjille sirukortin tiettyä maksua vastaan. Käyttäjän nimi on kirjoitettu kortin pinnalle ja se löytyy myös sirulta sähköisessä muodossa. Aina kun henkilö matkustaa bussilla tai raitiovaunulla, hänen on käytettävä sirukorttia lukulaitteen edessä. Laite tarkistaa tiedot sähköisesti tietokannasta, joka sisältää matkakortin ostaneiden henkilöiden nimet.

295 Uudistettu yleissopimus 108, 5 artiklan 4 kohdan c alakohta; yleinen tietosuoja-asetus, 5 artiklan 1 kohdan c alakohta.

296 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd v. Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

297 *Ibid.*, 44 ja 57 kohta.

Tämä järjestelmä ei vastaa tietojen minimoinnin periaatetta parhaalla mahdollisella tavalla: henkilön oikeus käyttää kulkuneuvoja olisi mahdollista tarkistaa vertaamatta kortin sirulla olevia henkilötietoja tietokantaan. Siihen riittäisi esimerkiksi, että kortin sirulla olisi erityinen sähköinen kuva, kuten viivakoodi, joka kertoisi lukulaitteen kohdalla, onko kortti voimassa. Tällainen järjestelmä ei tallentaisi tietoa siitä, kuka on käyttänyt kulkuneuvoa ja milloin. Tämä olisi tietojen minimoinnin periaatteen kannalta paras vaihtoehto, sillä periaate velvoittaa välttämään tietojen keräämistä.

Uudistetun yleissopimuksen 108 5 artiklan 1 kohdassa esitetään vaatimus henkilötietojen käsittelyn suhteellisuudesta tavoitteena olevaan lailliseen tarkoitukseen nähden. Kaikkien asianomaisten etujen on oltava asianmukaisessa tasapainossa kaikissa käsittelyn vaiheissa. Se tarkoittaa, että tiedot, jotka ovat asianmukaisia ja merkityksellisiä mutta joilla puututtaisiin suhteettomasti kyseessä oleviin perusoikeuksiin ja -vapauksiin, olisi katsottava liiallisiksi[298].

3.4 Tietojen täsmällisyyden periaate

Keskeiset kohdat

- Rekisterinpitäjän on noudatettava tietojen täsmällisyyden periaatetta kaikissa käsittelytoimissa.
- Epätäsmälliset tiedot on poistettava tai oikaistava viipymättä.
- Tietoja on ehkä tarkistettava säännöllisesti ja saatettava ajan tasalle täsmällisyyden takaamiseksi.

Rekisterinpitäjä, jolla on hallussaan henkilötietoja, ei saa käyttää kyseisiä tietoja, ellei hän ole saanut kohtuullista varmuutta tietojen täsmällisyydestä ja ajantasaisuudesta[299].

298 Uudistettu yleissopimus 108, selitysmuistio, 52 kohta, yleinen tietosuoja-asetus, 5 artiklan 1 kohdan c alakohta.

299 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan d alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan d alakohta.

Velvollisuutta varmistaa henkilötietojen täsmällisyys on tarkasteltava tietojen käsittelyn tarkoitusta vasten.

Esimerkki: Asiassa *Rijkeboer*[300] Euroopan unionin tuomioistuin käsitteli Alankomaiden kansalaisen pyyntöä saada Amsterdamin kaupungin paikallisviranomaiselta tietoa niiden henkilöiden henkilöllisyydestä, joille oli luovutettu häntä koskevia kunnallisesta rekisteristä peräisin olevia tietoja kahden edellisen vuoden aikana, sekä luovutettujen tietojen sisällöstä. Euroopan unionin tuomioistuin totesi, että ”oikeus yksityisyyden kunnioittamiseen edellyttää, että rekisteröity voi varmistua hänen henkilötietojensa käsittelyn paikkansapitävyydestä ja laillisuudesta, eli erityisesti siitä, että häntä koskevat perustiedot ovat paikkansapitäviä ja että ne on annettu sallituille vastaanottajille”. Tuomioistuin viittasi sitten tietosuojadirektiivin johdanto-osaan, jossa todetaan, että rekisteröidyillä on oltava oikeus tutustua itseään koskeviin käsiteltäviin tietoihin voidakseen varmistua tietojen paikkansapitävyydestä[301].

Joissakin tapauksissa säilytettyjen tietojen päivittäminen voi olla lailla kiellettyä siksi, että tietojen säilyttämisen syynä on pääasiallisesti tapahtumien dokumentointi.

Esimerkki: Hoitotoimenpiteen tietoja ei saa muuttaa, eli ”päivittää”, vaikka tiedoista paljastuisi myöhemmin virheitä. Tällaisessa tilanteessa tietoihin voidaan vain lisätä huomautuksia, kunhan ne merkitään selvästi jälkeenpäin tehdyiksi lisäyksiksi.

Toisaalta joissakin tilanteissa tietoja on ehdottomasti tarkistettava ja tarvittaessa päivitettävä säännöllisesti, koska tietojen säilyminen virheellisinä voisi aiheuttaa rekisteröidylle haittaa.

Esimerkki: Kun joku haluaa tehdä luottosopimuksen pankin kanssa, pankki yleensä tarkistaa mahdollisen asiakkaansa luottokelpoisuuden. Tätä tarkoitusta varten on erityisiä tietokantoja, jotka sisältävät tietoja henkilöiden

300 EUT, C-553/07, *College van burgemeester en wethouders van Rotterdam vastaan E. E. Rijkeboer*, 7.5.2009.

301 Entisen direktiivin 95/46/EY johdanto-osan 41 kappale.

luottohistoriasta. Jos tällainen tietokanta antaisi virheellistä tai vanhentunutta tietoa jostakin henkilöstä, tälle henkilölle voisi aiheutua merkittäviä ongelmia. Näiden tietokantojen rekisterinpitäjien onkin noudatettava täsmällisyyden periaatetta erityisen huolellisesti.

3.5 Säilytyksen rajoittamisen periaate

Keskeiset kohdat

- Säilytyksen rajoittamisen periaate tarkoittaa, että henkilötiedot on poistettava tai tehtävä anonyymeiksi heti, kun niitä ei enää tarvita siihen tarkoitukseen, jota varten niitä kerättiin.

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan e alakohdassa sekä uudistetun yleissopimuksen 108 5 artiklan 4 kohdan e alakohdassa vaaditaan, että ”ne on säilytettävä muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen tietojenkäsittelyn tarkoitusten toteuttamista varten”. Tiedot on näin ollen poistettava tai niistä on tehtävä anonyymeja, kun tarkoitus on toteutettu. Siksi ”[r]ekisterinpitäjän olisi asetettava määräajat henkilötietojen poistoa tai niiden säilyttämisen tarpeellisuuden määräaikaistarkastelua varten, jotta voidaan varmistaa, ettei henkilötietoja säilytetä pidempään kuin on tarpeen”[302].

Asiassa *S. ja Marper*, Euroopan ihmisoikeustuomioistuin totesi, että Euroopan neuvoston asiaa koskevien asiakirjojen pääperiaatteet sekä sopimuspuolien lainsäädäntö ja oikeuskäytäntö edellyttivät, että tietoja säilytetään oikeassa suhteessa niiden keräämisen tarkoitukseen ja vain rajoitetun ajan, erityisesti poliisialalla[303].

302 Yleinen tietosuoja-asetus, johdanto-osan 39 kappale.

303 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008; ks. myös esim. EIT, *M.M. v. Yhdistynyt kuningaskunta*, nro 24029/07, 13.11.2012.

Esimerkki: Asiassa *S. ja Marper*[304] Euroopan ihmisoikeustuomioistuin totesi, että kahden kantajan sormenjälkien, solunäytteiden ja dna-tunnisteiden säilyttäminen määrittelemättömän ajan oli suhteetonta ja tarpeetonta demokraattisessa yhteiskunnassa, koska toisen kantajan rikosoikeudenkäynti oli päättynyt syyttömäksi toteamiseen ja toisen keskeyttämiseen.

Henkilötietojen säilyttämisen aikarajoitus koskee kuitenkin vain tietoja, joita säilytetään sellaisessa muodossa, että rekisteröidyt voidaan tunnistaa. Tarpeettomia tietoja voitaisiin siis säilyttää laillisesti tekemällä ne anonyymeiksi.

Historiantutkimusta taikka tilastollisia tai tieteellisiä yleisen edun mukaisia tarkoituksia varten arkistoituja tietoja voidaan säilyttää kauemmin, mikäli niitä käytetään vain mainittuihin tarkoituksiin[305]. Henkilötietojen jatkuvaa säilyttämistä ja käyttöä varten on kuitenkin otettava käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet, jotta rekisteröidyn oikeuksia ja vapauksia voidaan suojata.

Uudistetussa yleissopimuksessa 108 sallitaan myös poikkeukset säilytyksen rajoittamisen periaatteeseen, jos niistä säädetään laissa, jos niissä kunnioitetaan perusoikeuksien ja -vapauksien keskeistä sisältöä ja jos ne ovat oikeassa suhteessa useiden laillisten tarkoitusten saavuttamiseen nähden[306]. Näitä tarkoituksia ovat muun muassa kansallisen turvallisuuden suojelu, rikosten tutkiminen ja rikoksista syytteeseen asettaminen, rikosoikeudellisten seuraamusten täytäntöönpano, rekisteröidyn suojelu ja toisten ihmisten oikeuksien ja perusvapauksien suojelu.

Esimerkki: Asiassa *Digital Rights Ireland*[307] Euroopan unionin tuomioistuin pohti tietojen säilyttämistä koskevan direktiivin pätevyyttä. Sen tarkoituksena on yhdenmukaistaa yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien henkilötietojen säilyttämistä koskevia kansallisia säännöksiä vakavan rikollisuuden, kuten järjestäytyneen rikollisuuden ja terrorismin torjumiseksi. Tietojen säilyttämistä koskevassa direktiivissä säädetään tietojen

304 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008.

305 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan e alakohta, uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta ja 11 artiklan 2 kohta.

306 Uudistettu yleissopimus 108, 11 artiklan 1 kohta, uudistettu yleissopimus 108, selitysmuistio, 91–98 kohta.

307 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

”säilyttämisestä vähintään kuuden kuukauden ajan tekemättä minkäänlaista eroa tämän direktiivin 5 artiklassa säädettyjen tietoluokkien välillä sen mukaan, kuinka hyödyllisiä ne mahdollisesti ovat tavoitellun päämäärän kannalta, tai kyseessä olevien henkilöiden mukaan”[308]. Euroopan unionin tuomioistuin nosti myös esiin sen, että tietojen säilyttämistä koskevassa direktiivissä ei ole objektiivisia perusteita, joiden nojalla tietojen säilyttämisen täsmällinen kesto – joka voi olla vähintään kuusi kuukautta ja enintään 24 kuukautta – on määritettävä sen takaamiseksi, että se rajoittuu täysin välttämättömään.[309]

3.6 Tietoturvan periaate

Keskeiset kohdat

- Henkilötietojen turvallisuus ja luottamuksellisuus ovat keskeisiä rekisteröityyn kohdistuvien haitallisten vaikutusten estämisessä.
- Turvatoimenpiteet voivat olla teknisiä ja/tai organisatorisia.
- Henkilötietoja voidaan suojata pseudonymisoinnilla.
- Turvatoimenpiteiden asianmukaisuudesta on päätettävä tapauskohtaisesti, ja ne on tarkistettava säännöllisesti.

Tietoturvan periaate edellyttää asianmukaisten teknisten tai organisatoristen toimenpiteiden käyttöönottoa henkilötietojen käsittelyssä, jotta tietoja voidaan suojella tahattomalta, luvattomalta tai lainvastaiselta pääsyltä, käytöltä, muuttamiselta, luovuttamiselta, häviämiseltä, tuhoamiselta tai vahingoittumiselta.[310] Yleisessä tietosuoja-asetuksessa todetaan, että rekisterinpitäjän ja henkilötietojen käsittelijän on kyseisiä toimenpiteitä toteuttaessaan otettava huomioon ”uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit”[311]. Kunkin tapauksen erityisolosuhteiden mukaan

308 *Ibid.*, 63 kohta.

309 *Ibid.*, 64 kohta.

310 Yleinen tietosuoja-asetus, johdanto-osan 39 kappale ja 5 artiklan 1 kohdan f alakohta; uudistettu yleissopimus 108, 7 artikla.

311 Yleinen tietosuoja-asetus, 32 artiklan 1 kohta.

asianmukaisia teknisiä ja organisatorisia toimenpiteitä voivat olla esimerkiksi henkilötietojen pseudonymisointi ja salaus ja/tai menettely, jolla testataan ja arvioidaan säännöllisesti toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi[312].

Kuten 2.1.1 kohdassa selitettiin, tietojen pseudonymisointi tarkoittaa henkilötietojen tunnisteiden – joiden avulla rekisteröity voidaan tunnistaa – korvaamista ns. salanimellä ja tunnisteiden pitämistä erillään teknisten tai organisatoristen toimenpiteiden avulla. Pseudonymisointia ei pidä sekoittaa anonymisointiin, jossa kaikki yhteydet, joista henkilön voi tunnistaa, poistetaan.

Esimerkki: Virke ”huhtikuun 3. päivänä 1967 syntynyt Charles Spencer on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä” voidaan pseudonymisoida esimerkiksi seuraavasti:

”C. S. 1967 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä” tai

”324 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä” tai

”YESz320l on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä”.

Pseudonymisoitujen tietojen käyttäjillä ei yleensä ole mahdollisuutta tunnistaa, että ”huhtikuun 3. päivänä 1967 syntynyt Charles Spencer” on ”324” tai ”YESz3201”. Tällaiset tiedot ovat siis todennäköisemmin turvassa väärinkäytöltä.

Ensimmäinen esimerkkivirke on kuitenkin heikoiten suojattu. Jos virkettä ”C.S. 1967 on nelilapsisen perheen isä, hänellä on kaksi poikaa ja kaksi tytärtä” käytettäisiin pienessä kylässä, jossa Charles Spencer asuu, hänet voitaisiin helposti tunnistaa. Pseudonymisoinnissa käytettävä menetelmä vaikuttaa tietosuojan kattavuuteen.

Henkilötietojen tunnisteiden salaamista tai niiden säilyttämistä eri paikassa käytetään monissa tilanteissa henkilöiden henkilöllisyyden salaamiseksi. Se on erityisen hyödyllistä silloin, kun rekisterinpitäjien on varmistettava, että ne käsittelevät samojen rekisteröityjen tietoja, mutta niiden ei tarvitse eikä pidä tietää rekisteröityjen

312 *Ibid.*

todellista henkilöllisyyttä. Näin voi olla esimerkiksi silloin, kun tutkija tutkii taudin kehittymistä potilailla, joiden henkilöllisyys tiedetään vain sairaalassa, jossa heitä on hoidettu ja josta tutkija on saanut pseudonymisoidut potilastiedot. Pseudonymisointi on näin ollen tärkeä työkalu yksityisyyttä suojaavan tekniikan varastossa. Se voi auttaa merkittävästi sisäänrakennetun yksityisyydensuojan toteuttamisessa. Tällä tarkoitetaan tietosuojan sisällyttämistä kehittyneisiin tiedonkäsittelyjärjestelmiin jo suunnitteluvaiheessa.

Yleisen tietosuoja-asetuksen 25 artiklassa käsitellään sisäänrakennettua tietosuojaa. Siinä viitataan yksiselitteisesti pseudonymisointiin esimerkkinä asianmukaisista teknisistä ja organisatorisista toimenpiteistä, joita rekisterinpitäjien pitäisi ottaa käyttöön, jotta tietosuojaperiaatteet voitaisiin toteuttaa ja tarvittavat suojatoimet saataisiin käsittelyn osaksi. Näin toimiessaan rekisterinpitäjät täyttävät asetuksen vaatimukset ja suojaavat rekisteröityjen oikeuksia käsitellessään heidän henkilötietojaan.

Hyväksyttyjen käytännesääntöjen tai hyväksytyn sertifiointimekanismin noudattaminen voi auttaa sen osoittamisessa, että käsittelyn turvallisuutta koskevaa vaatimusta noudatetaan[313]. Lausunnossaan tietosuojan vaikutuksista matkustajarekisteritietojen käsittelyyn Euroopan neuvosto antaa lisää esimerkkejä henkilötietojen suojaa matkustajarekisterijärjestelmissä koskevista asianmukaisista turvatoimista. Niitä ovat muun muassa tietojen säilyttäminen turvallisessa fyysisessä ympäristössä, pääsyn rajoittaminen kerrostetulla kirjautumisella ja tietojen välittämisen suojaaminen vahvalla salauksella.[314]

Esimerkki: Verkkoyhteisöpalvelujen verkkosivustot ja sähköpostipalvelujen tarjoajat antavat käyttäjille mahdollisuuden lisätä tarjoamiinsa palveluihin tietoturvan lisäkerroksen ottamalla käyttöön kaksivaiheisen todentamisen. Henkilökohtaisen salasanan antamisen lisäksi käyttäjien on tehtävä toinen kirjautuminen päästäkseen omalle tililleen. Toisessa kirjautumisessa voidaan esimerkiksi antaa omaan tiliin liitettyyn matkapuhelinnumeroon lähetetty turvakoodi. Tällä tavalla kaksivaiheisella todentamisella henkilötietoja voidaan suojella entistä paremmin hakkeroijien luvattomalta pääsyltä henkilökohtaisille tileille.

313 *Ibid.*, 32 artiklan 3 kohta.

314 Euroopan neuvosto, yleissopimuksen 108 komitea, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19.8.2016, s. 9.

Uudistetun yleissopimuksen 108 selitysmuistiossa annetaan lisää esimerkkejä asianmukaisista suojatoimista. Niitä ovat muun muassa vaitiolovelvollisuuden käyttöönotto ja pätevien teknisten turvatoimenpiteiden, kuten tietojen salauksen, hyväksyminen.[315] Kun erityisiä suojatoimenpiteitä otetaan käyttöön, rekisterinpitäjän – tai soveltuvin osin henkilötietojen käsittelijän – olisi otettava huomioon useita tekijöitä, kuten käsiteltävien henkilötietojen luonne ja määrä, mahdolliset haitalliset seuraukset rekisteröidyille ja tietoihin pääsyn rajoittamisen tarve[316]. Asianmukaisten suojatoimenpiteiden käyttöönotossa on otettava huomioon tietoturvamenetelmien ja tietojenkäsittelytekniikoiden uusin tekniikka. Toimenpiteiden kustannusten on oltava oikeassa suhteessa mahdollisten riskien vakavuuteen ja todennäköisyyteen. Suojatoimenpiteitä on tarkistettava määräajoin, jotta niitä voidaan tarvittaessa päivittää[317].

Jos tapahtuu henkilötietojen tietoturvaloukkaus, rekisterinpitäjän on sekä uudistetun yleissopimuksen 108 että yleisen tietosuoja-asetuksen mukaan ilmoitettava toimivaltaiselle viranomaiselle loukkauksesta sekä yksilöiden oikeuksille ja vapauksille aiheutuvista riskeistä ilman aiheetonta viivytystä[318]. Rekisteröidylle puolestaan on ilmoitettava samalla tavalla, kun henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin hänen oikeuksilleen ja vapauksilleen[319]. Rekisteröidylle on ilmoitettava tietoturvaloukkauksesta selkeällä ja yksinkertaisella kielellä[320]. Henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksesta rekisterinpitäjälle ilman aiheetonta viivytystä saatuaan sen tietoonsa[321]. Tietyissä tilanteissa ilmoitusvelvollisuuteen voidaan soveltaa poikkeuksia. Rekisterinpitäjän ei esimerkiksi tarvitse ilmoittaa valvontaviranomaiselle, ”jos henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä”[322]. Rekisteröidylle ei myöskään tarvitse ilmoittaa, kun rekisterinpitäjä on toteuttanut suojatoimenpiteet henkilötietojen muuttamiseksi muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, tai kun jatkotoimenpiteillä varmistetaan, että suuri riski ei

315 Uudistettu yleissopimus 108, selitysmuistio, 56 kohta.

316 *Ibid.*, 62 kohta.

317 *Ibid.*, 63 kohta.

318 Uudistettu yleissopimus 108, 7 artiklan 2 kohta; yleinen tietosuoja-asetus, 33 artiklan 1 kohta.

319 Uudistettu yleissopimus 108, 7 artiklan 2 kohta; yleinen tietosuoja-asetus, 34 artiklan 1 kohta.

320 Yleinen tietosuoja-asetus, 34 artiklan 2 kohta.

321 *Ibid.*, 33 artiklan 1 kohta.

322 *Ibid.*, 32 artiklan 1 kohta.

enää todennäköisesti toteudu[323]. Jos henkilötietojen tietoturvaloukkauksista ilmoittaminen rekisteröidyille vaatisi rekisterinpitäjältä kohtuutonta vaivaa, julkisella tiedonannolla tai vastaavalla toimenpiteellä voidaan varmistaa, että ”rekisteröidyille tiedotetaan yhtä tehokkaalla tavalla”[324].

3.7 Osoitusvelvollisuuden periaate

Keskeiset kohdat

- Osoitusvelvollisuus edellyttää rekisterinpitäjiltä ja henkilötietojen käsittelijöiltä aktiivisia ja jatkuvia toimenpiteitä tietosuojan edistämiseksi ja turvaamiseksi henkilötietoja käsiteltäessä.
- Rekisterinpitäjät ja henkilötietojen käsittelijät vastaavat siitä, että niiden käsittelytoimissa noudatetaan tietosuojalainsäädäntöä ja niiden velvoitteita.
- Rekisterinpitäjien on pystyttävä milloin tahansa todistamaan tietosuojamääräysten noudattaminen rekisteröidyille, yhteiskunnalle ja valvontaviranomaisille. Rekisterinpitäjien on myös noudatettava joitakin osoitusvelvollisuuteen tiiviisti liittyviä velvoitteita (kuten käsittelytoimien kirjaaminen ja tietosuojavastaavan nimittäminen).

Yleisen tietosuoja-asetuksen ja uudistetun yleissopimuksen 108 mukaan rekisterinpitäjä vastaa siitä, ja sen on pystyttävä osoittamaan se, että tässä luvussa kuvattuja tietojenkäsittelyn periaatteita on noudatettu[325]. Tämän takia rekisterinpitäjän on toteutettava tarvittavat asianmukaiset tekniset ja organisatoriset toimenpiteet[326]. Vaikka yleisen tietosuoja-asetuksen 5 artiklan 2 kohdan osoitusvelvollisuuden periaate on osoitettu vain rekisterinpitäjille, myös henkilötietojen käsittelijöiden odotetaan olevan osoitusvelvollisia, koska niiden on noudatettava useita velvoitteita ja koska ne liittyvät tiiviisti osoitusvelvollisuuteen.

EU:n ja Euroopan neuvoston tietosuojalainsäädännössä säädetään myös, että rekisterinpitäjä on vastuussa 3.1–3.6 kohdassa käsiteltyjen tietosuojaperiaatteiden noudattamisesta, ja sen on pystyttävä varmistamaan niiden noudattaminen.[327] Tieto-

323 *Ibid.*, 34 artiklan 3 kohdan a ja b alakohta.

324 *Ibid.*, 34 artiklan 3 kohdan c alakohta.

325 *Ibid.*, 5 artiklan 2 kohta, uudistettu yleissopimus 108, 10 artiklan 1 kohta.

326 Yleinen tietosuoja-asetus, 24 artikla.

327 *Ibid.*, 5 artiklan 2 kohta, uudistettu yleissopimus 108, 10 artiklan 1 kohta.

suojatyöryhmä panee merkille, että ”menettelyjen ja mekanismien tyyppi vaihtelisi tietojenkäsittelyyn liittyvien riskien ja tietojen luonteen mukaan”[328].

Rekisterinpitäjät voivat helpottaa tämän vaatimuksen noudattamista eri tavoilla, muun muassa

- laatimalla selosteen käsittelytoimista ja saattamalla selosteen pyydettäessä valvontaviranomaisen saataville[329]
- tietyissä tilanteissa nimittämällä tietosuojavastaavan, joka otetaan mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn[330]
- toteuttamalla arviointeja käsittelytoimien vaikutuksista henkilötietojen suojalle, jos tietyntyyppinen käsittely todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta korkean riskin[331]
- varmistamalla sisäänrakennetun ja oletusarvoisen tietosuojan toteutumisen[332]
- ottamalla käyttöön yksityiskohtaisia sääntöjä ja menettelyjä rekisteröidyn oikeuksien käyttöä varten[333]
- noudattamalla hyväksyttyjä käytännesääntöjä tai sertifiointimekanismeja[334].

Vaikka yleisen tietosuoja-asetuksen 5 artiklan 2 kohdassa tarkoitettua osoitusvelvollisuuden periaatetta ei ole nimenomaisesti osoitettu henkilötietojen käsittelijöille, osoitusvelvollisuuteen liittyy säännöksiä, jotka sisältävät velvollisuuksia myös niille. Niitä ovat muun muassa selosteen ylläpitäminen käsittelytoimista ja tietosuojavastaavan nimittäminen kaikkiin sitä edellyttäviin käsittelytoimiin.[335] Henkilötietojen käsittelijän on myös varmistettava, että kaikki tietojen turvallisuuden tarvittavat

328 Tietosuojatyöryhmä, *lausunto 3/2010 tilivelvollisuuden periaatteesta*, WP 173, Bryssel, 13.7.2010, 12 kohta.

329 Yleinen tietosuoja-asetus, 30 artikla.

330 *Ibid.*, 37–39 artikla.

331 *Ibid.*, 35 artikla; uudistettu yleissopimus 108, 10 artiklan 2 kohta.

332 Yleinen tietosuoja-asetus, 25 artikla; uudistettu yleissopimus 108, 10 artiklan 2 ja 3 kohta.

333 *Ibid.*, 12 ja 24 artikla.

334 *Ibid.*, 40 ja 42 artikla.

335 *Ibid.*, 5 artiklan 2 kohta, 30 ja 37 artikla.

toimenpiteet on toteutettu[336]. Rekisterinpitäjän ja henkilötietojen käsittelijän välisessä oikeudellisesti sitovassa sopimuksessa on määrättävä, että henkilötietojen käsittelijän on autettava rekisterinpitäjää joissakin noudattamista koskevissa vaatimuksissa. Niitä ovat esimerkiksi tietosuojaa koskevan vaikutustenarvioinnin tekeminen ja ilmoittaminen rekisterinpitäjälle kaikista henkilötietojen tietoturvaloukkauksista heti, kun ne tulevat henkilötietojen käsittelijän tietoon.[337]

Taloudellisen yhteistyön ja kehityksen järjestö (OECD) hyväksyi vuonna 2013 yksityisyyden suojaa koskevat suuntaviivat, joissa korostettiin rekisterinpitäjien tärkeää roolia tietosuojan toteuttamisessa käytännössä. Suuntaviivoissa käsitellään osoitusvelvollisuuden periaatetta toteamalla, että rekisterinpitäjän tulisi olla vastuussa sellaisten toimenpiteiden noudattamisesta, joilla toteutetaan aiemmin mainittuja olennaisia periaatteita[338].

Esimerkki: Lainsäädäntöön liittyvä esimerkki osoitusvelvollisuuden periaatteen merkityksestä on sähköisen viestinnän tietosuojadirektiiviin 2002/58/EY vuonna 2009 tehty muutos[339]. Muutetun direktiivin 4 artiklassa säädetään velvollisuudesta toteuttaa toimenpiteitä, joilla on ”varmistettava henkilötietojen käsittelyä koskevan turvapolitiikan toteuttaminen”. Lainsäätäjä siis katsoi, että direktiivin turvasäännösten osalta oli tarpeen lisätä nimenomainen vaatimus turvapolitiikan laatimisesta ja toteuttamisesta.

Tietosuojatyöryhmän lausunnon[340] mukaan vastuullisuuden ytimessä on rekisterinpitäjän velvollisuus

- toteuttaa toimenpiteitä, joilla tavallisissa olosuhteissa varmistetaan, että käsittelytoimissa noudatetaan tietosuojasääntöjä; ja

336 *Ibid.*, 28 artiklan 3 kohdan c alakohta.

337 *Ibid.*, 28 artiklan 3 kohdan d alakohta.

338 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data*, 14 artikla.

339 Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta, EUVL 2009, L 337, s. 11.

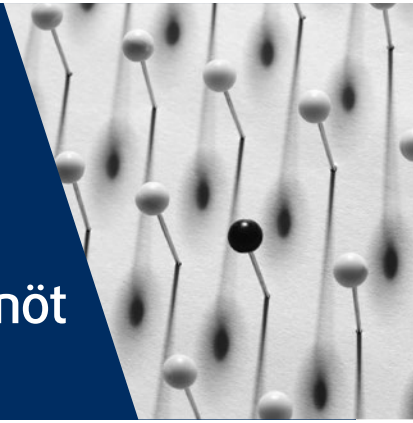
340 Tietosuojatyöryhmä, *lausunto 3/2010 tilivelvollisuuden periaatteesta*, WP 173, Bryssel, 13.7.2010.

- ylläpitää asiakirjoja, joilla se voi todistaa rekisteröidyille ja valvontaviranomaisille, mitä toimenpiteitä se on toteuttanut tietosuojasääntöjen noudattamiseksi.

Näin ollen osoitusvelvollisuuden periaate velvoittaa rekisterinpitäjät osoittamaan aktiivisesti sääntöjen noudattamisen sen sijaan, että ne vain odottaisivat, että rekisteröidyt tai valvontaviranomaiset tuovat esiin puutteita.

4

Euroopan tietosuojaoikeuden säännöt



EU	Käsiteltävät asiat	EN
Tietojen käsittelyn lainmukaisuutta koskevat säännöt		
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan a alakohta EUT, C-543/09, *Deutsche Telekom AG vastaan Bundesrepublik Deutschland*, 2011 EUT, C-536/15, *Tele2 (Netherlands) BV ym. vastaan Autoriteit Consument en Markt (AMC)*, 2017	**Suostumus**	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta ja 3 artiklan 6 kohta Uudistettu yleissopimus 108, 5 artiklan 2 kohta
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan b alakohta	**(Sopimusta edeltävä suhde) sopimussuhde**	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan c alakohta	**Rekisterinpitäjän lakisääteiset velvoitteet**	Profilointia koskeva suositus, 3 artiklan 4 kohdan a alakohta
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan d alakohta	**Rekisteröidyn elintärkeät edut**	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan e alakohta EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 2008	**Yleinen etu ja julkisen vallan käyttäminen**	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta

EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus, 6 artiklan 1 kohdan f alakohta EUT, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vastaan Rīgas pašvaldības SIA "Rīgas satiksme"*, 2017 EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 2011	**Muiden oikeutetut edut**	Profilointia koskeva suositus, 3 artiklan 4 kohdan b alakohta EIT, *Y v. Turkki*, nro 648/10, 2015
Yleinen tietosuoja-asetus, 6 artiklan 4 kohta	**Poikkeus käyttötarkoitussidonnaisuuteen: myöhempi käsittely muihin tarkoituksiin**	Uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta
Arkaluonteisten tietojen lainmukaista käsittelyä koskevat säännöt		
Yleinen tietosuoja-asetus, 9 artiklan 1 kohta	**Yleinen käsittelykielto**	Uudistettu yleissopimus 108, 6 artikla
Yleinen tietosuoja-asetus, 9 artiklan 2 kohta	**Poikkeukset yleisestä säännöstä**	Uudistettu yleissopimus 108, 6 artikla
Turvallista käsittelyä koskevat säännöt		
Yleinen tietosuoja-asetus, 32 artikla	**Velvollisuus turvata käsittely**	Uudistettu yleissopimus 108, 7 artiklan 1 kohta EIT, I v. Suomi, nro 20511/03, 2008
Yleinen tietosuoja-asetus, 28 artikla ja 32 artiklan 1 kohdan b alakohta	**Salassapitovelvollisuus**	Uudistettu yleissopimus 108, 7 artiklan 1 kohta
Yleinen tietosuoja-asetus, 34 artikla Sähköisen viestinnän tietosuojadirektiivi, 4 artiklan 2 kohta	**Ilmoitukset tietoturvaloukkauksista**	Uudistettu yleissopimus 108, 7 artiklan 2 kohta
Osoitusvelvollisuutta ja sääntöjen noudattamista edistävät säännöt		
Yleinen tietosuoja-asetus, 12, 13 ja 14 artikla	**Läpinäkyvyys yleisesti**	Uudistettu yleissopimus 108, 8 artikla
Yleinen tietosuoja-asetus, 37, 38 ja 39 artikla	**Tietosuojavastaavat**	Uudistettu yleissopimus 108, 10 artiklan 1 kohta
Yleinen tietosuoja-asetus, 30 artikla	**Seloste käsittelytoimista**	

EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus, 35 ja 36 artikla	Vaikutustenarviointi ja ennakkokuuleminen	Uudistettu yleissopimus 108, 10 artiklan 2 kohta
Yleinen tietosuoja-asetus, 33 ja 34 artikla	Ilmoitukset tietoturvaloukkauksista	Uudistettu yleissopimus 108, 7 artiklan 2 kohta
Yleinen tietosuoja-asetus, 40 ja 41 artikla	Käytännesäännöt	
Yleinen tietosuoja-asetus, 42 ja 43 artikla	Sertifiointi	
Sisäänrakennettu ja oletusarvoinen tietosuoja		
Yleinen tietosuoja-asetus, 25 artiklan 1 kohdan a alakohta	Sisäänrakennettu tietosuoja	Uudistettu yleissopimus 108, 10 artiklan 2 kohta
Yleinen tietosuoja-asetus, 25 artiklan 1 kohdan b alakohta	Oletusarvoinen tietosuoja	Uudistettu yleissopimus 108, 10 artiklan 3 kohta

Periaatteet ovat väistämättä yleisluonteisia. Niiden soveltamisessa konkreettisiin tapauksiin on tiettyä tulkinnan varaa ja vapautta keinojen valinnassa. **Euroopan neuvoston oikeudessa** on jätetty uudistetun yleissopimuksen 108 osapuolille tehtäväksi rajata kansallisessa lainsäädännössä tätä tulkinnan varaa. **EU:n oikeudessa** tilanne on toinen: tietosuojan turvaamiseksi sisämarkkinoilla on katsottu, että EU:n tasolla tarvitaan yksityiskohtaisia sääntöjä, joilla yhdenmukaistetaan tietosuojan tasoa jäsenvaltioiden kansallisissa lainsäädännöissä. Yleisessä tietosuoja-asetuksessa säädetään 5 artiklassa esitettyjen periaatteiden yhteydessä yksityiskohtaisia sääntöjä, jotka ovat suoraan sovellettavissa kansallisessa oikeusjärjestyksessä. Seuraavat huomiot Euroopassa sovellettavista yksityiskohtaisista tietosuojasäännöistä liittyvät näin ollen lähinnä EU:n lainsäädäntöön.

4.1 Lainmukaista käsittelyä koskevat säännöt

Keskeiset kohdat

- Henkilötietojen käsittely on lainmukaista, jos jokin seuraavista ehdoista täyttyy:
  - käsittely perustuu rekisteröidyn suostumukseen
  - sopimussuhde edellyttää henkilötietojen käsittelyä
  - käsittely on tarpeen rekisteripitäjän lakisääteisen velvoitteen noudattamiseksi
  - rekisteröityjen tai muiden henkilöiden elintärkeät edut edellyttävät heidän henkilötietojensa käsittelyä
  - käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi
  - käsittelyn syynä ovat rekisterinpitäjän tai muiden henkilöiden oikeutetut edut, mutta vain siinä tapauksessa, että ne eivät ole ristiriidassa rekisteröityjen perusoikeuksien suojaan liittyvien etujen kanssa.
- Arkaluonteisten henkilötietojen lainmukaisessa käsittelyssä on noudatettava erikseen määriteltyä, tiukempaa menettelyä.

4.1.1 Tietojenkäsittelyn lainmukaiset perusteet

Yleisen tietosuoja-asetuksen II luvun nimi on ”Periaatteet”. Sen mukaan kaikessa henkilötietojen käsittelyssä on noudatettava ensinnäkin yleisen tietosuoja-asetuksen 5 artiklassa esitettyjä tietojen laatua koskevia periaatteita Yksi periaatteista on, että henkilötietoja on ”käsiteltävä lainmukaisesti, asianmukaisesti ja [...] läpinäkyvästi”. Toiseksi käsittelyn lainmukaisuus edellyttää, että siinä noudatetaan jotakin tietojen käsittelyn laillisuutta koskevaa periaatetta, jotka luetellaan 6 artiklassa[341] muiden kuin arkaluonteisten henkilötietojen osalta ja 9 artiklassa erityisten tietoryhmien (tai arkaluonteisten henkilötietojen) osalta. Uudistetun yleissopimuksen 108 II luvussa, jossa esitetään henkilötietojen suojan perusperiaatteet, puolestaan

341 EUT, yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, *Rechnungshof vastaan Österreichischer Rundfunk ym. ja Christa Neukomm ja Joseph Lauermann vastaan Österreichischer Rundfunk*, 20.5.2003, 65 kohta; EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 16.12.2008, 48 kohta; EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011, 26 kohta.

säädetään, että tietojen käsittelyn lainmukaisuus edellyttää, että se on oikeassa suhteessa lainmukaiseen tavoitteeseen nähden.

Riippumatta siitä, mitä käsittelyn lainmukaista perustetta rekisterinpitäjä käyttää henkilötietojen käsittelytoimen käynnistämiseen, rekisterinpitäjän on sovellettava myös yleisessä tietosuojalainsäädännössä säädettyjä suojatoimia.

Suostumus

Euroopan neuvoston oikeudessa suostumus mainitaan uudistetun yleissopimuksen 108 5 artiklan 2 kohdassa. Se mainitaan myös Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä ja useissa Euroopan neuvoston suosituksissa[342]. **EU:n oikeudessa** suostumus on selkeästi vahvistettu henkilötietojen lainmukaisen käsittelyn perusteeksi yleisen tietosuoja-asetuksen 6 artiklassa, ja lisäksi se mainitaan yksiselitteisesti perusoikeuskirjan 8 artiklassa. Pätevän suostumuksen ominaisuudet selitetään yleisen tietosuoja-asetuksen 4 artiklassa olevassa suostumuksen määritelmässä. Pätevän suostumuksen saamista koskevat edellytykset puolestaan yksilöidään yleisen tietosuoja-asetuksen 7 artiklassa ja tietoyhteiskunnan palveluihin liittyvään lapsen suostumukseen sovellettavat ehdot 8 artiklassa.

Kuten 2.4 kohdassa selitetään, suostumuksen on oltava vapaaehtoinen, yksilöity, tietoinen ja yksiselitteinen. Suostumuksen on oltava lausuma tai selkeästi suostumusta ilmaiseva toimi, jolla henkilötietojen käsittely hyväksytään. Henkilöllä on myös oikeus peruuttaa suostumuksensa milloin tahansa. Rekisterinpitäjien on ylläpidettävä todennettavissa olevaa selostetta suostumuksesta.

Vapaaehtoinen suostumus

Euroopan neuvoston uudistetun yleissopimuksen 108 mukaan rekisteröidyn suostumuksen on oltava tietoiseen valintaan perustuva vapaaehtoinen tahdon ilmaisu[343]. Vapaaehtoinen suostumus on pätevä vain, ”jos rekisteröity pystyy tekemään aidon valinnan ilman pelottelun, harhaanjohtamisen tai pakottamisen riskiä ja ilman että hänelle aiheutuu merkittävää haittaa suostumuksen epäämisestä”[344]. **EU:n oikeu-**

342 Ks. esim. Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä, 23.11.2010, 3 artiklan 4 kohdan b alakohta.

343 Uudistettu yleissopimus 108, selitysmuistio, 42 kohta.

344 Ks. myös tietosuojatyöryhmä (2011), *lausunto 15/2011 suostumuksen määritelmästä*, WP 187, Bryssel, 13.7.2011, s. 13.

dessa säädetään tämän osalta, että suostumusta ei voida pitää vapaaehtoisesti annettuna, ”jos rekisteröidyllä ei ole todellista vapaan valinnan mahdollisuutta ja jos hän ei voi myöhemmin kieltäytyä suostumuksen antamisesta tai peruuttaa sitä ilman, että siitä aiheutuu hänelle haittaa”[345]. Yleisessä tietosuoja-asetuksessa korostetaan, että ”[a]rvioitaessa suostumuksen vapaaehtoisuutta on otettava mahdollisimman kattavasti huomioon muun muassa se, onko palvelun tarjoamisen tai muun sopimuksen täytäntöönpanon ehdoksi asetettu suostumus sellaisten henkilötietojen käsittelyyn, jotka eivät ole tarpeen kyseisen sopimuksen täytäntöönpanoa varten”[346]. Uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että rekisteröityyn ei saa yrittää vaikuttaa epäasianmukaisesti eikä häntä saa painostaa (taloudellisesti tai muutoin) suoraan tai välillisesti, eikä suostumusta pidä katsoa vapaaehtoisesti annetuksi, jos rekisteröidyllä ei ole todellista valinnan mahdollisuutta tai hän ei pysty kieltäytymään suostumuksen antamisesta tai peruuttamaan sitä ilman haitallisia seurauksia[347].

Esimerkki: Valtiossa A jotkin kunnat päättävät kehittää uusia henkilökortteja, joissa on upotettu siru. Elektronisten korttien hankinta ei ole pakollista asukkaille. Asukkaat, joilla ei ole korttia, eivät kuitenkaan pääse moniin tärkeisiin viranomaispalveluihin. He eivät esimerkiksi pysty maksamaan kunnallisveroja verkossa, jättämään verkossa valituksia, joihin viranomaisten on vastattava kolmessa päivässä, tai edes ohittamaan jonoja ja ostamaan alennuslippuja käydessään kunnan konserttisalissa, koska siihen on käytettävä sisäänkäynnin skannereita.

Tässä esimerkissä suostumusta ei voida käyttää kunnan tietojenkäsittelyn perustana. Koska asukkaita painostetaan vähintään välillisesti hankkimaan sähköinen kortti ja hyväksymään käsittely, suostumus ei ole vapaaehtoinen. Kuntien elektronisen korttijärjestelmän kehittämisen pitäisi näin ollen perustua muuhun käsittelyn oikeuttavaan lainmukaiseen perusteeseen. Ne voisivat esimerkiksi vedota siihen, että käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi, mikä on käsittelyn lainmukainen peruste yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan mukaisesti[348].

345 Yleinen tietosuoja-asetus, johdanto-osan 42 kappale.

346 *Ibid.*, 7 artiklan 4 kohta.

347 Uudistettu yleissopimus 108, selitysmuistio, 42 kohta.

348 Tietosuojatyöryhmä (2011), *lausunto 15/2011 suostumuksen määritelmästä*, WP187, Bryssel, 13.7.2011, s. 17. Lausunnon sivuilla 17 ja 21 on lisää esimerkkejä tapauksista, joissa tietojenkäsittely ei voi perustua suostumukseen, vaan käsittelyn oikeuttaminen edellyttää eri oikeudellista perustetta.

Suostumuksen vapaaehtoisuus voi olla kyseenalaista myös alaisuussuhteessa, kun suostumuksen tarvitsevan rekisterinpitäjän ja suostumuksen antavan rekisteröidyn välillä on merkittävä taloudellinen tai muu epätasapaino[349]. Tyypillinen esimerkki tällaisesta epätasapainosta ja alaisuussuhteesta on työnantajan suorittama henkilötietojen käsittely työsuhteen yhteydessä. Tietosuojatyöryhmän mukaan "[t]yöntekijät ovat tuskin koskaan sellaisessa asemassa, että he voivat vapaasti antaa, evätä tai peruuttaa suostumuksensa, kun otetaan huomioon työsuhteeseen liittyvä työntekijän riippuvuus työnantajasta. Tästä johtuvan vallan epätasapainon vuoksi työntekijät voivat antaa suostumuksensa vapaasti ainoastaan poikkeustilanteissa, joissa tarjouksen hyväksymisestä tai hylkäämisestä ei aiheudu minkäänlaisia seurauksia."[350]

Esimerkki: Suuri yritys haluaa luoda yksinomaan yrityksen sisäisen viestinnän parantamiseksi hakemiston, jossa on jokaisen työntekijän nimi, asema yrityksessä ja työosoite. Henkilöstöpäällikkö ehdottaa, että hakemistoon lisättäisiin esimerkiksi jokaisen työntekijän valokuva helpottamaan työtovereiden tunnistamista kokouksissa. Työntekijöiden edustajat vaativat, että tämä voitaisiin tehdä vain, jos työntekijä suostuu siihen.

Tässä tilanteessa työntekijän suostumusta tulisi pitää hakemistossa olevan valokuvan käsittelyn oikeudellisena perusteena, koska on selvää, ettei valokuvan julkaisemisella hakemistossa ole itsessään kielteisiä vaikutuksia, ja lisäksi voidaan olettaa, ettei työntekijälle aiheutuisi työnantajan taholta kielteisiä seurauksia, vaikka hän ei suostuisi valokuvansa julkaisemiseen hakemistossa.

Esimerkki: Yritys A suunnittelee kolmen työntekijänsä ja yrityksen B johtajien välistä tapaamista, jossa keskusteltaisiin mahdollisesta tulevasta yhteistyöstä eräässä hankkeessa. Tapaaminen järjestetään yrityksen B tiloissa. Yritys B pyytää yritystä A lähettämään sähköpostitse tapaamiseen osallistuvien nimet, ansioluettelot ja valokuvat. Yritys B sanoo tarvitsevansa osallistujien nimet ja valokuvat, jotta rakennuksen sisäänkäynnin turvallisuushenkilöstö voi tarkastaa osallistujien henkilöllisyyden, ja ansioluettelot, jotta johtajat voivat valmistautua tapaamiseen paremmin. Tässä tapauksessa yrityksen

349 Ks. myös tietosuojatyöryhmä (2001), *lausunto 8/2001 henkilötietojen käsittelystä työpaikoilla*, WP 48, Bryssel, 13.9.2001; tietosuojatyöryhmä (2005), valmisteluasiakirja 24. lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta, WP 114, Bryssel, 25.11.2005; tietosuojatyöryhmä (2017), *lausunto 2/2017 tietojenkäsittelystä työpaikalla*, WP 249, Bryssel, 8.6.2017.

350 Tietosuojatyöryhmä, *lausunto 2/2017 tietojenkäsittelystä työpaikalla*, WP 249, Bryssel, 8.6.2017.

A työntekijöiden henkilötietojen siirtäminen ei voi perustua suostumukseen. Suostumusta ei voida pitää ”vapaaehtoisena”, koska on mahdollista, että työntekijöille voi aiheutua tarjouksen hylkäämisestä kielteisiä seurauksia (heidät voidaan esimerkiksi vaihtaa toisiin työntekijöihin sekä tapaamisessa että yleisesti yhteydenpidossa yritykseen B ja hankkeeseen osallistumisessa). Käsittelyn on siksi perustuttava muuhun käsittelyn oikeuttavaan lainmukaiseen perusteeseen.

Tämä ei kuitenkaan tarkoita, että suostumus ei voi olla koskaan pätevä, jos sen antamatta jättämisestä aiheutuisi kielteisiä seurauksia. Esimerkiksi vaikka valintamyymälän kanta-asiakaskortista kieltäytyminen johtaisi siihen, ettei henkilö saa alennusta tietyistä tuotteista, suostumus on pätevä oikeudellinen peruste niiden asiakkaiden henkilötietojen käsittelylle, jotka ovat suostuneet hankkimaan kortin. Yrityksen ja asiakkaan välillä ei ole alistussuhdetta ja suostumuksen epäämisen seuraukset eivät ole niin vakavia, ettei rekisteröidyllä olisi vapautta valita (edellyttäen, että alennus on niin pieni, ettei se vaikuta vapaaehtoisuuteen).

Toisaalta, jos esimerkiksi välttämättömyyshyödykkeitä voi saada vain ja ainoastaan paljastamalla tietyt henkilötiedot sivullisille, rekisteröidyn suostumusta henkilötietojen käsittelyyn ei yleensä voida pitää vapaana päätöksenä, eikä se siten ole pätevä tietosuojasäännösten näkökulmasta[351]. Yleisessä tietosuoja-asetuksessa kielletään melko tiukasti suostumuksen asettaminen ehdoksi tavaroiden ja palvelujen tarjoamiselle[352].

Esimerkki: Matkustajien lentoyhtiölle antamaa suostumusta matkustajarekisterin tietojen, eli matkustajien henkilöllisyyttä, ruokailutottumuksia tai terveysongelmia koskevien tietojen, luovuttamiseen tietyn vieraan maan maahanmuuttoviranomaisille ei voida pitää tietosuojaoikeuden mukaan pätevänä suostumuksena, sillä matkustajilla ei ole vapautta valita, haluavatko he vierailla kyseisessä maassa. Jos nämä tiedot halutaan siirtää laillisesti, tarvitaan muu oikeudellinen peruste kuin suostumus – todennäköisesti erityinen laki.

351 Yleinen tietosuoja-asetus, 7 artiklan 4 kohta.

352 *Ibid.*

Tietoinen suostumus

Rekisteröidyllä on oltava riittävästi tietoa ennen päätöksen tekemistä. Yleensä tietoinen suostumus edellyttää tarkkaa ja helposti ymmärrettävää kuvausta asiasta, johon suostumus tarvitaan. Kuten tietosuojatyöryhmä selittää, suostumuksen on perustuttava tosiseikkojen ja sen toiminnan vaikutusten harkintaan ja ymmärtämiseen, jossa rekisteröity antaa suostumuksen käsittelylle. Näin ollen "[r]ekisteröidylle on annettava selkeässä ja ymmärrettävässä muodossa täsmälliset ja täydelliset tiedot kaikista asiaan liittyvistä kysymyksistä [...], kuten käsiteltävien tietojen luonteesta, käsittelyn tarkoituksista, tietojen mahdollisista vastaanottajista sekä rekisteröidyn oikeuksista"[353]. Rekisteröidyn on oltava tietoinen myös siitä, mitä seurauksia saattaa aiheutua siitä, että hän ei anna suostumustaan tietojensa käsittelyyn.

Koska tietoinen suostumus on tärkeä, yleisessä tietosuoja-asetuksessa ja uudistetun yleissopimuksen 108 selitysmuistiossa on pyritty selkeyttämään käsitettä. Yleisen tietosuoja-asetuksen johdanto-osan kappaleiden mukaan tietoinen suostumus tarkoittaa, että "rekisteröidyn olisi tiedettävä vähintään rekisterinpitäjän henkilöllisyys ja tarkoitukset, joita varten henkilötietoja on määrä käsitellä"[354].

Kun suostumusta käytetään erityistilanteessa poikkeuksena, jolla varmistetaan lainmukainen peruste kansainväliselle tiedonsiirrolle, suostumuksen päteväksi katsominen edellyttää, että rekisterinpitäjä ilmoittaa rekisteröidylle, että tällainen siirto voi aiheuttaa rekisteröidylle riskejä tietosuojan tason riittävyyttä koskevan päätöksen ja asianmukaisten suojatoimien puuttumisen vuoksi;[355]

Uudistetun yleissopimuksen 108 selitysmuistiossa täsmennetään, että rekisteröidyn päätöksen seurauksista on annettava tietoa, erityisesti suostumukseen sisältyvistä tosiseikoista ja suostumuksen laajuudesta[356].

Tietojen laatu on tärkeää. Tietojen laatu tarkoittaa, että tiedon antamisessa on käytettävä kieltä, jota ennakoitu vastaanottaja ymmärtää. Tiedot on annettavat selväkielisinä, käyttämättä ammattikieltä, helppotajuisina ja näkyvästi siten, että keskivertokäyttäjä ymmärtää ne[357]. Tietojen on oltava helposti rekisteröidyn saatavilla,

353 Tietosuojatyöryhmä (2007), valmisteluasiakirja potilastietojen käsittelystä sähköisissä potilastietokannoissa, WP 131, Bryssel, 15.2.2007.

354 Yleinen tietosuoja-asetus, johdanto-osan 42 kappale.

355 *Ibid.*, 49 artiklan 1 kohdan a alakohta.

356 Uudistettu yleissopimus 108, selitysmuistio, 42 kohta.

357 Tietosuojatyöryhmä (2011), *lausunto 15/2011 suostumuksen määritelmästä*, WP 187, Bryssel, 13.7.2011, s. 21.

ja ne voidaan antaa suullisesti tai kirjallisesti. Tietojen saatavuus ja näkyvyys ovat tärkeitä seikkoja: tietojen on oltava selvästi näkyvissä ja silmiinpistäviä. Sähköisessä ympäristössä tiedot voidaan esittää kerrostetusti siten, että rekisteröity pääsee lyhyestä tiedotteesta tutustumaan yksityiskohtaisempiin tietoihin.

Yksilöity suostumus

Jotta suostumus olisi pätevä, se on myös yksilöitävä käsittelytarkoituksen mukaan, ja tarkoitus on kuvattava selkeästi ja yksiselitteisesti. Tämä liittyy tiiviisti suostumuksen kohteesta annetun tiedon laatuun. Tässä on myös otettava huomioon tyypillisen rekisteröidyn kohtuulliset odotukset. Rekisteröidyltä on pyydettävä suostumus uudelleen, jos käsittelytoimia lisätään tai muutetaan tavalla, jota alkuperäisen suostumuksen antamisen yhteydessä ei voinut kohtuullisesti ennakoida ja jonka myötä tarkoitus muuttuu. Jos käsittelyllä on useita tarkoituksia, suostumus on annettava kaikkia käsittelytarkoituksia varten[358].

Esimerkkejä: Asiassa *Deutsche Telekom AG*[359] unionin tuomioistuin tarkasteli kysymystä siitä, tarvitsiko televerkko-operaattori, jonka oli luovutettava tilaajien henkilötietoja julkaistavaksi luetteloissa, rekisteröidyiltä uuden suostumuksen[360], sillä vastaanottajia ei ollut nimetty, kun alkuperäinen suostumus oli annettu.

Tuomioistuin katsoi, että sähköisen viestinnän tietosuojadirektiivin direktiivin 12 artiklan nojalla tietojen luovuttamista varten ei tarvittu uutta suostumusta. Koska rekisteröidyillä oli mahdollisuus suostua ainoastaan käsittelyn tarkoitukseen, joka oli heidän tietojensa julkaiseminen, he eivät voineet valita, missä luetteloissa tiedot julkaistaisiin.

Tuomioistuin korosti, että ”sähköisen viestinnän tietosuojadirektiivin 12 artiklan kontekstuaalisesta ja systemaattisesta tulkinnasta seuraa, että kyseisen artiklan 2 kohdassa tarkoitettu suostumus koskee tarkoitusta, jota varten henkilötiedot julkaistaan julkisessa luettelossa, eikä tiettyä luettelon

358 Yleinen tietosuoja-asetus, johdanto-osan 32 kappale.

359 EUT, C-543/09, *Deutsche Telekom AG vastaan Bundesrepublik Deutschland*, 5.5.2011. Ks. erityisesti 53 ja 54 kohta.

360 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, EYVL L 201, 31.7.2002, s. 37 (sähköisen viestinnän tietosuojadirektiivi).

tarjoajaa”[361]. Lisäksi ”juuri henkilötietojen julkaiseminen luettelossa, jolla on erityinen tarkoitus, voi osoittautua tilaajalle haitalliseksi”[362], eikä olennaista ole se, kuka tiedot julkaisee.

Asiassa *Tele2 (Netherlands) BV, Ziggo BV, Vodafone Libertel BV vastaan Autoriteit Consument en Markt (AMC)*[363] oli kyse siitä, että belgialainen numerotiedotus- ja puhelinluettelopalveluja tarjoava yhtiö pyysi puhelinnumeroita Alankomaissa tilaajien käyttöön antavia yrityksiä luovuttamaan sille niiden tilaajia koskevia tietoja. Belgialainen yhtiö vetosi yleispalveludirektiivin mukaiseen velvoitteeseen[364]. Direktiivissä vaaditaan, että puhelinnumeroita jakavien yhtiöiden on asetettava numeroita koskevat tiedot niitä pyytävien hakemistojen saataville, jos tilaajat ovat antaneet suostumuksensa numeroidensa julkaisemiseen. Alankomaalaiset yritykset kieltäytyivät siitä, koska niiden mukaan kyseessä olevia tietoja ei tarvinnut antaa toiseen jäsenvaltioon sijoittautuneelle yritykselle. Ne väittivät, että käyttäjien antama suostumus numeroidensa julkaisuun koski sitä, että numerot julkaistaisiin alankomaalaisessa hakemistossa. Euroopan unionin tuomioistuin totesi, että yleispalveludirektiivi kattaa kaikki hakemistopalveluyritysten pyynnöt riippumatta siitä, mihin jäsenvaltioon ne ovat sijoittautuneet. Tuomioistuin totesi lisäksi, että samojen tietojen luovuttaminen toiselle yritykselle, joka aikoo julkaista julkisen luettelon, ilman että kyseinen tilaaja on antanut uutta suostumusta, ei loukkaa henkilötietojen suojaa koskevan oikeuden keskeistä sisältöä[365]. Näin ollen tilaajille puhelinnumeroita antavalla yrityksellä ei ole velvollisuutta muotoilla tilaajalle esitettävää suostumuspyyntöä siten, että tilaaja ilmaisee suostumuksensa erikseen sen mukaan, mihin jäsenvaltioon häntä koskevat tiedot voidaan luovuttaa[366].

361 EUT, C-543/09, *Deutsche Telekom AG vastaan Bundesrepublik Deutschland*, 5.5.2011, 61 kohta.

362 *Ibid.*, 62 kohta.

363 EUT, C-536/15, *Tele2 (Netherlands) BV ym. vastaan Autoriteit Consument en Markt (AMC)*, 15.3.2017.

364 Euroopan parlamentin ja neuvoston direktiivi 2002/22/EY, annettu 7 päivänä maaliskuuta 2002, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla (yleispalveludirektiivi), EUVL 2002, L 108, s. 51, sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston 25 päivänä marraskuuta 2009 annetulla direktiivillä 2009/136/EY (yleispalveludirektiivi), EUVL 2009, L 337, s. 11.

365 EUT, C-536/15, *Tele2 (Netherlands) BV ym. vastaan Autoriteit Consument en Markt (AMC)*, 15.3.2017, 36 kohta.

366 *Ibid.*, 40–41 kohta.

Yksiselitteinen suostumus

Suostumus on annettava yksiselitteisesti[367]. Se tarkoittaa, että ei pitäisi olla perusteltua syytä epäillä sitä, että rekisteröity haluaa ilmaista hyväksyvänsä tietojensa käsittelyn. Esimerkiksi jonkin toimen toteuttamatta jättäminen ei merkitse yksiselitteistä suostumusta.

Tästä olisi kyse silloin, kun rekisterinpitäjä hankkii tietosuojaselosteessaan suostumuksen esimerkiksi lausumalla ”palvelun käyttöä jatkamalla annat suostumuksen henkilötietojesi käsittelyyn”. Siinä tapauksessa rekisterinpitäjien on ehkä varmistettava, että käyttäjät antavat manuaalisesti ja yksittäin suostumuksen kyseisessä selosteessa.

Jos suostumus annetaan sopimuksen osana kirjallisesti, henkilötietojen käsittelyä koskevan suostumuksen olisi oltava yksilöllinen ja joka tapauksessa ”olisi varmistettava suojatoimin, että rekisteröity on tietoinen antamastaan suostumuksesta ja siitä, kuinka pitkälle menevästä suostumuksesta on kyse”[368].

Lapsia koskevat suostumusvaatimukset

Yleisessä tietosuoja-asetuksessa säädetään lasten erityisestä suojelusta tietoyhteiskunnan palvelujen tarjoamisessa, koska ”he eivät välttämättä ole kovin hyvin perillä henkilötietojen käsittelyyn liittyvistä riskeistä, seurauksista, asianomaisista suojatoimista tai omista oikeuksistaan”[369]. Kun siis tietoyhteiskunnan palvelujen tarjoajat käsittelevät alle 16-vuotiaiden lasten tietoja suostumuksen perusteella, **EU:n oikeuden** mukaan tällainen käsittely on lainmukaista ”vain siinä tapauksessa ja siltä osin kuin lapsen vanhempainvastuunkantaja on antanut siihen suostumuksen tai valtuutuksen”[370]. Jäsenvaltiot voivat lainsäädännössään säätää tätä tarkoitusta koskevasta alemmasta iästä, joka ei saa olla alle 13 vuotta[371]. Vanhempainvastuunkantajan suostumus ei ole tarpeen ”tarjottaessa ennalta ehkäiseviä palveluja tai neuvontapalveluja suoraan lapselle”[372]. Kaikessa lapsiin kohdistuvaa tietojenkäsittelyä kos-

367 Yleinen tietosuoja-asetus, 4 artiklan 11 kohta.

368 *Ibid.*, johdanto-osan 42 kappale.

369 *Ibid.*, johdanto-osan 38 kappale.

370 *Ibid.* 8 artiklan 1 kohdan ensimmäinen alakohta. Tietoyhteiskunnan palvelut määritellään yleisen tietosuoja-asetuksen 4 artiklan 25 kohdassa.

371 Yleinen tietosuoja-asetus, 8 artiklan 1 kohdan toinen alakohta.

372 *Ibid.*, johdanto-osan 38 kappale.

kevassa tiedotuksessa ja viestinnässä on käytettävä niin selkeää ja yksinkertaista kieltä, että lapsen on helppo ymmärtää sitä[373].

Oikeus peruuttaa suostumus milloin tahansa

Yleiseen tietosuoja-asetukseen sisältyy yleinen oikeus peruuttaa suostumus milloin tahansa[374]. Rekisteröidylle on ilmoitettava tästä oikeudesta ennen suostumuksen antamista, ja hän voi käyttää oikeutta harkintansa mukaan. Perumiselle ei saisi vaatia perusteluja eikä sillä saisi olla muita kielteisiä seurauksia kuin niiden etujen päättyminen, joihin aiempi tietojen käytön hyväksyminen on oikeuttanut. Suostumuksen peruuttamisen on oltava yhtä helppoa kuin sen antaminen[375]. Suostumusta ei voida pitää vapaaehtoisesti annettuna, jos rekisteröity ei voi myöhemmin peruuttaa suostumustaan ilman, että siitä aiheutuu hänelle haittaa, tai jos suostumuksen peruuttaminen ei ole yhtä helppoa kuin sen antaminen[376].

Esimerkki: Asiakas suostuu vastaanottamaan mainospostia osoitteeseen, jonka hän antaa rekisterinpitäjälle. Jos asiakas peruu suostumuksensa, rekisterinpitäjän on välittömästi lopetettava mainospostin lähettäminen. Asiakkaalle ei saa määrätä mitään rangaistusta, kuten sakkoa. Peruuttaminen koskee kuitenkin tulevaisuutta eikä se vaikuta takautuvasti. Jakso, jonka aikana asiakkaan henkilötietoja käsiteltiin lainmukaisesti – asiakkaan suostumuksen perusteella – on ollut oikeutettua. Peruuttaminen estää kyseisten tietojen kaiken tulevan käsittelyn, ellei käsittely ole tietojen poistamista koskevan oikeuden mukaista[377].

Sopimuksen täytäntöönpanon tarve

EU:n oikeudessa yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan b alakohdassa säädetään toisesta lainmukaisen käsittelyn edellytyksestä eli siitä, että käsittely ”on tarpeen sellaisen sopimuksen täytäntöön panemiseksi, jossa rekisteröity on osapuolena”. Tämä säännös kattaa myös sopimusta edeltävät suhteet. Otetaan

373 *Ibid.*, johdanto-osan 58 kappale. Ks. myös uudistettu yleissopimus 108, 15 artiklan 2 kohdan e alakohta. Uudistettu yleissopimus 108, selitysmuistio, 68 ja 125 kohta.

374 Yleinen tietosuoja-asetus, 7 artiklan 3 kohta. Uudistettu yleissopimus 108, selitysmuistio, 45 kohta.

375 Yleinen tietosuoja-asetus, 7 artiklan 3 kohta.

376 Yleinen tietosuoja-asetus, johdanto-osan 42 kappale; uudistettu yleissopimus 108, selitysmuistio, 42 kohta.

377 Yleinen tietosuoja-asetus, 17 artiklan 1 kohdan b alakohta.

esimerkiksi tilanne, jossa osapuoli aikoo tehdä sopimuksen, muttei ole vielä tehnyt sitä, mahdollisesti siksi, että hän haluaa vielä tarkistaa joitakin asioita. Jos yhden osapuolen on käsiteltävä tietoja tätä tarkoitusta varten, käsittely on lainmukaista, kunhan se on tarpeen ”sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä”[378].

Uudistetun yleissopimuksen 108 5 artiklan 2 kohdan määritelmä tietojenkäsittelyn laissa säädetystä oikeusperustasta käsittää myös tietojenkäsittelyn sellaisen sopimuksen täytäntöön panemiseksi (tai sopimuksen tekemistä edeltävien toimenpiteiden toteuttamiseksi rekisteröidyn pyynnöstä), jonka osapuoli rekisteröity on[379].

Rekisterinpitäjän lakisääteiset velvoitteet

EU:n oikeuden mukaan toinen peruste, jolla henkilötietojen käsittely voi olla laillista, on, että ”käsittely on tarpeen rekisterinpitäjän lakisääteisen velvoitteen noudattamiseksi” (yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan c alakohta). Tämä säännös koskee sekä yksityisellä että julkisella sektorilla toimivia rekisterinpitäjiä. Julkisen sektorin rekisterinpitäjien oikeudelliset velvoitteet voivat kuulua myös yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdan soveltamisalaan. Yksityisellä sektorilla toimivilla rekisterinpitäjillä on monissa tilanteissa lakisääteinen velvollisuus käsitellä henkilötietoja. Työnantajien on esimerkiksi käsiteltävä työntekijöidensä henkilötietoja sosiaaliturvaan ja verotukseen liittyvistä syistä, ja yritysten on käsiteltävä asiakkaidensa henkilötietoja verotusta varten.

Lakisääteinen velvoite voi perustua unionin oikeuteen tai jäsenvaltioiden lainsäädäntöön, ja ne voivat olla yhden tai usean käsittelytoimen perustana. Oikeudessa tai lainsäädännössä olisi määriteltävä käsittelyn tarkoitus, täsmennettävä tarkat vaatimukset, joilla määritetään rekisterinpitäjä, käsiteltävien henkilötietojen tyyppi, asianomaiset rekisteröidyt, yhteisöt, joille henkilötietoja voidaan luovuttaa, tarkoituksen rajoitukset, säilyttämisaika ja muut toimenpiteet, joilla varmistetaan laillinen ja asianmukainen käsittely.[380] Kaiken henkilötietojen käsittelyn perustana olevan lainsäädännön on noudatettava sekä perusoikeuskirjan 7 ja 8 artiklaa että ihmisoikeussopimuksen 8 artiklaa.

378 *Ibid.*, 6 artiklan 1 kohta.

379 Uudistettu yleissopimus 108, selitysmuistio, 46 kohta; Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä, 23.11.2010, 3 artiklan 4 kohdan b alakohta.

380 Yleinen tietosuoja-asetus, johdanto-osan 45 kappale.

Rekisterinpitäjän oikeudelliset velvoitteet toimivat myös **Euroopan neuvoston oikeudessa** perusteena henkilötietojen lainmukaiselle käsittelylle[381]. Kuten edellä on todettu, yksityisellä sektorilla toimivan rekisterinpitäjän lailliset velvoitteet ovat vain yksi Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa tarkoitetuista muiden henkilöiden oikeutetuista eduista. Edellä esitetty esimerkki työntekijöidensä henkilötietoja käsittelevistä työnantajista pätee näin ollen myös Euroopan neuvoston oikeudessa.

Rekisteröidyn tai toisen luonnollisen henkilön elintärkeät edut

EU:n oikeudessa yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan d alakohdassa säädetään, että henkilötietojen käsittely on lainmukaista, jos se ”on tarpeen rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi”. Henkilötietoja voidaan käsitellä toisen luonnollisen henkilön elintärkeän edun perusteella ainoastaan silloin, kun ”käsittelyllä ei ole muuta ilmeistä käsittelyn oikeusperustetta”[382]. Joskus tietty käsittely voi perustua sekä yleistä etua että rekisteröidyn tai toisen luonnollisen henkilön elintärkeitä etuja koskeviin syihin. Tästä on kyse esimerkiksi epidemioiden ja niiden leviämisen seuraamisessa tai humanitaarisissa hätätilanteissa.

Euroopan neuvoston oikeudessa rekisteröidyn elintärkeitä etuja ei mainita ihmisoikeussopimuksen 8 artiklassa. Rekisteröidyn elintärkeiden etujen katsotaan kuitenkin kuuluvan uudistetun yleissopimuksen 108 5 artiklan 2 kohdan määritelmään oikeusperustasta, joka koskee henkilötietojen käsittelyn lainmukaisuutta[383].

Yleinen etu ja julkisen vallan käyttäminen

Koska yhteiskunnallisten asioiden järjestämiseen on monia tapoja, yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan e alakohdassa säädetään, että henkilötietojen käsittely on lainmukaista, jos se ”on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämiseksi”[384].

381 Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä, 23.11.2010, 3 artiklan 4 kohdan a alakohta.

382 Yleinen tietosuoja-asetus, johdanto-osan 46 kappale.

383 Uudistettu yleissopimus 108, selitysmuistio, 46 kohta.

384 Ks. yleinen tietosuoja-asetus, johdanto-osan 45 kappale.

Esimerkki: Asiassa *Huber vastaan Bundesrepublik Deutschland*[385] Saksassa asuva Itävallan kansalainen Heinz Huber pyysi liittotasavallan siirtolais- ja pakolaisvirastoa poistamaan häntä koskevat tiedot ulkomaalaisista pidettävästä keskusrekisteristä (AZR:stä). Tätä rekisteriä, jossa ovat niiden muiden kuin saksalaisten EU:n kansalaisten henkilötiedot, jotka oleskelevat Saksassa yli kolmen kuukauden ajan, käytetään tilastollisiin tarkoituksiin ja silloin, kun lainvalvontaviranomaiset ja oikeusviranomaiset tutkivat rikollisia toimia tai yleisen turvallisuuden vaarantavaa toimintaa syytteen nostamista varten. Ennakkoratkaisua pyytänyt tuomioistuin kysyi, oliko EU:n lainsäädännön mukaista käsitellä henkilötietoja, jotka oli kerätty sellaiseen ulkomaalaisista pidettävän keskusrekisterin kaltaiseen rekisteriin, johon muillakin viranomaisilla oli pääsy, kun tällaista rekisteriä ei pidetty Saksan kansalaisista.

Tuomioistuin katsoi ensinnäkin, että direktiivin 95/46/EY[386] 7 artiklan e alakohdan nojalla henkilötietoja voidaan käsitellä laillisesti vain, jos se on tarpeen yleistä etua koskevan tehtävän suorittamiseksi tai julkisen vallan käyttämiseksi.

Tuomioistuin totesi seuraavaa: ”Kun otetaan huomioon tavoite taata vastaavantasoinen suoja kaikissa jäsenvaltioissa, direktiivin 95/46[387] 7 artiklan e alakohdan mukainen tarpeellisuuden käsite [...] ei näin ollen voi olla sisällöltään erilainen eri jäsenvaltioissa. Tämän vuoksi kyse on yhteisön oikeuden itsenäisestä käsitteestä, jota on tulkittava siten, että se vastaa täysimääräisesti tämän direktiivin tavoitetta, joka on määritelty sen 1 artiklan 1 kohdassa”.[388]

Tuomioistuin toi esiin, että unionin kansalaisen oikeus oleskella vapaasti sellaisen jäsenvaltion alueella, jonka kansalainen hän ei ole, ei ole ehdoton vaan siihen voi liittyä perustamissopimuksessa määrättyjä ja sen soveltamisesta annetuissa säännöksissä säädettyjä rajoituksia ja ehtoja. Näin ollen vaikka jäsenvaltiolla on periaatteessa oikeus tarjota AZR:n kaltainen rekisteri oleskeluoikeutta koskevan lainsäädännön soveltamisesta vastaavien viranomaisten tueksi, tällainen rekisteri ei voi sisältää muita tietoja kuin ne,

385 EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 16.12.2008.

386 Entinen tietosuojadirektiivi, 7 artiklan 1 kohdan e alakohta, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan e alakohta.

387 *Ibid.*

388 EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 16.12.2008, 52 kohta.

jotka ovat tarpeen tähän tarkoitukseen. Tuomioistuin totesi, että tällainen henkilötietojen käsittelyjärjestelmä on EU:n lainsäädännön mukainen, jos se sisältää yksinomaan tiedot, jotka ovat tarpeen tämän lainsäädännön soveltamiseksi, ja jos sen keskitetyn luonteen avulla tätä lainsäädäntöä voidaan soveltaa tehokkaammin. Kansallisen tuomioistuimen oli kyseisessä tapauksessa varmistettava, täyttyivätkö mainitut ehdot. Jos ehdot eivät täyttyneet, henkilötietojen säilyttämistä ja käsittelyä AZR:n kaltaisen rekisterin puitteissa tilastollisiin tarkoituksiin ei voitu mitenkään pitää direktiivin 95/46/EY 7 artiklan e alakohdassa[389] tarkoitetulla tavalla tarpeellisena.[390]

Kysymykseen rekisterin sisältämien tietojen käytöstä rikollisuuden torjunnassa tuomioistuin vastasi, että tähän tavoitteeseen ”kuuluu väistämättä syytteiden nostaminen tehdyistä rikoksista ja rikkomuksista tekijöiden kansalaisuudesta riippumatta”. Kiistanalainen rekisteri ei sisältänyt asianomaisen jäsenvaltion kansalaisten henkilötietoja, ja tällainen eriarvoinen kohtelu oli SEUT-sopimuksen 18 artiklassa kiellettyä syrjintää. Näin ollen kyseistä määräystä oli tuomioistuimen mukaan tulkittava siten, että sen ”vastaista on se, että jäsenvaltio ottaa rikollisuuden torjumiseksi käyttöön henkilötietojen käsittelyjärjestelmän, joka koskee ainoastaan unionin kansalaisia, jotka eivät ole tämän jäsenvaltion kansalaisia”[391].

Henkilötietojen käyttöön viranomaisten julkisissa tehtävissä sovelletaan myös **ihmisoikeussopimuksen** 8 artiklaa, ja uudistetun yleissopimuksen 108 5 artiklan 2 kohdan on määrä kattaa se soveltuvin osin[392].

Rekisterinpitäjän tai kolmannen osapuolen oikeutetut edut

EU:n oikeuden mukaan rekisteröity ei ole ainoa, jolla on oikeutettuja etuja. Yleisen tietosuoja-asetuksen 6 artiklan 1 kohdan f alakohdassa säädetään, että henkilötietoja voidaan käsitellä lainmukaisesti, jos käsittely ”on tarpeen rekisterinpitäjän tai kolmannen osapuolen oikeutettujen etujen toteuttamiseksi [lukuun ottamatta tietojenkäsittelyä, jota viranomaiset suorittavat tehtäviensä yhteydessä], paitsi milloin

389 Entinen tietosuojadirektiivi, 7 artiklan e alakohta, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan e alakohta

390 EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 16.12.2008, 54, 58–59 ja 66–68 kohta.

391 *Ibid.*, 78 ja 81 kohta.

392 Uudistettu yleissopimus 108, selitysmuistio, 46 ja 47 kohta.

henkilötietojen suojaa edellyttävät rekisteröidyn edut tai perusoikeudet ja -vapaudet syrjäyttävät tällaiset edut [...]"[393].

Oikeutetun edun olemassaoloa on arvioitava huolellisesti jokaisessa yksittäistapauksessa[394]. Jos rekisterinpitäjällä todetaan olevan oikeutettuja etuja, on tehtävä puntarointia kyseisten etujen ja rekisteröidyn etujen tai perusoikeuksien ja -vapauksien välillä[395]. Tässä punninnassa on otettava huomioon rekisteröidyn kohtuulliset odotukset, jotta voidaan selvittää, syrjäyttävätkö rekisterinpitäjän edut rekisteröidyn edut tai perusoikeudet[396]. Jos rekisteröidyn oikeudet syrjäyttävät rekisterinpitäjän oikeutetut edut, rekisterinpitäjä voi ryhtyä toimenpiteisiin ja toteuttaa suojatoimia (esim. käyttää peitenimiä eli pseudonymisoida tietoja), joilla varmistetaan, että vaikutus rekisteröidyn oikeuksiin on mahdollisimman pieni, ja kääntää tasapainon, jotta tätä käsittelyn oikeutettua perustaa voidaan käyttää lainmukaisesti. Tietosuojatyöryhmä korosti rekisterinpitäjän oikeutetun edun käsitteestä antamassaan lausunnossa tilivelvollisuuden ja avoimuuden ratkaisevan tärkeää asemaa rekisterinpitäjän oikeutettujen etujen ja rekisteröidyn perusoikeuksia koskevien oikeutettujen etujen punninnassa. Siinä ovat tärkeitä myös rekisteröidyn oikeudet vastustaa tietojensa käsittelyä tai käyttää, muuttaa, poistaa tai siirtää omia tietojaan.[397]

Yleisen tietosuoja-asetuksen johdanto-osan kappaleissa annetaan esimerkkejä siitä, mitä rekisterinpitäjän oikeutetut edut voivat olla. Henkilötietojen käsittely on esimerkiksi sallittu ilman rekisteröidyn suostumusta, kun se tehdään suoramarkkinointitarkoituksissa tai kun käsittely on ehdottoman välttämätöntä "petosten estämistarkoituksissa"[398].

Euroopan unionin tuomioistuin on oikeuskäytännössään laajentanut testiä oikeutetun edun määrittelemiseksi.

393 Direktiiviin 95/46/EY verrattuna yleisessä tietosuoja-asetuksessa annetaan enemmän esimerkkejä tapauksista, joiden katsotaan muodostavan oikeutetun edun.

394 Yleinen tietosuoja-asetus, johdanto-osan 47 kappale.

395 Tietosuojatyöryhmä (2014), *lausunto 6/2014 direktiivin 95/46/EY 7 artiklan mukaisesta rekisterinpitäjän oikeutetun intressin käsitteestä*, WP 217, 4.4.2014.

396 *Ibid.*

397 *Ibid.*

398 Yleinen tietosuoja-asetus, johdanto-osan 47 kappale.

Esimerkki: Asiassa *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] oli kyse siitä, että Riian liikenneyhtiön (Rīgas satiksme) johdinauto vahingoittui, kun taksimatkustaja avasi äkkiä taksin oven. Rīgas satiksme halusi haastaa matkustajan oikeuteen vahinkojen korvaamisesta. Poliisi antoi kuitenkin vain matkustajan nimen ja kieltäytyi antamasta matkustajan henkilötunnusta ja osoitetta, koska sen mukaan tietojen luovuttaminen olisi kansallisten tietosuojalakien vastaista.

Ennakkoratkaisua pyytänyt latvialainen tuomioistuin pyysi Euroopan unionin tuomioistuinta tekemään ennakkoratkaisun siitä, asetetaanko EU:n tietosuojalainsäädännössä velvollisuus luovuttaa kaikki henkilötiedot, joita tarvitaan nostamaan siviilioikeudellinen kanne sellaista henkilöä vastaan, jonka väitetään olevan vastuussa hallinnollisesta rikkomuksesta[400].

Euroopan unionin tuomioistuin totesi, että EU:n tietosuojalainsäädäntöön sisältyy mahdollisuus – ei velvollisuutta – tietojen luovuttamiseen kolmannelle osapuolelle kyseisen osapuolen oikeutetun intressin toteuttamiseksi[401]. Tuomioistuin esitti kolme kumulatiivista edellytystä, joiden on täytyttävä, jotta henkilötietojen käsittely on lainmukaista ”oikeutetun intressin” perusteella[402]. Ensinnäkin kolmannella osapuolella, jolle tiedot luovutetaan, on oltava oikeutettu intressi. Tässä nimenomaisessa tapauksessa se tarkoittaa, että henkilötietojen pyytäminen omaisuusvahinkoja aiheuttaneen henkilön haastamiseksi oikeuteen on kolmannen osapuolen oikeutettu intressi. Toiseksi henkilötietojen käsittelyn on oltava tarpeen oikeutetun intressin toteuttamiseksi. Tässä tapauksessa henkilötietojen, kuten osoitteen ja/tai henkilötunnuksen saaminen on ehdottoman välttämätöntä henkilön tunnistamiseksi. Kolmanneksi rekisteröidyn perusoikeudet ja -vapaudet eivät saa syrjäyttää rekisterinpitäjän tai kolmansien osapuolten oikeutettua intressiä. Intressien vertailu on tehtävä tapauskohtaisesti, ja siinä on otettava huomioon rekisteröidyn perusoikeuksiin kohdistuvan loukkauksen vakavuus ja jopa rekisteröidyn ikä tietyissä olosuhteissa. Tässä nimenomaisessa asiassa

399 EUT, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vastaan Rīgas pašvaldības SIA ”Rīgas satiksme”*, 4.5.2017.

400 *Ibid.*, 23 kohta.

401 *Ibid.*, 26 kohta.

402 *Ibid.*, 28–34 kohta.

Euroopan unionin tuomioistuin kuitenkin katsoi, ettei ole perusteltua kieltäytyä henkilötietojen luovuttamisesta vain sen vuoksi, että rekisteröity oli alaikäinen.

Asiassa *ASNEF ja FECEMD* antamassaan tuomiossa Euroopan unionin tuomioistuin otti yksiselitteisesti kantaa tuolloin direktiivin 7 artiklan f alakohdassa vahvistettuun henkilötietojen käsittelyyn, jonka lainmukaisena perustana ovat ”oikeutetut edut”[403].

Esimerkki: Asiassa *ASNEF ja FECEMD*[404] Euroopan unionin tuomioistuin selvensi, että kansallisessa lainsäädännössä ei saa asettaa henkilötietojen lailliselle käsittelylle muita edellytyksiä kuin ne, jotka mainitaan direktiivin 7 artiklan f alakohdassa[405]. Käsiteltävänä olleessa tilanteessa Espanjan tietosuojalainsäädäntö sisälsi säännöksen, jonka mukaan sivulliset saattoivat vedota oikeutettuun etuunsa henkilötietojen käsittelyssä vain, jos tiedot olivat jo yleisön saatavilla olevissa lähteissä.

Tuomioistuin toi ensin esiin, että direktiivillä 95/46/EY[406] pyritään saattamaan henkilöiden oikeuksien ja vapauksien suoja henkilötietojen käsittelyssä samalle tasolle kaikissa jäsenvaltioissa. Alalla sovellettavien kansallisten lainsäädäntöjen lähentäminen ei saa johtaa lainsäädännöllä turvattavan tietosuojan heikentymiseen. Sillä on päinvastoin varmistettava tietosuojan korkea taso unionissa[407]. Näin ollen EUT totesi, että ”tavoitteesta taata kaikissa jäsenvaltioissa suojan saattaminen samalle tasolle johtuu siten, että direktiivin 95/46 7 artiklaan[408] on otettu tyhjentävä luettelo, johon on rajattu tilanteet, joissa henkilötietojen käsittelyn voidaan katsoa olevan laillista”.

403 Entinen tietosuojadirektiivi, 7 artiklan f alakohta, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan f alakohta.

404 EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011.

405 Entinen tietosuojadirektiivi, 7 artiklan f alakohta, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan f alakohta.

406 Entinen tietosuojadirektiivi, nyt yleinen tietosuoja-asetus.

407 EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011, 28 kohta. Ks. yleinen tietosuoja-asetus, johdanto-osan 8 ja 10 kappaleet.

408 Entinen tietosuojadirektiivi, 7 artikla, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan f alakohta.

Lisäksi ”jäsenvaltiot eivät voi lisätä direktiivin 95/46 7 artiklaan[409] uusia henkilötietojen käsittelyn laillistamista koskevia periaatteita eivätkä säätää lisävaatimuksista, joilla muutettaisiin jonkin niiden kuuden periaatteen ulottuvuutta, joista tässä artiklassa on säädetty”[410]. Tuomioistuin myönsi, että ”direktiivin 95/46 7 artiklan f alakohdan edellyttämää punnitsemista varten voidaan ottaa huomioon se, että rekisteröidyn perusoikeuksiin häntä koskevien tietojen käsittelyn vuoksi kohdistuvan loukkauksen vakavuus voi vaihdella sen mukaan, ovatko kyseessä olevat tiedot mahdollisesti jo yleisön saatavilla olevassa lähteessä”.

Se kuitenkin jatkoi toteamalla, että ”direktiivin 95/46 7 artiklan f alakohta on esteenä sille, että jäsenvaltio sulkee ehdottomasti ja yleisesti pois mahdollisuuden käsitellä tiettyihin tietoryhmiin kuuluvia henkilötietoja sallimatta niiden oikeuksien ja intressien punnitsemista, joista on kyse tietyssä yksittäisessä tapauksessa”.

Näiden näkökohtien perusteella tuomioistuin päätyi siihen johtopäätökseen, että ”direktiivin 95/46 7 artiklan f alakohtaa[411] on tulkittava siten, että se on esteenä kansalliselle lainsäädännölle, jonka mukaan silloin, kun rekisteröidyn suostumusta ei ole saatu, henkilötietojen käsittely, joka on tarpeen rekisterinpitäjän tai sivullisen, jolle tiedot on luovutettu, oikeutettujen intressien toteuttamiseksi, edellyttää rekisteröidyn perusoikeuksien ja vapauksien kunnioittamisen lisäksi sitä, että henkilötiedot ovat yleisön saatavilla olevissa lähteissä, ja jolla suljetaan näin ehdottomasti ja yleisesti pois mahdollisuus käsitellä tietoja, jotka eivät ole tällaisissa yleisön saatavilla olevissa lähteissä”[412].

Aina kun henkilötietoja käsitellään ”oikeutettujen etujen” perusteella, henkilöllä on yleisen tietosuoja-asetuksen 21 artiklan 1 kohdan mukaisesti oikeus milloin tahansa vastustaa käsittelyä erityiseen tilanteeseensa liittyvällä perusteella. Rekisterinpitäjän on lopetettava käsittely, paitsi jos se voi osoittaa, että käsittelyyn on olemassa huomattavan tärkeä ja perusteltu syy.

409 Entinen tietosuojadirektiivi, 7 artikla, nyt yleinen tietosuoja-asetus, 6 artikla.

410 *Ibid.*

411 Entinen tietosuojadirektiivi, 7 artiklan f alakohta, nyt yleinen tietosuoja-asetus, 6 artiklan 1 kohdan f alakohta.

412 EUT, yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011, 40, 44 ja 48–49 kohta.

Euroopan neuvoston oikeudessa esitetään samansuuntaisia päätelmiä uudistetussa yleissopimuksessa 108[413] ja Euroopan neuvoston suosituksissa. Profilointia koskevassa suosituksessa katsotaan, että henkilötietojen käsittely profilointia varten on laillista, jos se on välttämätöntä muiden henkilöiden oikeutettujen etujen suojaamiseksi paitsi silloin, kun rekisteröityjen perusoikeudet ja -vapaudet on asetettava näiden etujen edelle[414]. Lisäksi Euroopan ihmisoikeussopimuksen 8 artiklan 2 kohdassa muiden henkilöiden oikeuksien ja vapauksien turvaaminen mainitaan lainmukaiseksi syyksi rajoittaa oikeutta tietosuojaan.

Esimerkki: Asiassa *Y v. Turkki*[415] kantaja oli HIV-positiivinen. Koska hän oli tiedoton, kun hänet tuotiin sairaalaan, ambulanssin työntekijät kertoivat sairaalan henkilökunnalle hänen olevan HIV-positiivinen. Kantaja esitti Euroopan ihmisoikeustuomioistuimelle, että näiden tietojen luovuttaminen oli loukannut hänen oikeuttaan yksityiselämään. Tietojen jakamisen ei kuitenkaan katsottu loukanneen hänen oikeuksiaan, koska sairaalan henkilöstön turvallisuutta piti suojata.

4.1.2 Erityisten henkilötietoryhmien (arkaluonteisten tietojen) käsittely

Euroopan neuvoston oikeudessa asianmukaisen suojan vahvistaminen arkaluonteisten henkilötietojen käytölle on jätetty kansallisen lainsäädännön asiaksi edellyttäen, että uudistetun yleissopimuksen 108 6 artiklan ehdot täyttyvät eli että yleissopimuksen muita säännöksiä täydentävät asianmukaiset suojatoimet vahvistetaan lainsäädännössä. **EU:n oikeudessa** yleisen tietosuoja-asetuksen 9 artiklassa on yksityiskohtainen järjestelmä erityisiä henkilötietoryhmiä (joita sanotaan myös arkaluonteisiksi tiedoiksi) koskevalle käsittelylle. Näistä tiedoista ilmenee rotu tai etninen alkuperä, poliittisia mielipiteitä, uskonnollinen tai filosofinen vakaumus tai ammattiliiton jäsenyys. Tähän kuuluvat myös geneettisten tai biometristen tietojen käsittely henkilön yksiselitteistä tunnistamista varten tai terveyttä koskevien tietojen taikka luonnollisen henkilön seksuaalista käyttäytymistä ja suuntautumista

413 Uudistettu yleissopimus 108, selitysmuistio, 46 kohta.

414 Euroopan neuvosto, ministerikomitea (2010), suositus CM/Rec(2010)13 ja selitysmuistio yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä, 23.11.2010, 3 artiklan 4 kohdan b alakohta (profilointia koskeva suositus).

415 EIT, *Y v. Turkki*, nro 648/10, 17.2.2015.

koskevien tietojen käsittely. Arkaluonteisten henkilötietojen käsittely on periaatteessa kiellettyä[416].

Kieltoon on kuitenkin lueteltu tyhjentävästi poikkeuksia asetuksen 9 artiklan 2 kohdassa. Ne ovat lainmukaisia syitä arkaluonteisten henkilötietojen käsittelylle. Poikkeuksiin kuuluvat tilanteet, joissa

- rekisteröity on antanut nimenomaisen suostumuksensa tietojenkäsittelyyn
- käsittely suoritetaan poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä ja käsittely koskee ainoastaan näiden yhteisöjen (entisiä) jäseniä tai henkilöitä, joilla on yhteisöihin säännölliset, yhteisöjen tarkoituksiin liittyvät yhteydet
- käsittely koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi
- käsittely on tarpeen
    - rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työlainsäädännön, sosiaaliturvan ja sosiaalisen suojelun alalla
    - rekisteröidyn tai toisen luonnollisen henkilön elintärkeiden etujen suojaamiseksi (kun rekisteröity on estynyt antamasta suostumustaan)
    - oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi tai aina, kun tuomioistuimet suorittavat lainkäyttötehtäviään
    - ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten: ”työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi taikka terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten unionin oikeuden tai jäsenvaltion lainsäädännön perusteella tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti”
    - yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten

416 Entinen tietosuojadirektiivi, 7 artiklan f alakohta, nyt yleinen tietosuoja-asetus, 9 artiklan 1 kohta.

- kansanterveyteen liittyvän yleisen edun vuoksi tai
- tärkeää yleistä etua koskevasta syystä.

Erityisten henkilötietoryhmien käsittelemiseksi sopimussuhdetta rekisteröidyn kanssa ei näin ollen katsota oikeusperustaksi arkaluonteisten tietojen lainmukaiselle käsittelylle, lukuun ottamatta sopimusta sellaisen terveydenhuollon ammattilaisen kanssa, jolla on salassapitovelvollisuus[417].

Rekisteröidyn nimenomainen suostumus

EU:n oikeudessa rekisteröidyn suostumus mainitaan ensimmäisenä mahdollisena henkilötietojen lainmukaisen käsittelyn edellytyksenä, riippumatta siitä, ovatko tiedot arkaluonteisia vai eivät. Arkaluonteisten tietojen kohdalla tämän suostumuksen on oltava nimenomainen. Unionin oikeudessa tai kansallisessa lainsäädännössä voidaan kuitenkin säätää, että erityisten tietoryhmien käsittelyn kieltoa ei voida kumota rekisteröidyn suostumuksella[418], esimerkiksi silloin, kun käsittelystä aiheutuu rekisteröidylle erityisiä riskejä.

Työlainsäädäntö tai sosiaaliturvaa ja sosiaalista suojelua koskeva lainsäädäntö

EU:n oikeuden mukaisesti 9 artiklan 1 kohdan kielto voidaan kumota, jos käsittely on tarpeen rekisterinpitäjän tai rekisteröidyn velvoitteiden tai oikeuksien noudattamiseksi työoikeuden tai sosiaaliturvan alalla. Käsittely pitää kuitenkin sallia unionin oikeudessa tai jäsenvaltion lainsäädännössä tai jäsenvaltion lainsäädännön mukaisessa työehtosopimuksessa, jossa säädetään rekisteröidyn perusoikeuksia ja etuja koskevista asianmukaisista suojatoimista.[419] Organisaation ylläpitämiin työpaikkaa koskeviin tietoihin voi kuulua arkaluonteisia henkilötietoja tiettyjen yleisessä tietosuoja-asetuksessa ja asiaankuuluvassa kansallisessa lainsäädännössä määritetyin ehdoin. Arkaluonteisia tietoja voivat olla muun muassa ammattiliiton jäsenyys tai terveystiedot.

417 Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan h ja i alakohta.

418 *Ibid.*, 9 artiklan 2 kohdan a alakohta.

419 Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan b alakohta.

Rekisteröidyn tai toisen henkilön elintärkeät edut

EU:n oikeuden nojalla myös arkaluonteisia tietoja voidaan käsitellä muiden tietojen tavoin, kun rekisteröidyn tai toisen luonnollisen henkilön elintärkeät edut sitä edellyttävät[420]. Kun käsittely perustuu toisen henkilön elintärkeisiin etuihin, tähän lainmukaiseen syyhyn voidaan vedota vain, jos ”käsittelyllä ei ole muuta ilmeistä käsittelyn oikeusperustetta”[421]. Joissakin tapauksissa henkilötietojen käsittelyllä voidaan suojata sekä yksilön etua että yleistä etua, esimerkiksi silloin, kun käsittely on tarpeen humanitaarisista syistä[422].

Jotta arkaluonteisia henkilötietoja voitaisiin käsitellä laillisesti tällä perusteella, on rekisteröidyn täytynyt olla mahdotonta itse päättää asiasta esimerkiksi siksi, että hän on ollut tajuton tai poissa paikalta ja tavoittamattomissa. Toisin sanoen henkilö on fyysisesti tai oikeudellisesti estynyt antamasta suostumustaan.

Hyväntekeväisyysjärjestöt tai voittoa tavoittelemattomat elimet

Henkilötietojen käsittely on sallittua myös poliittisen, filosofisen, uskonnollisen tai ammattiliittotoimintaan liittyvän säätiön, yhdistyksen tai muun voittoa tavoittelemattoman yhteisön laillisen toiminnan yhteydessä. Käsittelyn täytyy kuitenkin koskea ainoastaan näiden yhteisöjen jäseniä tai entisiä jäseniä tai henkilöitä, joilla on yhteisöihin säännölliset, yhteisöjen tarkoituksiin liittyvät yhteydet.[423] Henkilötietoja ei saa luovuttaa yhteisön ulkopuolelle ilman rekisteröidyn suostumusta.

Tiedot, jotka rekisteröity on nimenomaisesti saattanut julkisiksi

Yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan e alakohdassa säädetään, että käsittely ei ole kiellettyä, jos se koskee henkilötietoja, jotka rekisteröity on nimenomaisesti saattanut julkisiksi. Vaikka asetuksessa ei määritellä, mitä ”rekisteröity on nimenomaisesti saattanut julkiseksi” tarkoittaa, niin koska se on poikkeus arkaluonteisten henkilötietojen käsittelyn kieltoon, sitä on tulkittava tiukasti siten, että rekisteröidyn on pitänyt harkitusti saattaa henkilötietonsa julkisiksi. Jos siis televisiossa esitetään valvontakamerasta saatu video, jossa näytetään muun muassa, että palomies loukkaantuu yrittäessään evakuoida ihmisiä rakennuksista, ei voida katsoa,

420 *Ibid.*, 9 artiklan 2 kohdan c alakohta.

421 *Ibid.*, johdanto-osan 46 kappale.

422 *Ibid.*

423 *Ibid.*, 9 artiklan 2 kohdan d alakohta.

että palomies on nimenomaisesti saattanut tiedot julkisiksi. Jos taas palomies on päättänyt kuvailla tapahtumaa ja julkaista videon ja kuvia julkisella verkkosivulla, hän on selkeästi ja harkitusti päättänyt saattaa henkilötiedot julkisiksi. On tärkeää panna merkille, että omien tietojen saattaminen julkisiksi ei tarkoita suostumusta, vaan se on toisenlainen lupa erityisten tietoryhmien käsittelylle.

Se, että rekisteröity on saattanut käsiteltävät henkilötiedot julkisiksi, ei vapauta rekisterinpitäjiä niiden tietosuojalainsäädännön mukaisista velvoitteista. Esimerkiksi käyttötarkoitussidonnaisuuden periaatetta sovelletaan henkilötietoihin edelleen, vaikka kyseiset tiedot olisi annettu julkisesti saataville[424].

Oikeusvaateet

Erityisten tietoryhmien käsittely, joka on ”tarpeen oikeusvaateen laatimiseksi, esittämiseksi tai puolustamiseksi” oikeudellisessa menettelyssä tai hallinnollisessa tai tuomioistuimen ulkopuolisessa menettelyssä[425], sallitaan myös yleisessä tietosuoja-asetuksessa[426]. Tässä tapauksessa käsittelyn täytyy koskea tiettyä oikeusvaadetta sekä sen esittämistä tai puolustamista, ja mikä tahansa kiistan osapuoli voi pyytää sitä.

Tuomioistuimet voivat lainkäyttötehtäviään suorittaessaan käsitellä erityisiä tietoryhmiä oikeusriidan ratkaisussa[427]. Tässä yhteydessä käsiteltäviä erityisiä tietoryhmiä voivat olla geenitiedot vanhemmuuden määrittämisessä tai terveystiedot, kun osa todisteista koskee rikoksen uhrille aiheutuneen vamman yksityiskohtia.

Tärkeät yleistä etua koskevat syyt

Yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan g alakohdan mukaan jäsenvaltiot voivat soveltaa muita olosuhteita, joissa arkaluonteisia tietoja voidaan käsitellä, kunhan

- tietojen käsittelyyn on tärkeä yleistä etua koskeva syy
- siitä säädetään unionin oikeudessa tai jäsenvaltion lainsäädännössä

424 Tietosuojatyöryhmä (2013), *Opinion 3/13 on purpose limitation*, WP 203, Bryssel, 2.4.2013, s. 14.

425 Yleinen tietosuoja-asetus, johdanto-osan 52 kappale.

426 *Ibid.*, 9 artiklan 2 kohdan f alakohta.

427 *Ibid.*

- unionin oikeus tai jäsenvaltion lainsäädäntö on oikeasuhteinen, siinä noudatetaan oikeutta henkilötietojen suojaan ja siinä säädetään asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn perusoikeuksien ja etujen suojaamiseksi[428].

Tärkeä esimerkki tällaisesta ovat sähköiset potilastietojärjestelmät. Näiden järjestelmien avulla terveydenhuoltopalvelujen tarjoaja voi saattaa potilaan hoidon yhteydessä keräämänsä terveystiedot muiden samalle potilaalle terveydenhuoltopalveluja tarjoavien toimijoiden saataville laajassa mittakaavassa, yleensä valtakunnallisesti.

Tietosuojatyöryhmä totesi, ettei sähköisiä potilastietojärjestelmiä voinut ottaa käyttöön potilastietojen käsittelyä säännelleiden oikeussääntöjen nojalla[429]. Sähköisiä potilastietojärjestelmiä voidaan kuitenkin ottaa käyttöön, jos ne voidaan perustella ”tärkeällä yleisellä edulla”[430]. Niiden käyttöönotto edellyttäisi nimenomaista oikeusperustaa, jossa olisi myös tarvittavat suojatoimet järjestelmän turvallisen käytön varmistamiseksi[431].

Muita arkaluonteisten tietojen käsittelyä koskevia perusteita

Yleisessä tietosuoja-asetuksessa säädetään, että arkaluonteisia tietoja voidaan käsitellä, kun käsittely on tarpeen[432]

- ennalta ehkäisevää tai työterveydenhuoltoa koskevia tarkoituksia varten, työntekijän työkyvyn arvioimiseksi, lääketieteellisiä diagnooseja varten, terveys- tai sosiaalihuollollisen hoidon tai käsittelyn suorittamiseksi taikka terveys- tai sosiaalihuollon palvelujen ja järjestelmien hallintoa varten unionin oikeuden tai jäsenvaltion lainsäädännön perusteella tai terveydenhuollon ammattilaisen kanssa tehdyn sopimuksen mukaisesti

- kansanterveyteen liittyvän yleisen edun vuoksi, kuten vakavilta rajatylittäviltä terveysuhkilta suojautumiseksi tai terveydenhuollon, lääkevalmisteiden

428 *Ibid.*, 9 artiklan 2 kohdan g alakohta.

429 Tietosuojatyöryhmä (2007), *valmisteluasiakirja potilastietojen käsittelystä sähköisissä potilastietokannoissa*, WP 131, Bryssel, 15.2.2007. Ks. myös yleinen tietosuoja-asetus, 9 artiklan 3 kohta.

430 Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan g alakohta.

431 Tietosuojatyöryhmä (2007), *valmisteluasiakirja potilastietojen käsittelystä sähköisissä potilastietokannoissa*, WP 131, Bryssel, 15.2.2007.

432 Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan h, i ja j alakohta.

tai lääkinnällisten laitteiden korkeiden laatu- ja turvallisuusnormien varmistamiseksi unionin oikeuden tai jäsenvaltion lainsäädännön perusteella. Laissa on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien suojaamiseksi

- arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten unionin oikeuden tai jäsenvaltion lainsäädännön nojalla. Lain on oltava oikeasuhteinen tavoitteeseen nähden, siinä on noudatettava keskeisiltä osin oikeutta henkilötietojen suojaan ja siinä on säädettävä asianmukaisista ja erityisistä toimenpiteistä rekisteröidyn oikeuksien ja etujen suojaamiseksi.

Kansallisen lainsäädännön mukaiset lisäehdot

Yleisen tietosuoja-asetuksen mukaan jäsenvaltiot voivat myös ottaa käyttöön tai pitää voimassa lisäehtoja, mukaan lukien rajoituksia, jotka koskevat geneettisten tietojen, biometristen tietojen tai terveystietojen käsittelyä[433].

4.2 Käsittelyn turvallisuutta koskevat säännöt

Keskeiset kohdat

- Käsittelyn turvallisuutta koskevat säännöt asettavat rekisterinpitäjälle ja henkilötietojen käsittelijälle velvollisuuden toteuttaa asianmukaiset tekniset ja organisatoriset toimenpiteet, joilla ehkäistään luvaton puuttuminen henkilötietojen käsittelytoimiin.
- Tietoturvan riittävä taso määräytyy seuraavien perusteella:
  - markkinoilla tietynlaista käsittelyä varten saatavilla olevat turvatoiminnot
  - kustannukset
  - tietojenkäsittelystä rekisteröityjen perusoikeuksille ja -vapauksille aiheutuvat riskit.
- Henkilötietojen luottamuksellisuuden varmistaminen on osa yleisessä tietosuoja-asetuksessa tunnustettua yleistä periaatetta.

433 *Ibid.*, 9 artiklan 2 kohdan h alakohta ja 9 artiklan 4 kohta.

Rekisterinpitäjillä on sekä **EU:n että Euroopan neuvoston oikeudessa** yleinen velvollisuus toimia avoimesti ja vastuullisesti henkilötietoja käsitellessään ja erityisesti ilmoittaa henkilötietojen tietoturvaloukkauksista, jos niitä tapahtuu. Rekisterinpitäjän on ilmoitettava henkilötietojen tietoturvaloukkauksista valvontaviranomaiselle, paitsi jos siitä ei todennäköisesti aiheudu luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä. Myös rekisteröidyille on ilmoitettava henkilötietojen tietoturvaloukkauksista, jos se todennäköisesti aiheuttaa luonnollisen henkilön oikeuksien ja vapauksien kannalta suuren riskin.

4.2.1 Tietoturvaan liittyvät näkökohdat

EU:n oikeudessa asiasta säädetään seuraavaa:

> *"Ottaen huomioon uusin tekniikka ja toteuttamiskustannukset, käsittelyn luonne, laajuus, asiayhteys ja tarkoitukset sekä luonnollisten henkilöiden oikeuksiin ja vapauksiin kohdistuvat, todennäköisyydeltään ja vakavuudeltaan vaihtelevat riskit rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava riskiä vastaavan turvallisuustason varmistamiseksi asianmukaiset tekniset ja organisatoriset toimenpiteet."*[434]

Näitä toimenpiteitä ovat muun muassa

- henkilötietojen pseudonymisointi ja salaus[435]
- käsittelyjärjestelmien ja palveluiden jatkuvan luottamuksellisuuden, eheyden, käytettävyyden ja vikasietoisuuden takaaminen[436]
- tietojen saatavuuden ja tietoihin pääsyn nopea palauttaminen tietojen kadotessa[437]
- menettely, jolla testataan, tutkitaan ja arvioidaan toimenpiteiden tehokkuutta tietojenkäsittelyn turvallisuuden varmistamiseksi[438].

434 *Ibid.*, 32 artiklan 1 kohta.

435 *Ibid.*, 32 artiklan 1 kohdan a alakohta.

436 *Ibid.*, 32 artiklan 1 kohdan b alakohta.

437 *Ibid.*, 32 artiklan 1 kohdan c alakohta.

438 *Ibid.*, 32 artiklan 1 kohdan d alakohta.

Euroopan neuvoston oikeudessa on olemassa vastaavanlainen määräys:

> *Kunkin osapuolen on taattava, että rekisterinpitäjä ja soveltuvin osin henkilötietojen käsittelijä ryhtyvät asianmukaisiin turvatoimiin henkilötietojen suojelemiseksi vahingossa tapahtuvalta tai luvattomalta tuhoamiselta tai vahingossa tapahtuvalta katoamiselta samoin kuin luvattoman henkilötietoihin pääsyn, henkilötietojen käytön, muuttamisen tai levittämisen varalta.*[439]

EU:n ja Euroopan neuvoston oikeudessa rekisterinpitäjän on ilmoitettava valvontaviranomaiselle tietoturvaloukkauksesta, joka vaikuttaa yksilöiden oikeuksiin ja vapauksiin (ks. 4.2.3 kohta).

Tietojen turvallista käsittelyä varten on myös laadittu useita toimialakohtaisia, kansallisia tai kansainvälisiä standardeja. Esimerkiksi eurooppalainen yksityisyyden suojaa koskeva tunnus (EuroPriSe) on Euroopan laajuisia televerkkoja koskeva (eTEN) hanke, jossa on tutkittu mahdollisuuksia sertifioida tuotteita, erityisesti ohjelmistoja, jotka täyttävät Euroopan tietosuojaoikeuden vaatimukset. Euroopan unionin verkko- ja tietoturvavirasto (ENISA) perustettiin parantamaan EU:n, sen jäsenvaltioiden ja sen yritysmaailman mahdollisuuksia ehkäistä, käsitellä ja ratkaista verkko- ja tietoturvaongelmia[440]. ENISA julkaisee säännöllisesti analyysejä uusista turvauhista ja ohjeita niiden käsittelemiseen[441].

Tietoturvaa ei saavuteta pelkästään oikeilla välineillä – laitteistoilla ja ohjelmistoilla. Siihen tarvitaan myös asianmukaiset organisaation sisäiset säännöt. Tällaisten sääntöjen olisi hyvä kattaa seuraavat asiat:

- säännöllinen tiedottaminen kaikille työntekijöille tietoturvasäännöistä ja heille tietosuojasäännösten nojalla kuuluvista velvollisuuksista, erityisesti velvollisuudesta säilyttää tietojen luottamuksellisuus

439 Uudistettu yleissopimus 108, 7 artiklan 1 kohta.

440 Euroopan parlamentin ja neuvoston asetus (EU) N:o 526/2013, annettu 21 päivänä toukokuuta 2013, Euroopan unionin verkko- ja tietoturvavirastosta (ENISA) ja asetuksen (EY) N:o 460/2004 kumoamisesta, EUVL 2013, L 165.

441 Esimerkiksi ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

- selkeä vastuunjako ja selkeästi määritellyt valtuudet käsitellä henkilötietoja, erityisesti sellaisten päätösten osalta, jotka koskevat henkilötietojen käsittelyä ja luovuttamista sivullisille

- henkilötietojen käyttäminen ainoastaan toimivaltaisen henkilön ohjeiden tai yleisesti sovittujen sääntöjen mukaisesti

- rekisterinpitäjän tai henkilötietojen käsittelijän tiloihin sekä laitteistoihin ja ohjelmistoihin pääsyn suojaaminen, mukaan lukien pääsyn luvallisuuden tarkistaminen

- sen varmistaminen, että toimivaltainen henkilö on antanut luvan käsitellä henkilötietoja ja että luvat dokumentoidaan asianmukaisesti

- henkilötietojen sähköisen käytön automaattiset yhteyskäytännöt ja niiden sisäisen valvontapalvelun tekemät säännölliset tarkistukset (minkä vuoksi kaikki tietojenkäsittelytoimet on tallennettava)

- muiden tietojen luovuttamisen muotojen kuin automaattisen tietoihin pääsyn huolellinen dokumentointi sen todistamiseksi, ettei tietoja ole siirretty laittomasti.

Myös riittävän tietoturvakoulutuksen tarjoaminen henkilöstölle on tärkeä osa tehokkaita turvatoimia. Todentamismenettelyillä (kuten sisäisillä tai ulkoisilla tarkastuksilla) on varmistettava, että asianmukaiset toimenpiteet todella toteutetaan ja niitä noudatetaan käytännössä.

Toimenpiteisiin, joilla rekisterinpitäjät tai henkilötietojen käsittelijät voivat parantaa turvallisuutta, kuuluvat muun muassa tietosuojavastaavan nimeäminen, työntekijöiden turvallisuuskoulutus, säännölliset tarkastukset, koehyökkäykset sekä laatua koskevat tunnukset.

Esimerkki: Asiassa *I v. Suomi*[442] kantaja ei ollut pystynyt todistamaan, että muut työntekijät siinä sairaalassa, jossa hän työskenteli, olivat käyneet laittomasti katsomassa hänen potilastietojaan. Näin ollen kansalliset tuomioistuimet hylkäsivät hänen väitteensä yksityiselämän suojaa koskevan

442 EIT, *I v. Suomi*, nro 20511/03, 17.7.2008.

oikeuden rikkomisesta. Euroopan ihmisoikeustuomioistuin kuitenkin katsoi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu, sillä sairaalan potilastietojen rekisterijärjestelmästä ei voinut takautuvasti selvittää potilasasiakirjojen käyttöä, vaan järjestelmä näytti ainoastaan viisi viimeisintä käyttäjää ja tämäkin tieto poistui, kun asiakirja palautettiin arkistoon. Tuomioistuimen näkemyksen mukaan ratkaisevaa oli se, että sairaalassa käytössä ollut rekisterijärjestelmä ei selvästikään ollut vastannut kansallisen lain vaatimuksia, mitä kansalliset tuomioistuimet eivät olleet riittävästi painottaneet.

EU:ssa on otettu käyttöön direktiivi verkko- ja tietoturvajärjestelmien turvallisuudesta (verkko- ja tietoturvadirektiivi)[443]. Se on ensimmäinen EU:n laajuinen säädös kyberturvallisuudesta. Direktiivin tavoitteena on toisaalta parantaa kyberturvallisuutta kansallisella tasolla ja toisaalta lisätä yhteistyötä EU:ssa. Siinä myös asetetaan keskeisten palvelujen tarjoajille (muun muassa energia-, terveydenhuolto-, pankki-, liikenne- ja digitaali-infrastruktuurialojen toimijoille) ja digitaalisten palvelujen tarjoajille vaatimuksia riskien hallinnasta, niiden verkko- ja tietojärjestelmien turvallisuuden varmistamisesta ja turvapoikkeamista ilmoittamisesta.

Tulevaisuudennäkymät

Euroopan komissio antoi syyskuussa 2017 ehdotuksen asetukseksi, jonka tarkoituksena on vahvistaa ENISAn toimeksiantoa ja ottaa huomioon viraston uudet verkko- ja tietoturvadirektiivin mukaiset valtuudet ja vastuut. Ehdotetun asetuksen tavoitteena on kehittää ENISAn tehtäviä ja vahvistaa sen roolia ”EU:n kyberturvallisuusekosysteemin viitekeskuksena”[444]. Ehdotettu asetus ei vaikuta yleisen tietosuoja-asetuksen periaatteisiin, ja sen pitäisi vahvistaa myös henkilötietojen suojaa selkeyttämällä tarvittavia tekijöitä, joista Euroopan kyberturvallisuuden sertifiointijärjestelmät koostuvat. Euroopan komissio antoi myös syyskuussa 2017 ehdotuksen täytäntöönpanoasetukseksi, jossa yksilöidään näkökohtia, joita digitaalisten palvelujen tarjoajien pitäisi ottaa huomioon varmistaakseen, että niiden verkko- ja tietojärjestelmät ovat turvallisia verkko- ja tietoturvadirektiivin 16 artiklan 8 kohdan mukaisesti. Käsikirjaa laadittaessa molemmat ehdotukset olivat käsiteltävinä.

443 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/1148, annettu 6 päivänä heinäkuuta 2016, toimenpiteistä yhteisen korkeatasoisen verkko- ja tietojärjestelmien turvallisuuden varmistamiseksi koko unionissa, EUVL 2016, L 194.

444 Ehdotus Euroopan parlamentin ja neuvoston asetukseksi EU:n kyberturvallisuusvirastosta ENISAsta ja asetuksen (EU) N:o 526/2013 kumoamisesta sekä tieto- ja viestintätekniikan kyberturvallisuussertifioinnista (”kyberturvallisuusasetus”), COM(2017) 477, 13.9.2017, s. 6.

4.2.2 Luottamuksellisuus

EU:n oikeudessa yleisessä tietosuoja-asetuksessa tunnustetaan henkilötietojen luottamuksellisuus yleisen periaatteen osaksi[445]. Yleisesti saatavilla olevien sähköisten viestintäpalvelujen tarjoajien on varmistettava luottamuksellisuus. Niiden on myös taattava palvelujen turvallisuus.[446]

Esimerkki: Vakuutusyhtiön työntekijä saa työpaikallaan puhelun henkilöltä, joka väittää olevansa asiakas ja joka haluaa saada tietoa vakuutussopimuksestaan.

Velvollisuus säilyttää asiakkaiden tiedot luottamuksellisina edellyttää, että työntekijä toteuttaa ainakin vähimmäisturvatoimet ennen henkilötietojen luovuttamista. Sen voi tehdä esimerkiksi ehdottamalla soittamista takaisin asiakastiedoissa olevaan puhelinnumeroon.

Yleisen tietosuoja-asetuksen 5 artiklan 1 kohdan f alakohdan mukaan henkilötietoja on käsiteltävä tavalla, jolla varmistetaan henkilötietojen asianmukainen turvallisuus, mukaan lukien suojaaminen luvattomalta ja lainvastaiselta käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta käyttäen asianmukaisia teknisiä tai organisatorisia toimia (”eheys ja luottamuksellisuus”).

Asetuksen 32 artiklan mukaan rekisterinpitäjän ja henkilötietojen käsittelijän on toteutettava korkean turvallisuustason varmistamiseksi teknisiä ja organisatorisia toimenpiteitä. Näitä toimenpiteitä ovat muun muassa henkilötietojen pseudonymisointi ja salaus, kyky taata käsittelyjärjestelmien ja palveluiden jatkuva luottamuksellisuus, eheys, käytettävyys ja vikasietoisuus, toimenpiteiden tehokkuuden arviointi ja testaus sekä kyky palauttaa tietojen saatavuus ja pääsy tietoihin fyysisen tai teknisen vian sattuessa. Hyväksyttyjen käytännesääntöjen tai hyväksytyn sertifiointimekanismin noudattamista voidaan myös käyttää sen osoittamisessa, että käsittelyn eheyttä ja luottamuksellisuutta koskevaa periaatetta noudatetaan. Lisäksi yleisen tietosuoja-asetuksen 28 artiklan mukaan sopimuksella, joka sitoo rekisterinpitäjää henkilötietojen käsittelijään, on säädettävä, että henkilötietojen käsittelijä varmistaa, että henkilöt, joilla on oikeus käsitellä henkilötietoja, ovat sitoutuneet noudattamaan salassapitovelvollisuutta tai heitä koskee asianmukainen lakisääteinen salassapitovelvollisuus.

445 Yleinen tietosuoja-asetus, 5 artiklan 1 kohdan f alakohta.

446 Sähköisen viestinnän tietosuojadirektiivi, 5 artiklan 1 kohta.

Salassapitovelvollisuus ei kata tilanteita, joissa henkilö saa tiedon yksityishenkilönä eikä rekisterinpitäjän tai henkilötietojen käsittelijän työntekijänä. Tässä tapauksessa yleisen tietosuoja-asetuksen 32 ja 28 artiklaa ei sovelleta, koska yksityishenkilöiden suorittama henkilötietojen käsittely jää kokonaan asetuksen soveltamisalan ulkopuolelle silloin, kun sen katsotaan kuuluvan kotitaloutta koskevan poikkeuksen piiriin[447]. Kotitaloutta koskevalla poikkeuksella tarkoitetaan henkilötietojen käyttöä, jonka "luonnollinen henkilö suorittaa yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa"[448]. Euroopan unionin tuomioistuimen asiassa *Bodil Lindqvist*[449] antaman ratkaisun jälkeen tätä poikkeusta on kuitenkin pitänyt tulkita suppeasti, erityisesti tietojen luovuttamisen yhteydessä. Kotitaloutta koskeva poikkeus ei etenkään kata henkilötietojen julkaisemista internetissä rajoittamattomalle määrälle vastaanottajia eikä tietojenkäsittelyä, johon liittyy ammattimaisia tai kaupallisia näkökohtia (asiaa käsitellään tarkemmin 2.1.2, 2.2.2 ja 2.3.1 kohdassa)

"Viestinnän luottamuksellisuus" on luottamuksellisuuden osa, johon sovelletaan erityissäännöstä. Sähköisen viestinnän tietosuojadirektiivin sähköisen viestinnän luottamuksellisuuden varmistamista koskevissa erityissäännöissä vaaditaan jäsenvaltioita kieltämään se, että muut henkilöt kuin käyttäjät ilman kyseisten käyttäjien nimenomaista suostumusta kuuntelevat, salakuuntelevat, tallentavat tai muulla tavalla sieppaavat tai valvovat viestintää ja siihen liittyviä liikennetietoja[450]. Jäsenvaltioiden lainsäädännössä voidaan sallia tästä periaatteesta poikkeuksia vain kansallisen turvallisuuden, puolustuksen, rikosten ehkäisyn tai selvittämisen varmistamiseksi ja vain, jos ne ovat tarpeen ja oikeassa suhteessa tavoitteisiin nähden[451]. Samoja sääntöjä sovelletaan tulevan sähköisen viestinnän tietosuoja-asetuksen nojalla, mutta sähköisen viestinnän tietosuojaa koskevan säädöksen soveltamisalaa laajennetaan yleisesti saatavilla olevista sähköisistä viestintäpalveluista myös internetissä tapahtuvassa jakelussa tehtävään viestintään (kuten mobiilisovelluksiin).

Euroopan neuvoston oikeudessa luottamuksellisuuden säilyttämistä koskeva velvollisuus sisältyy implisiittisesti tietoturvan käsitteeseen uudistetun yleissopimuksen 108 7 artiklan 1 kohdassa, joka koskee tietoturvaa.

447 Yleinen tietosuoja-asetus, 2 artiklan 2 kohdan c alakohta.

448 *Ibid.*

449 EUT, C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003.

450 Sähköisen viestinnän tietosuojadirektiivi, 5 artiklan 1 kohta.

451 *Ibid.*, 15 artiklan 1 kohta.

Henkilötietojen käsittelijöiden osalta luottamuksellisuudella tarkoitetaan, että ne eivät saa luovuttaa tietoja kolmansille osapuolille tai muille vastaanottajille ilman lupaa. Rekisterinpitäjän tai henkilötietojen käsittelijän työntekijöiden kohdalla luottamuksellisuus edellyttää, että he noudattavat henkilötietojen käsittelyssä toimivaltaisten esimiestensä ohjeita.

Salassapitovelvollisuus on sisällytettävä kaikkiin rekisterinpitäjien ja henkilötietojen käsittelijöiden välillä tehtäviin sopimuksiin. Lisäksi rekisterinpitäjien ja henkilötietojen käsittelijöiden on toteutettava erityisiä toimenpiteitä, joilla ne määräävät työntekijänsä salassapitovelvollisiksi. Yleensä tämä tehdään sisällyttämällä työntekijän työsopimukseen salassapitolauseke.

Ammattitoimintaan liittyvän salassapitovelvollisuuden rikkominen on monissa EU:n jäsenvaltioissa ja yleissopimuksen 108 sopimusvaltioissa rikoslain nojalla rangaistava teko.

4.2.3 Henkilötietojen tietoturvaloukkauksista ilmoittaminen

Henkilötietojen tietoturvaloukkauksella tarkoitetaan tietoturvaloukkausta, jonka seurauksena on käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin[452]. Vaikka uusien teknologioiden, kuten salauksen, ansiosta on entistä enemmän mahdollisuuksia käsittelyn turvallisuuden varmistamiseen, tietoturvaloukkaukset ovat edelleen yleinen ilmiö. Tietoturvaloukkausten syyt vaihtelevat organisaatiossa työskentelevien ihmisten vahingossa tekemistä virheistä aina hakkerien ja kyberrikollisjärjestöjen kaltaisiin ulkoisiin uhkiin.

Tietoturvaloukkaukset voivat olla erittäin haitallisia yksilöiden yksityisyydensuojaa ja tietosuojaa koskeville oikeuksille, sillä loukkauksen vuoksi he eivät enää pysty hallitsemaan henkilötietojaan. Loukkaukset voivat johtaa identiteettivarkauteen tai -petokseen, taloudellisiin tappioihin tai aineellisiin vahinkoihin, vaitiolovelvollisuudella suojattujen henkilötietojen luottamuksellisuuden menettämiseen ja rekisteröidyn maineen vahingoittumiseen. Tietosuojatyöryhmä selittää asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta

452 Yleinen tietosuoja-asetus, 4 artiklan 12 kohta; ks. myös tietosuojatyöryhmä (2017), *suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta*, WP250, 3.10.2017, s. 9.

antamissaan suuntaviivoissa, että loukkauksilla voi olla kolmenlaisia vaikutuksia henkilötietoihin: niiden luvaton luovuttaminen, häviäminen ja/tai muuttaminen[453]. Sen lisäksi, että käsittelyn turvallisuuden varmistamiseksi on ryhdyttävä toimenpiteisiin, kuten 4.2 kohdassa selitetään, yhtä tärkeää on varmistaa, että rekisterinpitäjät puuttuvat tapahtuneisiin tietoturvaloukkauksiin asianmukaisesti ja ajoissa.

Valvontaviranomaiset ja yksityishenkilöt eivät usein ole tietoisia tietoturvaloukkauksen tapahtumisesta, eivätkä henkilöt siksi pysty ryhtymään toimenpiteisiin suojellakseen itseään sen kielteisiltä seurauksilta. Yksilöiden oikeuksien vahvistamiseksi ja tietoturvaloukkausten vaikutusten rajoittamiseksi **EU:n ja Euroopan neuvoston oikeudessa** säädetään rekisterinpitäjien ilmoitusvaatimuksesta tietyissä olosuhteissa.

Euroopan neuvoston oikeudessa uudistetun yleissopimuksen 108 mukaan sopimusosapuolten on vähintään vaadittava rekisterinpitäjiä ilmoittamaan toimivaltaiselle valvontaviranomaiselle tietoturvaloukkauksista, jotka voivat vaikuttaa vakavasti rekisteröityjen oikeuksiin. Tällainen ilmoitus on tehtävä viipymättä[454].

EU:n oikeudessa säädetään ilmoitusten ajankohtaa ja sisältöä sääntelevästä yksityiskohtaisesta järjestelmästä[455]. Sen mukaan rekisterinpitäjien on ilmoitettava tietyistä tietoturvaloukkauksista valvontaviranomaisille ilman aiheetonta viivytystä ja mahdollisuuksien mukaan 72 tunnin kuluessa sen ilmitulosta. Jos 72 tunnin määräaika ylittyy, ilmoituksen mukana on toimitettava selitys viivytyksestä. Rekisterinpitäjät vapautetaan ilmoitusvaatimuksesta vain, jos ne pystyvät osoittamaan, että henkilötietojen tietoturvaloukkauksesta ei todennäköisesti aiheudu kyseessä olevien henkilöiden oikeuksiin ja vapauksiin kohdistuvaa riskiä.

Asetuksessa yksilöidään vähimmäistiedot, joiden täytyy sisältyä ilmoitukseen, jotta valvontaviranomainen voi ryhtyä tarvittaviin toimiin[456]. Ilmoituksessa on vähintään kuvattava henkilötietojen tietoturvaloukkaus sekä asianomaisten rekisteröityjen ryhmät ja arvioidut lukumäärät, kuvattava henkilötietojen tietoturvaloukkauksen todennäköiset seuraukset sekä toimenpiteet, jotka rekisterinpitäjä on toteuttanut henkilötietojen tietoturvaloukkauksen haittavaikutusten lieventämiseksi. Lisäksi on

453 Tietosuojatyöryhmä (2017), *suuntaviivat asetuksen (EU) 2016/679 mukaisesta henkilötietojen tietoturvaloukkauksen ilmoittamisesta*, WP250, 3.10.2017, s. 7.

454 Uudistettu yleissopimus 108, 7 artiklan 2 kohta, uudistettu yleissopimus 108, selitysmuistio, 64–66 kohta.

455 Yleinen tietosuoja-asetus, 33 ja 34 artikla.

456 *Ibid.*, 33 artiklan 3 kohta.

ilmoitettava tietosuojavastaavan nimi ja yhteystiedot tai muu yhteyspiste, josta toimivaltainen viranomainen voi saada tarvittaessa lisätietoa.

Jos henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin luonnollisten henkilöiden oikeuksille ja vapauksille, rekisterinpitäjien on ilmoitettava tietoturvaloukkauksesta näille henkilöille (rekisteröidylle) ilman aiheetonta viivytystä[457]. Rekisteröidylle annettavat tiedot, myös tietoturvaloukkauksen kuvaus, on esitettävä selkeällä ja yksinkertaisella kielellä, ja niissä on annettava samat tiedot kuin valvontaviranomaisille annettavissa ilmoituksissa. Tietyissä olosuhteissa rekisterinpitäjät voidaan vapauttaa velvollisuudesta ilmoittaa rekisteröidyille kyseisistä tietoturvaloukkauksista. Poikkeuksia sovelletaan, kun rekisterinpitäjä on toteuttanut asianmukaiset tekniset ja organisatoriset suojatoimenpiteet ja henkilötietojen tietoturvaloukkauksen kohteena oleviin henkilötietoihin on sovellettu kyseisiä toimenpiteitä, erityisesti niitä, joiden avulla henkilötiedot muutetaan muotoon, jossa ne eivät ole sellaisten henkilöiden ymmärrettävissä, joilla ei ole lupaa päästä tietoihin, kuten salausta. Rekisterinpitäjä voidaan vapauttaa rekisteröidyille ilmoittamista koskevasta velvollisuudesta, jos se on tietoturvaloukkauksen jälkeen toteuttanut toimenpiteitä, joilla varmistetaan, että rekisteröidyn oikeuksiin kohdistuva haitta ei enää toteudu. Jos taas ilmoittaminen vaatisi rekisterinpitäjältä kohtuutonta vaivaa, rekisteröidyille voidaan ilmoittaa tietoturvaloukkauksesta muilla keinoilla, kuten julkisella tiedonannolla tai vastaavilla toimenpiteillä.[458]

Velvollisuus ilmoittaa henkilötietojen tietoturvaloukkauksista valvontaviranomaisille ja rekisteröidyille koskee rekisterinpitäjiä. Tietoturvaloukkauksia voi kuitenkin tapahtua riippumatta siitä, toteuttaako käsittelyn rekisterinpitäjä vai henkilötietojen käsittelijä. Siksi on olennaisen tärkeää varmistaa, että myös henkilötietojen käsittelijöiden on ilmoitettava tietoturvaloukkauksista. Tällaisissa tapauksissa henkilötietojen käsittelijän on ilmoitettava henkilötietojen tietoturvaloukkauksista rekisterinpitäjälle ilman aiheetonta viivytystä[459]. Rekisterinpitäjän on sitten ilmoitettava valvontaviranomaisille ja asianomaisille rekisteröidyille edellä mainittujen sääntöjen ja määräajan mukaisesti.

457 *Ibid.*, 34 artikla.

458 *Ibid.*, 34 artiklan 3 kohdan c alakohta.

459 *Ibid.*, 33 artiklan 2 kohta.

4.3 Osoitusvelvollisuutta ja sääntöjen noudattamista edistävät säännöt

Keskeiset kohdat

- Osoitusvelvollisuuden varmistamiseksi henkilötietojen käsittelyssä rekisterinpitäjien ja henkilötietojen käsittelijöiden on ylläpidettävä rekisteriä vastuullaan olevista käsittelytoimista ja esitettävä ne valvontaviranomaisille pyydettäessä.
- Yleisessä tietosuoja-asetuksessa esitetään useita tapoja sääntöjen noudattamisen edistämiseksi:
  - tietosuojavastaavien nimittäminen tietyissä tilanteissa
  - vaikutustenarvioinnin tekeminen ennen sellaisten käsittelytoimien aloittamista, jotka todennäköisesti aiheuttavat suuria riskejä yksilöiden oikeuksien ja vapauksien kannalta
  - asianomaisen valvontaviranomaisen ennakkokuuleminen, jos vaikutustenarvioinnista käy ilmi, että käsittely aiheuttaa riskejä, joita ei voida pienentää
  - rekisterinpitäjien ja henkilötietojen käsittelijöiden käytännesäännöt, joissa yksilöidään asetuksen soveltaminen käsittelyn eri sektoreilla
  - sertifiointimekanismit, tietosuojasinetit ja -merkit.
- Euroopan neuvoston oikeudessa ehdotetaan samanlaisia tapoja sääntöjen noudattamisen edistämiseen uudistetussa yleissopimuksessa 108.

Osoitusvelvollisuuden periaate on erityisen tärkeä, jotta tietosuojasääntöjen valvonta Euroopassa voidaan taata. Rekisterinpitäjä on vastuussa tietosuojasääntöjen noudattamisesta, ja sen on pystyttävä osoittamaan se. Osoitusvelvollisuutta ei pitäisi soveltaa ainoastaan rikkomuksen jälkeen. Rekisterinpitäjillä on sen sijaan ennakoiva velvollisuus noudattaa asianmukaisia tiedonhallintakäytäntöjä kaikissa tietojenkäsittelyn vaiheissa. Euroopan tietosuojalainsäädännön mukaan rekisterinpitäjän on toteutettava teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan, että käsittely tehdään lain mukaan, ja rekisterinpitäjän on pystyttävä osoittamaan lainmukaisuus. Näitä toimenpiteitä ovat muun muassa tietosuojavastaavien nimittäminen, käsittelyyn liittyvien rekisterien ja asiakirjojen ylläpito ja yksityisyydensuojaa koskevien vaikutustenarviointien tekeminen.

4.3.1 Tietosuojavastaavat

Tietosuojavastaavat ovat henkilöitä, jotka antavat tietojenkäsittelyä tekevissä organisaatioissa neuvontaa tietosuojasääntöjen noudattamisesta. He ovat ”osoitusvelvollisuuden kulmakivi”, koska he helpottavat sääntöjen noudattamista ja toimivat myös välittäjinä valvontaviranomaisten, rekisteröityjen ja heidät nimittäneen organisaation välillä.

Euroopan neuvoston oikeudessa uudistetun yleissopimuksen 108 10 artiklan 1 kohdassa annetaan yleinen osoitusvelvollisuus rekisterinpitäjille ja henkilötietojen käsittelijöille. Se edellyttää, että rekisterinpitäjät ja henkilötietojen käsittelijät ryhtyvät kaikkiin asianmukaisiin toimenpiteisiin yleissopimuksessa säädettyjen tietosuojasääntöjen noudattamiseksi ja että ne pystyvät osoittamaan, että niiden valvonnassa tehty tietojenkäsittely on yleissopimuksen säännösten mukaista. Vaikka yleissopimuksessa ei yksilöidä konkreettisia toimenpiteitä, jotka rekisterinpitäjien ja henkilötietojen käsittelijöiden olisi toteutettava, uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että tietosuojavastaavan nimittäminen olisi yksi mahdollinen toimenpide, joka auttaisi sääntöjen noudattamisen osoittamisessa. Tietosuojavastaaville olisi annettava kaikki heidän tehtäviensä täyttämiseen tarvittavat keinot[460].

Euroopan neuvoston oikeudesta poiketen **EU:n oikeudessa** tietosuojavastaavan nimittäminen ei ole aina rekisterinpitäjien ja henkilötietojen käsittelijöiden harkinnassa, vaan se on pakollista tietyin ehdoin. Yleisessä tietosuoja-asetuksessa tunnustetaan, että tietosuojavastaavalla on keskeinen asema uudessa hallintojärjestelmässä, ja siinä on yksityiskohtaisia säännöksiä tietosuojavastaavan nimittämisestä, asemasta, velvollisuuksista ja tehtävistä.[461]

Yleisen tietosuoja-asetuksen mukaan tietosuojavastaavan nimittäminen on pakollista kolmessa erityistapauksessa: kun viranomainen tai julkishallinnon elin suorittaa käsittelyä, kun rekisterinpitäjän tai henkilötietojen käsittelijän ydintehtävät muodostuvat käsittelytoimista, jotka edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa, tai kun ydintehtävät muodostuvat laajamittaisesta käsittelystä, joka kohdistuu erityisiin henkilötietoryhmiin ja rikostuomioita tai rikkomuksia koskeviin tietoihin[462]. Vaikka ”laajamittaista järjestelmällistä seurantaa” ja

460 Uudistettu yleissopimus 108, selitysmuistio, 87 kohta.

461 Yleinen tietosuoja-asetus, 37–39 artikla.

462 *Ibid.*, 37 artiklan 1 kohta.

”ydintehtäviä” ei ole määritetty asetuksessa, tietosuojatyöryhmä on antanut ohjeita niiden tulkinnasta[463].

Esimerkki: Sosiaalisen median yritykset ja hakukoneet katsotaan todennäköisesti rekisterinpitäjiksi, joiden käsittelytoimet edellyttävät laajamittaista rekisteröityjen säännöllistä ja järjestelmällistä seurantaa. Tällaisten yritysten liiketoimintamalli perustuu henkilötietojen suurten määrien käsittelyyn, ja ne saavat huomattavia tuloja tarjoamalla kohdennettuja mainontapalveluja ja antamalla yritysten mainostaa sivustoillaan. Kohdennettu mainonta tarkoittaa mainosten sijoittelua väestötietojen ja kuluttajien aiemman ostohistorian tai käytöksen perusteella. Se edellyttää siksi rekisteröityjen verkkoympäristön tapojen ja käytöksen järjestelmällistä seurantaa.

Esimerkki: Sairaala ja sairausvakuutusyhtiö ovat tyypillisiä esimerkkejä rekisterinpitäjistä, joiden toimet muodostuvat erityisten henkilötietoryhmien laajamittaisesta käsittelystä. Tiedot, joista ilmenee yksilön terveyttä koskevia tietoja, ovat sekä Euroopan neuvoston että EU:n oikeuden mukaan erityisiä henkilötietoryhmiä, jotka vaativat vahvempaa suojaa. EU:n oikeudessa tunnustetaan myös geneettiset ja biometriset tiedot erityisiksi tietoryhmiksi. Mikäli sairaalat ja vakuutusyhtiö käsittelevät tällaisia tietoja laajamittaisesti, niiden on yleisen tietosuoja-asetuksen mukaan nimitettävä tietosuojavastaava.

Yleisen tietosuoja-asetuksen 37 artiklan 4 kohdassa säädetään lisäksi, että muissa tapauksissa kuin 37 artiklan 1 kohdassa tarkoitetussa kolmessa pakollisessa tapauksessa, rekisterinpitäjä tai henkilötietojen käsittelijä tai rekisterinpitäjien tai henkilötietojen käsittelijöiden eri ryhmiä edustavat yhdistykset ja muut elimet voivat nimittää tietosuojavastaavan tai, jos unionin oikeudessa tai jäsenvaltion lainsäädännössä niin vaaditaan, niiden on nimitettävä tietosuojavastaava.

Millään muilla organisaatioilla ei ole sitovaa velvoitetta nimittää tietosuojavastaavaa. Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjät ja henkilötietojen käsittelijät voivat kuitenkin nimittää vapaaehtoisesti tietosuojavastaavan ja jäsenvaltiot

463 Tietosuojatyöryhmä (2017), *tietosuojavastaavia koskevat ohjeet*, WP 243 rev.01, viimeksi tarkistettu ja hyväksytty 5.4.2017.

voivat tehdä tietosuojavastaavan nimittämisestä pakollista useamman tyyppisille organisaatioille kuin asetuksessa säädetään[464].

Kun rekisterinpitäjä nimittää tietosuojavastaavan, sen on varmistettava, että ”tietosuojavastaava otetaan asianmukaisesti ja riittävän ajoissa mukaan kaikkien henkilötietojen suojaa koskevien kysymysten käsittelyyn” organisaatiossa[465]. Tietosuojavastaava olisi esimerkiksi otettava mukaan antamaan neuvoja tietosuojan vaikutustenarviointien tekemisestä ja organisaation tietojenkäsittelytoimien luomiseen ja niitä koskevien rekisterien pitämiseen. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on annettava tietosuojavastaaville tarvittavat resurssit, myös taloudelliset resurssit, infrastruktuuri ja laitteet, jotta he voivat suorittaa tehtävänsä tehokkaasti. Muita vaatimuksia ovat muun muassa se, että tietosuojavastaaville varataan riittävästi aikaa tehtävien hoitamiseen ja heille tarjotaan jatkuvasti koulutusta, jotta he pystyvät lisäämään asiantuntemustaan jatkuvasti ja pysymään ajan tasalla tietosuoja-alan kehityksestä.[466]

Yleisessä tietosuoja-asetuksessa vahvistetaan joitakin perustakeita, joilla varmistetaan, että tietosuojavastaavat toimivat riippumattomasti. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on varmistettava, etteivät tietosuojavastaavat ota vastaan ohjeita tietosuojaan liittyvien tehtäviensä hoitamisen yhteydessä yritykseltä, eivät edes ylimpään johtoon kuuluvilta henkilöiltä. Heitä ei saa myöskään erottaa tai rangaista heidän tehtäviensä hoitamisen vuoksi.[467] Otetaan esimerkiksi tapaus, jossa tietosuojavastaava neuvoo rekisterinpitäjää tai henkilötietojen käsittelijää tekemään tietosuojaa koskevan vaikutustenarvioinnin, koska hän katsoo, että käsittely aiheuttaa todennäköisesti suuria riskejä rekisteröityjen kannalta. Yritys on eri mieltä tietosuojavastaavan neuvosta, koska ei pidä sitä perusteltuna, ja päättää olla tekemättä vaikutustenarviointia. Yritys voi jättää noudattamatta neuvoa mutta se ei voi erottaa tai rangaista tietosuojavastaavaa sen antamisen takia.

Tietosuojavastaavan tehtävät ja velvollisuuden yksilöidään yleisen tietosuoja-asetuksen 39 artiklassa. Niihin kuuluvat vaatimukset antaa yrityksille ja henkilötietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat näiden lainsäädännön mukaisia velvollisuuksia, ja seurata, että noudatetaan unionin ja jäsenvaltion

464 Yleinen tietosuoja-asetus, 37 artiklan 3 ja 4 kohta.

465 *Ibid.*, 38 artiklan 1 kohta.

466 Tietosuojatyöryhmä (2017), *tietosuojavastaavia koskevat ohjeet*, WP 243 rev.01, viimeksi tarkistettu ja hyväksytty 5.4.2017, 3.1 kohta.

467 Yleinen tietosuoja-asetus, 38 artiklan 2 ja 3 kohta.

tietosuojalainsäännöksiä tekemällä tarkastuksia ja kouluttamalla käsittelytoimiin osallistuvaa henkilöstöä. Tietosuojavastaavien on myös tehtävä yhteistyötä valvontaviranomaisen kanssa ja toimittava valvontaviranomaisen yhteyspisteenä käsittelyyn liittyvissä kysymyksissä, kuten esimerkiksi tietoturvaloukkauksissa.

Asetuksessa (EY) N:o 45/2001 säädetään, että EU:n toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä kunkin unionin toimielimen ja elimen on nimitettävä tietosuojavastaava. Tietosuojavastaavan tehtävänä on varmistaa, että asetuksen säännöksiä sovelletaan moitteettomasti EU:n toimielimissä ja elimissä ja että sekä rekisteröidyille että rekisterinpitäjille tiedotetaan heidän oikeuksistaan ja velvollisuuksistaan[468]. Hänen tehtävänään on myös vastata Euroopan tietosuojavaltuutetun kysymyksiin ja olla tarvittaessa yhteistyössä Euroopan tietosuojavaltuutetun kanssa. Yleistä tietosuoja-asetusta vastaavasti asetuksessa (EY) N:o 45/2001 on säännöksiä tietosuojavastaavan riippumattomuudesta tehtäviensä suorittamisessa sekä siitä, että hänen käyttöönsä on järjestettävä tarvittava henkilöstö ja resurssit[469]. Tietosuojavastaaville on ilmoitettava ennen kuin EU:n toimielin tai elin (tai niiden osastot) tekevät käsittelytoimia, ja heidän on pidettävä rekisteriä kaikista ilmoitetuista käsittelytoimista[470].

4.3.2 Seloste käsittelytoimista

Laissa edellytetään usein, että yritysten on dokumentoitava ja tallennettava toimensa, jotta ne voivat osoittaa noudattavansa sääntöjä ja jotta niitä voidaan pitää vastuussa. Tärkeä esimerkki tästä on verolainsäädäntö ja -tarkastus, jotka edellyttävät kaikilta yrityksiltä kattavien asiakirjojen ylläpitämistä ja tietojen kirjaamista. Muilla lainsäädännön aloilla, erityisesti tietosuojalainsäädännössä, on myös tärkeää laatia samanlaisia vaatimuksia, koska tietojen kirjaaminen ja ylläpitäminen on tärkeä tapa helpottaa tietosuojasääntöjen noudattamista. **EU:n oikeudessa** säädetään siksi, että rekisterinpitäjien tai rekisterinpitäjien edustajien on ylläpidettävä selostetta vastuullaan olevista käsittelytoimista[471]. Tämän velvoitteen tarkoituksena on varmistaa, että tarvittaessa valvontaviranomaisilla on tarvittavat asiakirjat, joiden perusteella ne voivat vahvistaa käsittelyn lainmukaisuuden.

468 Asetuksen (EY) N:o 45/2001 24 artiklan 1 kohdassa on täydellinen luettelo tietosuojavastaavien tehtävistä.

469 Asetus (EY) N:o 45/2001, 24 artiklan 6 ja 7 kohta.

470 *Ibid.*, 25 ja 26 artikla.

471 Yleinen tietosuoja-asetus, 30 artikla.

Dokumentoitavia tietoja ovat seuraavat:

- rekisterinpitäjän ja mahdollisen yhteisrekisterinpitäjän, rekisterinpitäjän edustajan ja tietosuojavastaavan nimi ja yhteystiedot soveltuvin osin
- käsittelyn tarkoitukset
- kuvaus käsittelyyn liittyvistä rekisteröityjen ryhmistä ja henkilötietoryhmistä
- tiedot henkilötietojen vastaanottajien ryhmistä, joille henkilötietoja on luovutettu tai luovutetaan
- tiedot siitä, onko henkilötietoja siirretty tai siirretäänkö niitä kolmanteen maahan tai kansainväliselle järjestölle
- mahdollisuuksien mukaan eri tietoryhmien poistamisen suunnitellut määräajat sekä yleinen kuvaus käsittelyn turvallisuuden varmistamiseksi toteutetuista teknisistä ja organisatorisista turvatoimista[472].

Yleisen tietosuoja-asetuksen mukaan velvollisuus käsittelytoimia koskevan selosteen ylläpitämisestä koskee rekisterinpitäjien lisäksi henkilötietojen käsittelijöitä. Tämä on merkittävä edistysaskel, koska ennen asetuksen antamista rekisterinpitäjän ja henkilötietojen käsittelijän välinen sopimus koski ensisijaisesti rekisterinpitäjän velvollisuuksia. Niiden velvollisuudesta ylläpitää selostetta säädetään nyt suoraan laissa.

Yleisessä tietosuoja-asetuksessa säädetään poikkeuksesta tähän velvollisuuteen. Velvollisuus ylläpitää selostetta ei koske yritystä tai järjestöä (rekisterinpitäjää tai henkilötietojen käsittelijää), jossa on alle 250 työntekijää. Poikkeuksen soveltaminen edellyttää kuitenkin, että kyseinen järjestö ei suorita käsittelyä, joka todennäköisesti aiheuttaa riskin rekisteröidyn oikeuksille ja vapauksille, että käsittely on vain satunnaista tai että käsittely ei kohdistu 9 artiklan 1 kohdassa tarkoitettuihin erityisiin tietoryhmiin tai 10 artiklassa tarkoitettuihin rikostuomioita tai rikkomuksia koskeviin henkilötietoihin.

Käsittelytoimia koskevaa selostetta ylläpitämällä rekisterinpitäjät ja henkilötietojen käsittelijät pystyvät osoittamaan noudattavansa asetusta. Sen avulla myös

472 *Ibid.*, 30 artiklan 1 kohta.

valvontaviranomaiset pystyvät valvomaan käsittelyn lainmukaisuutta. Kun valvontaviranomainen pyytää pääsyä kyseisiin selosteisiin, rekisterinpitäjien ja henkilötietojen käsittelijöiden on tehtävä yhteistyötä ja annettava ne saataville.

4.3.3 Tietosuojaa koskeva vaikutustenarviointi ja ennakkokuuleminen

Käsittelyyn liittyy luonnostaan riskejä yksilöiden oikeuksille. Henkilötiedot voivat kadota, niitä voidaan luovuttaa luvattomille osapuolille tai niitä voidaan käsitellä lainvastaisella tavalla. Riskit tietenkin vaihtelevat käsittelyn luonteen ja laajuuden mukaan. Laajamittaisissa toimissa, joihin kuuluu arkaluonteisten henkilötietojen käsittelyä, rekisteröidyille aiheutuva riski on esimerkiksi paljon suurempi kuin mahdolliset riskit, kun pieni yritys käsittelee työntekijöidensä osoitteita ja henkilökohtaisia puhelinnumeroita.

Koska käyttöön tulee uusia tekniikoita ja käsittely mutkistuu jatkuvasti, rekisterinpitäjien on puututtava tällaisiin riskeihin selvittämällä suunnitellun käsittelyn todennäköinen vaikutus ennen käsittelytoimen aloittamista. Näin organisaatiot pystyvät asianmukaisesti määrittämään riskit, puuttumaan niihin ja pienentämään niitä etukäteen. Siten voidaan rajoittaa huomattavasti käsittelystä yksilöille aiheutuvan kielteisen vaikutuksen todennäköisyyttä.

Tietosuojaa koskevista vaikutustenarvioinneista säädetään sekä **Euroopan neuvoston että EU:n oikeudessa**. Euroopan neuvoston oikeudellisessa kehyksessä uudistetun yleissopimuksen 108 10 artiklan 2 kohdan mukaan sopimuspuolten on varmistettava, että rekisterinpitäjät ja henkilötietojen käsittelijät tutkivat suunnitellun tietojenkäsittelyn todennäköisen vaikutuksen rekisteröityjen oikeuksiin ja perusvapauksiin ennen kyseisen käsittelyn aloittamista. Arvioinnin jälkeen käsittely on suunniteltava siten, että käsittelyyn liittyvät riskit ehkäistään tai minimoidaan.

EU:n oikeudessa säädetään samankaltainen mutta yksityiskohtaisempi velvollisuus yleisen tietosuoja-asetuksen soveltamisalaan kuuluville rekisterinpitäjille. Asetuksen 35 artiklassa säädetään, että vaikutustenarviointi on tehtävä, kun käsittely todennäköisesti aiheuttaa yksilön oikeuksien ja vapauksien kannalta korkean riskin. Asetuksessa ei määritellä, miten riskin todennäköisyyttä on arvioitava, mutta siinä esitetään, mitä kyseiset riskit voisivat olla[473]. Siinä on luettelo käsittelytoimista, joiden

473 Yleinen tietosuoja-asetus, johdanto-osan 75 kappale.

riski katsotaan korkeaksi ja joissa etukäteen tehtävä vaikutustenarviointi on erityisen tarpeen. Kyse on tapauksista, joissa

- henkilötietoja käsitellään päätösten tekemiseksi luonnollisista henkilöistä yksilöihin liittyvien henkilökohtaisten ominaisuuksien järjestelmällisen ja kattavan arvioinnin perusteella (profilointi)

- arkaluonteisia tietoja tai rikostuomioihin ja rikkomuksiin liittyviä henkilötietoja käsitellään laajamittaisesti

- käsittelyyn kuuluu yleisölle avoimen alueen järjestelmällistä laajamittaista valvontaa.

Valvontaviranomaisten on laadittava ja julkaistava luettelo käsittelytoimien tyypeistä, joiden yhteydessä vaaditaan vaikutustenarviointi. Valvontaviranomaiset voivat myös laatia luettelon tästä velvollisuudesta vapautetuista käsittelytoimista.[474]

Kun vaikutustenarviointi on tehtävä, rekisterinpitäjien on arvioitava käsittelyn välttämättömyys ja oikeasuhteisuus sekä yksilöiden oikeuksille mahdollisesti aiheutuvat riskit. Vaikutustenarviointiin täytyy myös sisältyä suunnitellut suoja- ja turvallisuustoimet, joilla puututaan havaittuihin riskeihin. Luettelojen laatimista varten jäsenvaltioiden valvontaviranomaisten on tehtävä yhteistyötä toistensa ja Euroopan tietosuojaneuvoston kanssa. Näin varmistetaan koko EU:ssa yhdenmukainen lähestymistapa kyseisiin vaikutustenarviointia edellyttäviin toimiin, ja rekisterinpitäjillä on samanlaiset vaatimukset sijainnista riippumatta.

Jos vaikutustenarviointi osoittaa, että käsittely aiheuttaisi korkean riskin yksilöiden oikeuksien kannalta ja jos riskin pienentämiseksi ei ole toteutettu toimenpiteitä, rekisterinpitäjän on ennen käsittelytoimien aloittamista kuultava asianomaista valvontaviranomaista[475].

Tietosuojatyöryhmä on antanut ohjeet tietosuojaa koskevista vaikutustenarvioinneista ja siitä, miten selvitetään, aiheuttaako käsittely todennäköisesti korkean

474 *Ibid.*, 35 artiklan 4 ja 5 kohta.

475 *Ibid.*, 36 artiklan 1 kohta; tietosuojatyöryhmä (2017), *ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää "liittyykö käsittelyyn todennäköisesti" asetuksessa (EU) 2016/679 tarkoitettu "korkea riski"*, WP 248 rev.01, Bryssel, 4.10.2017.

riskin[476]. Se on laatinut yhdeksän kriteeriä, jotka auttavat määrittämään, tarvitaanko tietyssä tapauksessa tietosuojaa koskevaa vaikutustenarviointia:[477] 1) arviointi tai pisteytys, 2) automaattinen päätöksenteko, jolla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia, 3) järjestelmällinen valvonta, 4) arkaluontoiset tiedot tai luonteeltaan hyvin henkilökohtaiset tiedot, 5) tietojen laajamittainen käsittely, 6) tietokokonaisuuksien sovittaminen yhteen tai yhdistäminen, 7) heikossa asemassa olevia rekisteröityjä koskevat tiedot, 8) uusien teknisten tai organisatoristen ratkaisujen innovatiivinen käyttö tai soveltaminen, 9) tapaukset, joissa itse käsittelytoimet ”estävät rekisteröityjä käyttämästä oikeutta tai palvelua tai sopimusta”. Tietosuojatyöryhmän nyrkkisäännön mukaan alle kaksi kriteeriä täyttävissä käsittelytoimissa riskitaso on matalampi eivätkä ne edellytä tietosuojaa koskevaa vaikutustenarviointia, kun taas vähintään kaksi kriteeriä täyttävät toimet edellyttävät sitä. Tapauksissa, joissa ei ole selvää, vaaditaanko tietosuojaa koskeva vaikutustenarviointi, tietosuojatyöryhmä suosittelee sen tekemistä joka tapauksessa, koska ”se auttaa rekisterinpitäjiä noudattamaan tietosuojalainsäädäntöä”[478]. Tietosuojaa koskevan vaikutustenarvioinnin tekeminen on erityisen tärkeää silloin, kun otetaan käyttöön uutta henkilötietojen käsittelytekniikkaa[479].

4.3.4 Käytännesäännöt

Useilla toimialoilla käytetään käytännesääntöjä, joissa esitetään ja yksilöidään yleisen tietosuoja-asetuksen soveltaminen näillä nimenomaisilla aloilla. Rekisterinpitäjien ja henkilötietojen käsittelijöiden kannalta näiden sääntöjen laatiminen voi parantaa huomattavasti sääntöjen noudattamista ja edistää EU:n tietosuojasääntöjen täytäntöönpanoa. Alan jäsenten asiantuntemus auttaa löytämään ratkaisuja, jotka ovat käytännöllisiä ja joita siksi todennäköisesti kannattaa noudattaa. Yleisessä tietosuoja-asetuksessa tunnustetaan käytännesääntöjen merkitys tietosuojalainsäädännön tehokkaassa soveltamisessa ja kehotetaan jäsenvaltioita, valvontaviranomaisia, tietosuojaneuvostoa ja komissiota edistämään sellaisten käytännesääntöjen laatimista, joiden avulla tuetaan asetuksen asianmukaista soveltamista koko EU:ssa[480]. Käytännesäännöissä voidaan yksilöidä asetuksen soveltaminen

476 Tietosuojatyöryhmä (2017), *ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää ”liittyykö käsittelyyn todennäköisesti” asetuksessa (EU) 2016/679 tarkoitettu ”korkea riski”*, WP 248 rev.01, Bryssel, 4.10.2017.

477 *Ibid.*, s. 10–12.

478 *Ibid.*, s. 9.

479 *Ibid.*

480 Yleinen tietosuoja-asetus, 40 artiklan 1 kohta.

nimenomaisilla aloilla, muun muassa henkilötietojen keräämisen, rekisteröidyille ja yleisölle annettavien tietojen ja rekisteröityjen oikeuksien käyttämisen osalta.

Käytännesäännöt on toimitettava toimivaltaiselle valvontaviranomaiselle ennen niiden hyväksymistä, jotta voidaan varmistaa, että niissä noudatetaan yleisellä tietosuoja-asetuksella vahvistettuja sääntöjä. Valvontaviranomainen antaa lausunnon siitä, onko käytännesääntöjen luonnos asetuksen mukainen, ja hyväksyy käytännesäännöt, jos se katsoo niiden tarjoavan riittävät asianmukaiset suojatoimet.[481] Valvontaviranomaisten on julkaistava hyväksytyt käytännesäännöt sekä kriteerit, joihin hyväksyntä perustui. Jos käytännesääntöjen luonnos liittyy käsittelytoimiin useissa eri jäsenvaltioissa, toimivaltainen valvontaviranomainen toimittaa sen ennen käytännesääntöjen, muutoksen tai laajennuksen hyväksymistä tietosuojaneuvostolle, joka antaa lausunnon siitä, onko se yleisen tietosuoja-asetuksen mukainen. Komissio voi antaa täytäntöönpanosäädöksiä, joissa se toteaa, että hyväksytyt käytännesäännöt ovat yleisesti päteviä unionissa.

Käytännesääntöjen noudattamisesta on merkittäviä etuja sekä rekisteröidyille että rekisterinpitäjille ja henkilötietojen käsittelijöille. Käytännesäännöistä saadaan yksityiskohtaisia ohjeita, joilla oikeudellista vaatimusta voidaan muokata nimenomaisten alojen mukaan ja joiden avulla voidaan lisätä käsittelytoimien läpinäkyvyyttä. Noudattamalla käytännesääntöjä rekisterinpitäjät ja henkilötietojen käsittelijät voivat myös osoittaa noudattavansa EU:n lainsäädäntöä sekä parantaa julkisuuskuvaansa organisaatioina, jotka ovat sitoutuneet asettamaan tietosuojan etusijalle toimissaan. Hyväksyttyjä käytännesääntöjä voidaan yhdessä sitovien ja täytäntöönpanokelpoisten sitoumusten kanssa pitää asianmukaisina takeina tietojen siirtämisessä kolmansiin maihin. Käytännesääntöjen tosiasiallisen noudattamisen varmistamiseksi organisaatiossa voidaan nimetä erityiselin (jonka asianomainen valvontaviranomainen akkreditoi), joka valvoo sääntöjen noudattamista ja varmistaa sen. Tehtävien tehokas täyttäminen edellyttää, että elin on riippumaton, sillä on todistettua asiantuntemusta käytännesäännöillä säänneltävistä asioista ja sillä on käytössä avoimet menettelyt ja rakenteet käytännesääntöjen rikkomisia koskevien valitusten käsittelemiseksi.[482]

Euroopan neuvoston oikeudessa uudistetun yleissopimuksen 108 mukaan jäsenvaltioiden lainsäädännössä vahvistettua tietosuojan tasoa voidaan parantaa vapaaehtoisilla sääntelytoimenpiteillä, kuten hyvän käytännön säännöillä ja

481 *Ibid.*, 40 artiklan 5 kohta.

482 *Ibid.*, 41 artiklan 1 ja 2 kohta.

ammattieettisillä säännöillä. Ne ovat kuitenkin vain vapaaehtoisia toimenpiteitä uudistetun yleissopimuksen 108 mukaan. Niistä ei voida johtaa oikeudellista velvoitetta ottaa kyseisiä toimenpiteitä käyttöön, vaikka se onkin suositeltavaa. Nämä toimenpiteet eivät myöskään yksinään riitä varmistamaan riittävästi yleissopimuksen täydellistä noudattamista.[483]

4.3.5 Sertifiointi

Käytännesääntöjen lisäksi sertifiointimekanismit sekä tietosuojasinetit ja -merkit ovat toinen keino, jolla rekisterinpitäjät ja henkilötietojen käsittelijät voivat osoittaa noudattavansa yleistä tietosuoja-asetusta. Tämän takia asetuksessa säädetään vapaaehtoisesta sertifiointijärjestelmästä, jossa tietyt elimet ja valvontaviranomaiset voivat myöntää sertifiointeja. Rekisterinpitäjät ja henkilötietojen käsittelijät, jotka päättävät liittyä sertifiointimekanismiin, voivat lisätä näkyvyyttään ja uskottavuuttaan, koska rekisteröidyt pystyvät sertifiointien, sinettien ja merkkien avulla arvioimaan nopeasti organisaation tietojenkäsittelyn suojan tason. On kuitenkin huomattava, että tällaisen sertifioinnin hallussapito ei vähennä rekisterinpitäjän tai henkilötietojen käsittelijän tehtäviä ja velvollisuuksia asetuksen kaikkien vaatimusten noudattamisessa.

4.4 Sisäänrakennettu ja oletusarvoinen tietosuoja

Sisäänrakennettu tietosuoja

EU:n oikeudessa edellytetään, että rekisterinpitäjä ottaa käyttöön tietosuojaperiaatteiden tehokasta täytäntöönpanoa koskevat toimenpiteet ja sisällyttää niihin tarvittavat suojatoimet, jotta käsittely vastaisi asetuksen vaatimuksia ja rekisteröityjen oikeuksia suojattaisiin[484]. Nämä toimenpiteet on toteutettava sekä itse käsittelyn että käsittelytapojen määrittämisen yhteydessä. Toimenpiteitä toteuttaessaan rekisterinpitäjän on otettava huomioon uusin tekniikka,

483 Uudistettu yleissopimus 108, selitysmuistio, 33 kohta.

484 Yleinen tietosuoja-asetus, 25 artiklan 1 kohta.

täytäntöönpanokustannukset, henkilötietojen käsittelyn luonne, laajuus ja tarkoitukset sekä rekisteröidyn oikeuksille ja vapauksille aiheutuvat riskit ja niiden vakavuus[485].

Euroopan neuvoston oikeudessa edellytetään, että rekisterinpitäjät ja henkilötietojen käsittelijät arvioivat henkilötietojen käsittelyn todennäköisen vaikutuksen rekisteröityjen oikeuksiin ja vapauksiin ennen käsittelyn aloittamista. Rekisterinpitäjien ja henkilötietojen käsittelijöiden on myös suunniteltava tietojenkäsittely siten, että ehkäistään tai minimoidaan riski kyseisiin oikeuksiin ja vapauksiin puuttumisesta, ja niiden on toteutettava teknisiä ja organisatorisia toimenpiteitä, joissa otetaan huomioon vaikutukset henkilötietojen suojaa koskevaan oikeuteen kaikissa tietojenkäsittelyn vaiheissa.[486]

Oletusarvoinen tietosuoja

EU:n oikeuden mukaan rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet, joilla varmistetaan, että oletusarvoisesti käsitellään vain käsittelyn kunkin erityisen tarkoituksen kannalta tarpeellisia henkilötietoja. Tämä velvollisuus koskee kerättyjen henkilötietojen määriä, käsittelyn laajuutta, säilytysaikaa ja saatavilla oloa.[487] Näiden toimenpiteiden avulla on varmistettava esimerkiksi se, että rekisteröityjen henkilötiedot eivät ole rekisterinpitäjien kaikkien työntekijöiden saatavilla. Lisäohjeita on Euroopan tietosuojavaltuutetun tarpeellisuutta koskevissa ohjeissa (*Necessity Toolkit*)[488].

Euroopan neuvoston oikeuden mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on toteutettava teknisiä ja organisatorisia toimenpiteitä, joiden avulla voidaan ottaa huomioon vaikutukset tietosuojaa koskevaan oikeuteen, ja niiden on toteutettava teknisiä ja organisatorisia toimenpiteitä, joissa otetaan huomioon vaikutukset henkilötietojen suojaa koskevaan oikeuteen kaikissa tietojenkäsittelyn vaiheissa[489].

485 Ks. tietosuojatyöryhmä (2017), *ohjeet tietosuojaa koskevasta vaikutustenarvioinnista ja keinoista selvittää "liittyykö käsittelyyn todennäköisesti" asetuksessa (EU) 2016/679 tarkoitettu "korkea riski*, WP 248 rev.01, 4.10.2017. Ks. myös ENISA (2015), Privacy and Data Protection by Design-from policy to engineering, 12.1.2015.

486 Uudistettu yleissopimus 108, 10 artiklan 2 ja 3 alakohta, uudistettu yleissopimus 108, selitysmuistio, 89 kohta.

487 Yleinen tietosuoja-asetus, 25 artiklan 2 kohta.

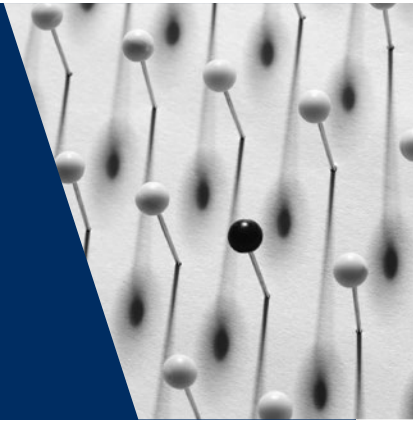
488 Euroopan tietosuojavaltuutettu (EDPS), (2017), *Necessity Toolkit*, Bryssel, 11.4.2017.

489 Uudistettu yleissopimus 108, 10 artiklan 3 kohta, uudistettu yleissopimus 108, selitysmuistio, 89 kohta.

ENISA julkaisi vuonna 2016 raportin saatavilla olevista yksityisyydensuojaa koskevista työkaluista ja palveluista[490]. Tässä arvioinnissa on muun muassa laadittu hakemisto kriteereistä ja muuttujista, joita voidaan käyttää hyvien tai huonojen yksityisyydensuojaa koskevien käytäntöjen indikaattoreina. Jotkin kriteerit liittyvät suoraan yleisen tietosuoja-asetuksen säännöksiin – kuten pseudonymisoinnin ja hyväksyttyjen sertifiointimekanismien käyttö – kun taas toisista saa innovatiivisia aloitteita sisäänrakennetun ja oletusarvoisen yksityisyydensuojan varmistamiseen. Esimerkiksi käytettävyyden kriteeri ei liity suoraan yksityisyydensuojaan, mutta sillä voidaan edistää yksityisyydensuojaa, koska sen ansiosta yksityisyydensuojaa koskeva työkalu tai palvelu voidaan ottaa käyttöön aiempaa laajemmin. Suuri yleisö käyttääkin hyvin vähän yksityisyydensuojaa koskevia työkaluja, joiden käytännön täytäntöönpano on vaikeaa, vaikka ne tarjoavat erittäin vahvat takeet yksityisyydensuojalle. Ratkaisevan tärkeä on myös yksityisyydensuojaa koskevan työkalun kypsyyttä ja vakautta mittaava kriteeri. Sillä arvioidaan, miten työkalu kehittyy ajan myötä ja miten se reagoi nykyisiin tai uusiin yksityisyydensuojaan liittyviin haasteisiin. Muita yksityisyydensuojaa edistäviä tekniikoita esimerkiksi suojatun viestinnän yhteydessä ovat päästä päähän -salaus (viestintä, jossa viestejä pystyvät lukemaan vain viestivät ihmiset), asiakas–palvelin-salaus (asiakkaan ja palvelimen välille luodun viestintäkanavan salaus), todentaminen (viestinnän osapuolten henkilöllisyyksien tarkastaminen) ja anonyymi viestintä (kolmas osapuoli ei pysty tunnistamaan viestinnän osapuolia).

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20.12.2016.

5 Riippumaton valvonta



EU	Käsiteltävät asiat	EN
Perusoikeuskirja, 8 artiklan 3 kohta Euroopan unionin toiminnasta tehty sopimus, 16 artiklan 2 kohta Yleinen tietosuoja-asetus, 51–59 artikla EUT, C-518/07, *Euroopan komissio vastaan Saksan liittotasavalta* [suuri jaosto], 2010 EUT, C-614/10, *Euroopan komissio vastaan Itävallan tasavalta* [suuri jaosto], 2012 EUT, C-288/12, *Euroopan komissio vastaan Unkari* [suuri jaosto], 2014 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 2015	**Valvontaviranomaiset**	Uudistettu yleissopimus 108, 15 artikla
Yleinen tietosuoja-asetus, 60–67 artikla	**Valvontaviranomaisten välinen yhteistyö**	Uudistettu yleissopimus 108, 16–21 artikla
Yleinen tietosuoja-asetus, 68–76 artikla	**Euroopan tietosuojaneuvosto**	

Keskeiset kohdat

- Riippumaton valvonta on Euroopan tietosuojalainsäädännön olennainen osa, joka vahvistetaan perusoikeuskirjan 8 artiklan 3 kohdassa.
- Tehokkaan tietosuojan varmistamiseksi kansallisessa lainsäädännössä on säädettävä riippumattoman valvontaviranomaisen perustamisesta.
- Kansallisten valvontaviranomaisten on oltava toiminnassaan täysin riippumattomia. Tämä on taattava niiden perustamisesta annettavalla lailla ja tuotava esiin valvontaviranomaisen organisaatiorakenteessa.
- Valvontaviranomaisilla on erityisiä valtuuksia ja tehtäviä, muun muassa seuraavat:
  - tietosuojan seuraaminen ja edistäminen kansallisella tasolla
  - rekisteröityjen ja rekisterinpitäjien sekä julkisen hallinnon ja suuren yleisön neuvominen
  - valitusten vastaanottaminen ja rekisteröityjen avustaminen tietosuojaa koskevien oikeuksien väitetyissä rikkomistapauksissa
  - rekisterinpitäjien ja henkilötietojen käsittelijöiden valvominen.
- Valvontaviranomaisilla on myös oikeus tarvittaessa puuttua tilanteisiin
  - antamalla rekisterinpitäjille ja henkilötietojen käsittelijöille huomautuksia tai varoituksia ja jopa sakkoja
  - määräämällä tietoja oikaistaviksi, suojattaviksi tai poistettaviksi
  - kieltämällä käsittely tai määräämällä hallinnollinen sakko
  - saattamalla asia tuomioistuimen käsiteltäväksi.
- Koska henkilötietojen käsittelyssä on usein mukana eri valtioissa sijaitsevia rekisterinpitäjiä, henkilötietojen käsittelijöitä ja rekisteröityjä, valvontaviranomaisten on tehtävä rajatylittävissä asioissa keskenään yhteistyötä, jotta yksilöiden tehokas suojelu Euroopassa voidaan varmistaa.
- EU:n yleisellä tietosuoja-asetuksella luodaan yhden luukun järjestelmä rajatylittäviä tapauksia varten. Jotkin yritykset suorittavat rajatylittäviä käsittelytoimia, koska ne käsittelevät henkilötietoja useammassa kuin yhdessä jäsenvaltiossa sijaitsevien toimipaikkojen toimien yhteydessä, tai ne käsittelevät tietoja unionissa sijaitsevassa yhdessä toimipaikassa, mutta se vaikuttaa merkittävästi rekisteröityihin useammassa kuin yhdessä jäsenvaltiossa. Mekanismissa näiden yritysten tarvitsee toimia vain yhden kansallisen tietosuojan valvontaviranomaisen kanssa.

- Yhteistyö- ja yhdenmukaisuusmekanismin ansiosta kaikki tapauksessa mukana olevat valvontaviranomaiset pystyvät toimimaan koordinoidusti. Johtava valvontaviranomainen (päätoimipaikassa tai ainoassa toimipaikassa) kuulee muita asianomaisia valvontaviranomaisia ja toimittaa päätösehdotuksensa niille.
- Nykyisen tietosuojatyöryhmän mukaan kunkin jäsenvaltion valvontaviranomainen ja Euroopan tietosuojavaltuutettu (EDPS) kuuluvat Euroopan tietosuojaneuvostoon.
- Tietosuojaneuvoston tehtävänä on muun muassa seurata asetuksen asianmukaista soveltamista, antaa komissiolle neuvoja asiaankuuluvista kysymyksistä ja antaa suuntaviivoja, suosituksia tai parhaita käytänteitä eri aiheista.
- Suurin ero on se, että Euroopan tietosuojaneuvosto ei anna pelkästään lausuntoja, kuten direktiivin 95/46/EY nojalla. Se antaa myös sitovia päätöksiä, jos valvontaviranomainen on esittänyt merkityksellisen ja perustellun vastalauseen yhden luukun järjestelmää koskevissa tapauksissa, jos esiintyy eriäviä näkemyksiä siitä, mikä valvontaviranomaisista on johtava valvontaviranomainen, ja jos toimivaltainen valvontaviranomainen ei pyydä tietosuojaneuvostolta lausuntoa tai ei noudata sen antamaa lausuntoa. Tavoitteena on varmistaa asetuksen yhdenmukainen soveltaminen kaikissa jäsenvaltioissa.

Riippumaton valvonta on olennainen osa Euroopan tietosuojalainsäädäntöä. Sekä EU:n että Euroopan neuvoston oikeudessa riippumattomat valvontaviranomaiset katsotaan välttämättömiksi, jotta yksilöiden oikeuksia ja vapauksia voidaan suojella tehokkaasti heidän henkilötietojensa käsittelyssä. Koska henkilötietoja käsitellään kaikkialla ja yksilöiden on entistä vaikeampaa ymmärtää sitä, nämä viranomaiset ovat digitaaliajan vahtikoiria. EU:ssa riippumattomat valvontaviranomaiset katsotaan yhdeksi henkilötietojen suojaa koskevan oikeuden olennaisimmista tekijöistä, ja niiden toiminta on vahvistettu EU:n primaarilainsäädännössä. Euroopan unionin perusoikeuskirjan 8 artiklan 3 kohdassa ja SEUT-sopimuksen 16 artiklan 2 kohdassa henkilötietojen suoja tunnustetaan perusoikeudeksi ja vahvistetaan, että riippumattoman viranomaisen on valvottava tietosuojasääntöjen noudattamista.

Tietosuojalainsäädännön riippumattoman valvonnan merkitys on tunnustettu myös oikeuskäytännössä.

Esimerkki: Asiassa *Schrems*[491] Euroopan unionin tuomioistuin pohti, onko henkilötietojen siirtäminen Yhdysvaltoihin ensimmäisen EU:n ja Yhdysvaltojen välisen safe harbor -sopimuksen nojalla EU:n tietosuojalainsäädännön mukaista, kun otetaan huomioon Edward Snowdenin tekemät paljastukset

491 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

Yhdysvaltojen National Security Agencyn (NSA) harjoittamasta joukkovalvonnasta. Henkilötietojen siirtäminen Yhdysvaltoihin perustui Euroopan komission vuonna 2000 tekemään päätökseen, jonka nojalla tietoja voitiin siirtää EU:sta yhdysvaltalaisille yrityksille, jotka ilmoittavat noudattavansa niin sanottuja safe harbor -periaatteita, joilla varmistetaan henkilötietojen suojan riittävä taso. Irlannin valvontaviranomaista pyydettiin tutkimaan kantajan kantelu tietojen siirtämisen laillisuudesta Snowdenin paljastusten jälkeen. Valvontaviranomainen hylkäsi kantelun sillä perusteella, että safe harbor -periaatteiden perustana oleva komission päätös Yhdysvaltojen tietosuojajärjestelmän riittävyydestä (ns. safe harbor -päätös) esti sitä tutkimasta kantelua edelleen.

Euroopan unionin tuomioistuin katsoi kuitenkin, että komission päätös, jonka nojalla sallitaan tietojen siirrot kolmansiin maihin, jotka varmistavat tietosuojan riittävän tason, ei tee tyhjäksi eikä heikennä kansallisten valvontaviranomaisten toimivaltaa. Tuomioistuin pani merkille, että viranomaisten toimivalta seurata EU:n tietosuojasääntöjen noudattamista ja varmistaa se perustuu unionin primaarioikeuteen, muun muassa perusoikeuskirjan 8 artiklan 3 kohtaan ja SEUT-sopimuksen 16 artiklan 2 kohtaan. ”Itsenäisten valvontaviranomaisten perustaminen jäsenvaltioissa on siis […] keskeinen tekijä yksilöiden suojelussa henkilötietojen käsittelyssä”[492].

Näin ollen unionin tuomioistuin päätti, että silloinkin, kun komissio on tehnyt henkilötietojen siirtämisestä tietosuojan riittävyyttä koskevan päätöksen, kun kantelu on saatettu kansallisen valvontaviranomaisen käsiteltäväksi, viranomaisen on tutkittava kantelu huolellisesti. Viranomainen voi hylätä kantelun, jos se katsoo sen perusteettomaksi. Sellaisessa tapauksessa tuomioistuin korosti oikeuden tehokkaisiin oikeussuojakeinoihin edellyttävän, että henkilöillä on oltava mahdollisuus riitauttaa kyseinen päätös kansallisissa tuomioistuimissa, jotka voivat saattaa asian unionin tuomioistuimen käsiteltäväksi ja pyytää ennakkoratkaisua komission päätöksen pätevyydestä. Jos valvontaviranomainen taas pitää kantelua perusteltuna, sen on voitava olla asianosaisena oikeudenkäynnissä ja sen on voitava saattaa asia kansallisten tuomioistuinten käsiteltäväksi. Kansalliset tuomioistuimet voivat

492 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015, 41 kohta.

saattaa asian Euroopan unionin tuomioistuimen käsiteltäväksi, koska se on ainoa elin, jolla on toimivalta tehdä päätös tietosuojan tason riittävyydestä tehdyn komission päätöksen pätevyydestä.[493]

Euroopan unionin tuomioistuin tutki seuraavaksi safe harbor -päätöksen pätevyyttä voidakseen selvittää, onko siirtojärjestelmä EU:n tietosuojasääntöjen mukainen. Se totesi, että safe harbor -päätöksen 3 artiklassa rajoitettiin kansallisten valvontaviranomaisten toimivaltaa (joka myönnettiin tietosuojadirektiivissä) ryhtyä toimenpiteisiin tietosiirtojen estämiseksi, jos henkilötietojen suojan taso Yhdysvalloissa olisi riittämätön. Koska riippumattomat valvontaviranomaiset ovat tärkeitä tietosuojalainsäädännön noudattamisen varmistamisessa, Euroopan unionin tuomioistuin totesi, että tietosuojadirektiivin nojalla ja luettuna perusoikeuskirjan valossa komissiolla ei ollut toimivaltaa rajoittaa riippumattomien valvontaviranomaisten toimivaltaa tällä tavalla. Valvontaviranomaisten toimivallan rajoittaminen oli yksi syy sille, miksi Euroopan unionin tuomioistuin totesi safe harbor -päätöksen pätemättömäksi.

EU:n oikeudessa edellytetään näin ollen riippumatonta valvontaa tehokkaan tietosuojan varmistamisen tärkeänä mekanismina. Riippumattomat valvontaviranomaiset ovat rekisteröityjen ensimmäinen yhteyspiste yksityisyydensuojan loukkauksia koskevissa tapauksissa[494]. Valvontaviranomaisten perustaminen on pakollista sekä EU:n että Euroopan neuvoston oikeudessa. Molemmissa oikeudellisissa kehyksissä viranomaisten tehtävät ja toimivalta kuvataan samalla tavalla kuin yleisessä tietosuoja-asetuksessa. Valvontaviranomaisten pitäisi siis periaatteessa toimia samalla tavalla EU:n oikeuden ja Euroopan neuvoston oikeuden nojalla.[495]

5.1 Riippumattomuus

Sekä **EU:n** että **Euroopan neuvoston oikeudessa** edellytetään, että kukin valvontaviranomainen toimii täysin riippumattomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan[496]. Valvontaviranomaisen ja sen jäsenten sekä henkilöstön riippumattomuus suorista tai välillisistä ulkopuolisista vaikutuksista on olennaisen tärkeää,

493 *Ibid.*, 53–66 kohta.

494 Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan d alakohta.

495 *Ibid.*, 51 artikla; uudistettu yleissopimus 108, 15 artikla.

496 Yleinen tietosuoja-asetus, 52 artiklan 1 kohta, uudistettu yleissopimus 108, 15 artiklan 5 kohta.

jotta tietosuoja-asioista päätettäessä voidaan taata täydellinen puolueettomuus. Ei riitä, että valvontaelimen perustamisesta annettava laki sisältää erityiset säännökset, joilla taataan riippumattomuus, vaan viranomaisen organisaatiorakenteen on ilmennettävä riippumattomuutta. Euroopan unionin tuomioistuin käsitteli vuonna 2010 ensimmäisen kerran tietosuojan valvontaviranomaisten riippumattomuutta koskevan vaatimuksen laajuutta[497]. Seuraavat esimerkit havainnollistavat sen tästä asiasta tekemää tulkintaa.

Esimerkki: Asiassa *Euroopan komissio vastaan Saksan liittotasavalta*[498] Euroopan komissio oli pyytänyt unionin tuomioistuinta toteamaan, että Saksa oli pannut virheellisesti täytäntöön tietosuojasta vastaavien valvontaviranomaisten ”täydellistä itsenäisyyttä” koskevan vaatimuksen ja siten jättänyt noudattamatta tietosuojadirektiivin 28 artiklan kohdan mukaisia velvoitteitaan. Komissio katsoi, että Saksan eri osavaltioissa (*Länder*) henkilötietojen käsittelyä valvovien valvontaviranomaisten asettaminen valtion valvonnan alaisuuteen tietosuojalainsäädännön noudattamisen varmistamiseksi on itsenäisyyttä koskevan vaatimuksen vastaista.

Tuomioistuin toi esiin, että ilmaisun ”itsenäisesti” tulkinnassa oli otettava huomioon sekä säännöksen sanamuoto että EU:n tietosuojalainsäädännön tavoitteet ja rakenne[499]. Tuomioistuin painotti, että valvontaviranomaiset ovat henkilötietojen käsittelyn alalla taattujen oikeuksien ”vartijoita” ja että niiden perustamista jäsenvaltioissa pidetään ”keskeisenä tekijänä yksilöiden suojelussa henkilötietojen käsittelyssä”[500]. Tuomioistuin totesi, että ”valvontaviranomaisten on tehtäviään hoitaessaan toimittava objektiivisesti ja puolueettomasti. Tässä tarkoituksessa niiden on oltava suojattuna kaikelta ulkopuoliselta vaikuttamiselta, myös suoralta tai välilliseltä vaikuttamiselta valtion tai osavaltioiden taholta, ei ainoastaan valvottavien elinten taholta.”[501]

497 FRA (2010), *Perusoikeudet: Haasteet ja saavutukset vuonna 2010*, Vuosikertomus 2010, s. 59. FRA: *Data protection in the European Union: the role of National Data Protection Authorities*, toukokuu 2010.

498 EUT, C-518/07, *Euroopan komissio vastaan Saksan liittotasavalta* [suuri jaosto], 9.3.2010, 27 kohta.

499 *Ibid.*, 17 ja 29 kohta.

500 *Ibid.*, 23 kohta.

501 *Ibid.*, 25 kohta.

Euroopan unionin tuomioistuin katsoi lisäksi, että ilmaisun ”itsenäisesti” tulkinnassa oli otettava huomioon Euroopan tietosuojavaltuutetun riippumattomuus, sellaisena kuin se määritellään EU:n toimielinten tietosuoja-asetuksessa. Kyseisen asetuksen mukaan riippumattomuuden käsite edellyttää, että Euroopan tietosuojavaltuutettu ei pyydä eikä ota ohjeita miltään taholta.

Edellä esitetyn perusteella tuomioistuin totesi, että Saksan valvontaviranomaiset eivät olleet itsenäisiä EU:n tietosuojalainsäädännössä tarkoitetulla tavalla, koska ne olivat valtion valvonnan alaisia.

Esimerkki: Asiassa *Euroopan komissio vastaan Itävallan tasavalta*[502] Euroopan unionin tuomioistuin toi esiin samankaltaisia ongelmia Itävallan tietosuojaviranomaisen (Datenschutzkommission, DSK) tiettyjen jäsenten ja henkilöstön asemassa. Tuomioistuin katsoi, että valvontaviranomaisen itsenäisyyttä ei ollut turvattu EU:n tietosuojalainsäädännössä tarkoitetulla tavalla, koska liittokanslerinvirasto palkkasi valvontaviranomaisen työntekijät. Tuomioistuin totesi myös, että valvontaviranomaisen itsenäisyyttä heikensi myös vaatimus tiedottaa jatkuvasti liittokanslerinvirastolla sen työstä.

Esimerkki: Asiassa *Euroopan komissio vastaan Unkari*[503] kiellettiin samankaltaisia kansallisia käytäntöjä, jotka vaikuttavat työntekijöiden itsenäisyyteen. Euroopan unionin tuomioistuin huomautti, että ”vaatimus, jonka mukaan on taattava, että kukin valvontaviranomainen hoitaa täysin itsenäisesti sille annettuja tehtäviä, [edellyttää,] sitä, että kyseinen jäsenvaltio kunnioittaa tällaisen viranomaisen toimikauden kestoa sen alun perin määritettyyn loppuun saakka”. Tuomioistuin katsoi myös, että ”Unkari ei ole noudattanut [...] direktiivin 95/46/EY mukaisia velvoitteitaan, koska se on päättänyt henkilötietojen suojaa valvovan viranomaisen toimikauden ennenaikaisesti”.

Käsitteestä ”täysin riippumattomasti” ja sitä koskevista kriteereistä säädetään nyt yksiselitteisesti yleisessä tietosuoja-asetuksessa, ja se sisältää Euroopan unionin tuomioistuimen edellä mainituilla tuomioilla vahvistetut periaatteet. Asetuksen mukaan tehtävien hoitaminen ja toimivallan käyttäminen täysin riippumattomasti tarkoittaa, että[504]

502 EUT, C-614/10, *Euroopan komissio vastaan Itävallan tasavalta* [suuri jaosto], 16.10.2012, 59 ja 63 kohta.

503 EUT, C-288/12, *Euroopan komissio vastaan Unkari* [suuri jaosto], 8.4.2014, 50 ja 67 kohta.

504 Yleinen tietosuoja-asetus, 69 artikla.

- minkään valvontaviranomaisen jäseniin ei saa vaikuttaa ulkopuolelta suoraan eikä välillisesti eivätkä he saa pyytää eivätkä ottaa ohjeita miltään taholta

- kunkin valvontaviranomaisen jäsenten on pidättäydyttävä kaikesta toiminnasta, joka ei sovi yhteen heidän tehtäviensä hoitamisen kanssa, eturistiriitojen estämiseksi

- jäsenvaltioiden on osoitettava jokaiselle valvontaviranomaiselle tekniset, taloudelliset ja henkilöresurssit, tilat ja infrastruktuuri, jotka ovat tarpeen tehtävien suorittamiseksi tehokkaasti

- jäsenvaltioiden on varmistettava, että kukin valvontaviranomainen valitsee oman henkilöstönsä

- jokaiseen valvontaviranomaiseen kansallisen lainsäädännön nojalla sovellettava varainhoidon valvonta ei saa vaikuttaa sen riippumattomuuteen. Valvontaviranomaisilla on oltava erilliset julkiset vuotuiset talousarviot, jotka takaavat niiden moitteettoman toiminnan.

Valvontaviranomaisten riippumattomuus katsotaan keskeiseksi vaatimukseksi myös Euroopan neuvoston oikeudessa. Uudistetun yleissopimuksen 108 mukaan valvontaviranomaisten on toimittava täysin riippumattomasti ja puolueettomasti hoitaessaan tehtäviään ja käyttäessään valtuuksiaan eivätkä ne saa pyytää tai vastaanottaa ohjeita[505]. Näin yleissopimuksessa tunnustetaan, että kyseiset viranomaiset pystyvät turvaamaan tietojenkäsittelyyn liittyvät yksilöiden oikeudet ja vapaudet tehokkaasti vain, jos ne hoitavat tehtäviään täysin riippumattomasti. Uudistetun yleissopimuksen 108 selitysmuistiossa esitetään useita seikkoja, joilla edistetään tämän riippumattomuuden takaamista. Niitä ovat muun muassa valvontaviranomaisten mahdollisuus palkata oma henkilöstönsä ja tehdä päätöksiä altistumatta ulkopuoliselle vaikutukselle sekä tekijät, jotka liittyvät tehtävien hoitamisen kestoon sekä ehtoihin, joiden nojalla tehtävän hoitamisen voi lopettaa.[506]

5.2 Toimivalta ja valtuudet

EU:n oikeudessa yleisessä tietosuoja-asetuksessa esitetään valvontaviranomaisten toimivalta ja organisaatiorakenne sekä säädetään, että niiden on oltava

505 Uudistettu yleissopimus 108, 15 artiklan 5 kohta.

506 Uudistetun yleissopimuksen 108 selitysmuistio.

toimivaltaisia ja niillä on oltava valtuudet suorittaa asetuksessa vaaditut tehtävät. Valvontaviranomainen on kansallisessa lainsäädännössä keskeinen elin, joka varmistaa EU:n tietosuojalainsäädännön noudattamisen. Valvontaviranomaisilla on seurannan lisäksi kattava valikoima tehtäviä ja valtuuksia, joihin kuuluu ennakoivia ja ennalta ehkäiseviä valvontatoimia. Näiden tehtävien suorittamiseksi valvontaviranomaisilla on oltava yleisen tietosuoja-asetuksen 57 ja 58 artiklassa luetellut asianmukaiset tutkintavaltuudet, korjaavat toimivaltuudet ja neuvontavaltuudet, muun muassa valtuudet[507]

- antaa rekisterinpitäjille ja rekisteröidyille neuvoja kaikista tietosuojaan liittyvistä asioista
- hyväksyä sopimuslausekkeita, yritystä koskevia sitovia sääntöjä tai hallinnollisia järjestelyjä
- tutkia käsittelytoimia ja puuttua niihin
- vaatia toimittamaan kaikki rekisterinpitäjän toimien valvontaa varten tarvittavat tiedot
- antaa varoitus tai huomautus rekisterinpitäjille ja määrätä lähettämään ilmoitus henkilötietojen tietoturvaloukkauksesta rekisteröidyille
- määrätä tietojen oikaisusta, suojaamisesta, poistamisesta tai tuhoamisesta
- asettaa väliaikainen tai pysyvä rajoitus käsittelylle tai määrätä hallinnollisia sakkoja
- saattaa asia tuomioistuimen käsiteltäväksi.

Voidakseen hoitaa tehtäviään valvontaviranomaisella on oltava mahdollisuus tutustua kaikkiin selvityksen kannalta tarpeellisiin henkilötietoihin ja muihin tietoihin sekä päästä kaikkiin tiloihin, joissa rekisterinpitäjä säilyttää asiaa koskevia tietoja. Euroopan unionin tuomioistuimen mukaan valvontaviranomaisen valtuuksia on tulkittava laajasti, jotta rekisteröityjen tietosuojan täydellinen toimivuus EU:ssa voidaan varmistaa.

507 Yleinen tietosuoja-asetus, 57 ja 58 artikla. Ks. myös yleissopimus 108, lisäpöytäkirja, 1 artikla.

Esimerkki: Asiassa *Schrems* Euroopan unionin tuomioistuin pohti, onko henkilötietojen siirtäminen Yhdysvaltoihin ensimmäisen EU:n ja Yhdysvaltojen välisen safe harbor -sopimuksen nojalla EU:n tietosuojalainsäädännön mukaista, kun otetaan huomioon Edward Snowdenin tekemät paljastukset. Euroopan unionin tuomioistuimen perusteluissa katsottiin, että kansalliset valvontaviranomaiset voivat – toimiessaan rekisterinpitäjien suorittaman tietojenkäsittelyn itsenäisinä valvojina – estää henkilötietojen siirron kolmanteen maahan riippumatta tietosuojan tason riittävyyttä koskevasta päätöksestä, jos kolmannessa maassa ei enää taata riittävää suojaa[508].

Kukin valvontaviranomainen on toimivaltainen käyttämään alueellaan tutkinta- ja toimivaltuuksia. Koska rekisterinpitäjien ja henkilötietojen käsittelijöiden toimet ovat kuitenkin usein rajatylittäviä ja tietojenkäsittely vaikuttaa useissa jäsenvaltioissa sijaitseviin rekisteröityihin, herää kysymys valtuuksien jaosta eri valvontaviranomaisten välillä. Euroopan unionin tuomioistuin pääsi selvittämään tätä kysymystä asiassa *Weltimmo*.

Esimerkki: Asiassa *Weltimmo*[509] Euroopan unionin tuomioistuin selvitti kansallisten valvontaviranomaisten toimivaltaa käsitellä asioita, joissa on mukana niiden oikeudenkäyttöalueen ulkopuolelle sijoittautuneita organisaatioita. Weltimmo oli Slovakiassa rekisteröity yhtiö, joka piti yllä internetsivustoa, jolla se julkaisi Unkarissa sijaitsevia kiinteistöjä koskevia ilmoituksia. Ilmoittajat tekivät kantelun Unkarin tietosuojan valvontaviranomaiselle Unkarin tietosuojalainsäädännön rikkomisesta, ja viranomainen määräsi Weltimmolle sakon. Yhtiö riitautti sakon kansallisissa tuomioistuimissa, ja asia saatettiin Euroopan unionin tuomioistuimen käsiteltäväksi, jotta voitiin selvittää, voivatko yhden jäsenvaltion valvontaviranomaiset soveltaa EU:n tietosuojalainsäädännön nojalla kansallista tietosuojalainsäädäntöään toisessa jäsenvaltioissa rekisteröityyn yhtiöön.

Euroopan unionin tuomioistuin tulkitsi tietosuojadirektiivin 4 artiklan 1 kohdan a alakohtaa siten, että sen nojalla on mahdollista soveltaa muun jäsenvaltion tietosuojalainsäädäntöä kuin sen, jossa rekisterinpitäjä on rekisteröity, ”kunhan rekisterinpitäjä harjoittaa kyseisen valtion alueella olevan kiinteän

508 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015, 26–36 kohta ja 40–41 kohta.

509 EUT, C-230/14, *Weltimmo s.r. o. vastaan Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1.10.2015.

toimipaikan välityksin aitoa ja todellista, vaikka vähäistäkin, toimintaa, jonka yhteydessä tämä tietojenkäsittely suoritetaan". Tuomioistuin katsoi saamiensa tietojen perusteella, että Weltimmo harjoitti aitoa ja todellista toimintaa Unkarissa, koska yhtiöllä oli Unkarissa edustaja, joka mainitaan Slovakian yritysrekisterissä Unkarissa sijaitsevan osoitteen kera, sekä pankkitili ja postilokero Unkarissa. Yhtiö myös harjoitti toimiaan Unkarissa unkarin kielellä. Näistä tiedoista kävi ilmi toimipaikan olemassaolo, jonka perusteella Weltimmon toimintaan sovellettaisiin Unkarin tietosuojalainsäädäntöä ja se kuuluisi Unkarin valvontaviranomaisen toimivaltaan. Euroopan unionin tuomioistuin jätti kuitenkin kansallisen tuomioistuimen tehtäväksi tarkistaa tiedot ja päättää, oliko Weltimmolla tosiasiallisesti toimipaikka Unkarissa.

Jos ennakkoratkaisupyynnön esittänyt tuomioistuin havaitsisi, että Weltimmolla oli toimipaikka Unkarissa, Unkarin valvontaviranomaisella olisi valtuudet määrätä sakko. Jos taas kansallinen tuomioistuin päättäisi toisin eli että Weltimmolla ei olisi toimipaikkaa Unkarissa, sovellettava lainsäädäntö olisi silloin sen jäsenvaltion, johon (jäsenvaltioiden, joihin) yhtiö oli rekisteröitynyt. Koska tässä tapauksessa valvontaviranomaisen valtuuksia on käytettävä toisten jäsenvaltioiden alueellisen itsemääräämisoikeuden mukaisesti, Unkarin viranomainen ei pystyisi määräämään seuraamuksia. Koska tietosuojadirektiiviin sisältyi valvontaviranomaisten yhteistyövelvoite, Unkarin viranomainen voisi kuitenkin pyytää Slovakian viranomaista tutkimaan asiaan, toteamaan Slovakian lainsäädännön rikkomuksen ja määräämään Slovakian lainsäädännössä säädetyt seuraamukset.

Yleisen tietosuoja-asetuksen antamisen myötä nyt on käytössä yksityiskohtaisia sääntöjä valvontaviranomaisten toimivallasta rajatylittävissä tapauksissa. Asetuksella perustetaan yhden luukun järjestelmä, ja se sisältää säännöksiä eri valvontaviranomaisten välisestä yhteistyöstä. Tehokkaan yhteistyön takaamiseksi rajatylittävissä tapauksissa yleisen tietosuoja-asetuksen mukaan johtava valvontaviranomainen on rekisterinpitäjän tai henkilötietojen käsittelijän päätoimipaikan tai ainoan toimipaikan valvontaviranomainen[510]. Johtava valvontaviranomainen vastaa rajatylittävistä tapauksista, on rekisterinpitäjän tai henkilötietojen käsittelijän ainoa yhteystaho ja koordinoi yhteistyötä muiden valvontaviranomaisten kanssa konsensuksen saavuttamiseksi. Yhteistyöhön kuuluu tietojenvaihtoa, keskinäistä avunantoa valvonnassa ja tutkinnassa sekä sitovien päätösten tekemistä.[511]

510 Yleinen tietosuoja-asetus, 56 artiklan 1 kohta.

511 *Ibid.*, 60 artikla.

Euroopan neuvoston oikeudessa valvontaviranomaisten toimivallasta ja valtuuksista säädetään uudistetun yleissopimuksen 108 15 artiklassa. Nämä valtuudet vastaavat EU:n oikeudessa valvontaviranomaisille annettuja valtuuksia, ja niitä ovat muun muassa tutkinta- ja toimivaltuudet, valtuudet tehdä päätöksiä ja määrätä hallinnollisia seuraamuksia yleissopimuksen säännösten rikkomisesta sekä valtuudet olla asianosaisena oikeudenkäynnissä. Riippumattomilla valvontaviranomaisilla on myös toimivalta käsitellä rekisteröityjen esittämiä pyyntöjä ja kanteluita, valistaa yleisöä tietosuojalainsäädännöstä ja antaa kansallisille päätöksentekijöille neuvontaa kaikista henkilötietojen käsittelyä koskevista lainsäädännöllisistä tai hallinnollisista toimenpiteistä.

5.3 Yhteistyö

Yleisellä tietosuoja-asetuksella luodaan yleinen kehys valvontaviranomaisten väliselle yhteistyölle ja säädetään entistä yksityiskohtaisemmista säännöistä valvontaviranomaisten väliselle yhteistyölle tietojenkäsittelyn rajatylittävissä toimissa.

Yleisen tietosuoja-asetuksen mukaan valvontaviranomaisten on annettava toisilleen tarvittavat tiedot ja keskinäistä apua tämän asetuksen johdonmukaisen täytäntöönpanon ja soveltamisen varmistamiseksi.[512] Tähän kuuluu myös se, että valvontaviranomainen, jolle pyyntö on osoitettu, tekee tarkastuksia ja tutkimuksia. Valvontaviranomaiset voivat toteuttaa yhteisiä operaatioita, mukaan lukien yhteisiä tutkimuksia ja yhteisiä täytäntöönpanotoimenpiteitä, joihin osallistuu kaikkien valvontaviranomaisten henkilöstöä[513].

EU:ssa rekisterinpitäjät ja henkilötietojen käsittelijät toimivat jatkuvasti yhä kansainvälisemmin. Tämä edellyttää tiivistä yhteistyötä jäsenvaltioiden toimivaltaisten valvontaviranomaisten välillä, jotta voidaan varmistaa yleisen tietosuoja-asetuksen vaatimusten noudattaminen tietojenkäsittelyssä. Asetuksen yhden luukun järjestelmän mukaan on niin, että jos rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikkoja useissa jäsenvaltioissa tai jos sillä on yksi ainoa toimipaikka, mutta käsittelytoimet vaikuttavat merkittävästi rekisteröityihin useammassa kuin yhdessä jäsenvaltiossa, päätoimipaikan (tai ainoan toimipaikan) valvontaviranomainen on johtava viranomainen rekisterinpitäjän tai henkilötietojen käsittelijän rajatylittävissä toimissa. Johtavilla viranomaisilla on valtuudet ryhtyä pakkotoimiin rekisterinpitäjää tai henkilötietojen käsittelijää vastaan. Yhden luukun järjestelmän tavoitteena

512 *Ibid.*, 61 artiklan 1–3 kohta ja 62 artiklan 1 kohta.

513 *Ibid.*, 62 artiklan 1 kohta.

on parantaa EU:n tietosuojalainsäädännön yhdenmukaistamista ja sen yhtenäistä soveltamista eri jäsenvaltioissa. Se on hyödyllinen myös yrityksille, koska niiden tarvitsee toimia vain yhden johtavan eikä usean valvontaviranomaisen kanssa. Se parantaa yritysten oikeusvarmuutta, ja käytännössä sen pitäisi myös tarkoittaa päätöksenteon nopeutumista sekä sitä, että yrityksillä ei ole vastassaan eri valvontaviranomaisia, jotka määräävät niille ristiriitaisia vaatimuksia.

Johtavan viranomaisen määrittäminen tarkoittaa yrityksen päätoimipaikan sijainnin määrittämistä EU:ssa. Päätoimipaikan määritelmä annetaan yleisessä tietosuoja-asetuksessa. Tietosuojatyöryhmä on myös antanut ohjeita rekisterinpitäjän tai henkilötietojen käsittelijän johtavan valvontaviranomaisen määrittämiseen. Ne sisältävät myös kriteerit päätoimipaikan määrittämiselle.[514]

Tietosuojan korkean tason varmistamiseksi koko EU:ssa johtava valvontaviranomainen ei toimi yksin. Sen on tehtävä rekisterinpitäjien ja henkilötietojen käsittelijöiden suorittamaa tietojenkäsittelyä koskevassa päätöksenteossa yhteistyötä muiden osallistuvien valvontaviranomaisten kanssa ja pyrittävä näin konsensukseen ja johdonmukaisuuden varmistamiseen. Asianomaisten valvontaviranomaisten väliseen yhteistyöhön kuuluu tietojen vaihtamista, keskinäistä avunantoa, yhteisten tutkimusten tekemisestä ja seurantatoimia.[515] Antaessaan toisilleen keskinäistä apua valvontaviranomaisten on käsiteltävä viipymättä toisten valvontaviranomaisten esittämät tietopyynnöt ja toteutettava valvontatoimia, esimerkiksi rekisterinpitäjän käsittelytoimia koskevia ennakkohyväksyntiä ja -kuulemisia sekä tutkimuksia. Muiden jäsenvaltioiden valvontaviranomaisille on annettava keskinäistä apua pyynnöstä ilman aiheetonta viivytystä ja viimeistään kuukauden kuluttua pyynnön vastaanottamisesta.[516]

Kun rekisterinpitäjällä on toimipaikkoja useissa jäsenvaltioissa, valvontaviranomaiset voivat toteuttaa yhteisiä operaatioita, mukaan lukien tutkimuksia ja täytäntöönpanotoimenpiteitä, joihin osallistuu muiden jäsenvaltioiden valvontaviranomaisten jäseniä tai muuta henkilöstöä[517].

514 Tietosuojatyöryhmä (2016), *ohjeet rekisterinpitäjän tai henkilötietojen käsittelijän johtavan valvontaviranomaisen määrittämiseen*, WP 244, Bryssel, 13.12.2016, viimeksi tarkistettu ja hyväksytty 5.4.2017.

515 Yleinen tietosuoja-asetus, 60 artiklan 1–3 kohta.

516 *Ibid.*, 61 artiklan 1 ja 2 kohta.

517 *Ibid.*, 62 artiklan 1 kohta.

Eri valvontaviranomaisten yhteistyötä koskeva vaatimus on tärkeä myös EU:n oikeudessa. Uudistetun yleissopimuksen 108 mukaan valvontaviranomaisten on tehtävä keskenään yhteistyötä niiden tehtävien suorittamisen edellyttämässä laajuudessa[518]. Se pitäisi tehdä esimerkiksi antamalla toinen toisilleen kaikki asiaankuuluvat ja hyödylliset tiedot sekä koordinoimalla tutkimuksia ja toteuttamalla yhteisiä toimia[519].

5.4 Euroopan tietosuojaneuvosto

Tässä luvussa on aiemmin kuvattu riippumattomien valvontaviranomaisten merkitys ja niiden Euroopan tietosuojalainsäädännön mukaiset tärkeimmät valtuudet. Euroopan tietosuojaneuvosto on toinen tärkeä toimija sen varmistamisessa, että tietosuojasääntöjä sovelletaan tehokkaasti ja yhdenmukaisesti koko EU:ssa.

Yleisellä tietosuoja-asetuksella perustettiin Euroopan tietosuojaneuvosto unionin elimeksi, jolla on oikeushenkilöllisyys[520]. Se on seuraaja tietosuojatyöryhmälle[521], joka perustettiin tietosuojadirektiivillä antamaan komissiolle neuvontaa kaikista EU:n toimenpiteistä, jotka vaikuttavat yksilöiden oikeuksiin henkilötietojen käsittelyn ja yksityisyydensuojan kannalta, edistämään direktiivin yhdenmukaista soveltamista ja antamaan komissiolle asiantuntijalausuntoja tietosuojaan liittyvissä asioissa. Tietosuojatyöryhmässä oli edustajia EU:n jäsenvaltioiden valvontaviranomaisista sekä komissiosta ja Euroopan tietosuojavaltuutetusta.

Tietosuojatyöryhmän tapaan tietosuojaneuvoston muodostavat valvontaviranomaisten johtajat kustakin jäsenvaltiosta ja Euroopan tietosuojavaltuutettu tai näiden edustajat[522]. Euroopan tietosuojavaltuutetulla on yhtäläiset äänioikeudet lukuun ottamatta kiistanratkaisua koskevia tapauksia, joissa se voi äänestää vain päätöksissä, jotka koskevat unionin toimielimiin sovellettavia periaatteita ja sääntöjä, jotka vastaavat asiasisällöltään yleisen tietosuoja-asetuksen periaatteita ja sääntöjä. Komissiolla on oikeus osallistua tietosuojaneuvoston toimintaan ja kokouksiin,

518 Uudistettu yleissopimus 108, 16 ja 17 artikla.

519 *Ibid.*, 12 a artiklan 7 kohta.

520 Yleinen tietosuoja-asetus, 68 artikla.

521 Direktiivin 95/46/EY mukaan tietosuojatyöryhmän tehtävänä oli antaa komissiolle neuvontaa kaikista EU:n toimenpiteistä, jotka vaikuttavat yksilöiden oikeuksiin henkilötietojen käsittelyn ja yksityisyydensuojan kannalta, edistää direktiivin yhdenmukaista soveltamista ja antaa komissiolle asiantuntijalausuntoja tietosuojaan liittyvissä asioissa. Tietosuojatyöryhmässä oli edustajia EU:n jäsenvaltioiden valvontaviranomaisista sekä komissiosta ja Euroopan tietosuojavaltuutetusta.

522 Yleinen tietosuoja-asetus, 68 artiklan 3 kohta.

mutta ilman äänioikeutta.[523] Tietosuojaneuvosto valitsee jäsentensä keskuudesta puheenjohtajan (jonka tehtävänä on tietosuojaneuvoston edustaminen) ja kaksi varapuheenjohtajaa yksinkertaisella enemmistöllä viiden vuoden toimikaudeksi. Tietosuojaneuvostolla on käytössään myös sihteeristö, jonka henkilöstöstä vastaa Euroopan tietosuojavaltuutettu, jotta tietosuojaneuvosto saa analyyttista, hallinnollista ja logistista tukea.[524]

Tietosuojaneuvoston tehtävät eritellään yleisen tietosuoja-asetuksen 64, 65 ja 70 artiklassa, ja niihin kuuluu kokonaisvaltaisia velvollisuuksia, jotka voidaan jakaa kolmeen päätoimeen:

- **Yhdenmukaisuus:** Tietosuojaneuvosto voi antaa oikeudellisesti sitovia päätöksiä kolmessa tapauksessa: jos valvontaviranomainen on esittänyt merkityksellisen ja perustellun vastalauseen yhden luukun järjestelmää koskevissa tapauksissa, jos esiintyy eriäviä näkemyksiä siitä, mikä valvontaviranomaisista on johtava valvontaviranomainen, ja jos toimivaltainen valvontaviranomainen ei pyydä tietosuojaneuvostolta lausuntoa tai ei noudata sen antamaa lausuntoa[525]. Tietosuojaneuvoston tärkeimpänä tehtävänä on varmistaa, että yleistä tietosuoja-asetusta sovelletaan yhdenmukaisesti koko EU:ssa, ja sillä on keskeinen asema 5.5 kohdassa kuvatussa yhdenmukaisuusmekanismissa.

- **Kuuleminen:** Tietosuojaneuvoston tehtäviin kuuluu antaa komissiolle neuvoja kaikista henkilötietojen suojaan unionissa liittyvistä kysymyksistä, kuten yleisen tietosuoja-asetuksen muutoksista, tarkistuksista EU:n lainsäädäntöön, joka sisältää tietojenkäsittelyä ja voisi olla ristiriidassa EU:n tietosuojasääntöjen kanssa, sekä antaa komission tietosuojan tason riittävyyttä koskevia päätöksiä, joiden nojalla henkilötietoja voidaan siirtää kolmanteen maahan tai kansainväliselle järjestölle.

- **Ohjeet:** Tietosuojaneuvosto antaa myös suuntaviivoja, suosituksia ja parhaita käytänteitä asetuksen johdonmukaisen soveltamisen tukemiseksi ja edistää valvontaviranomaisten välistä yhteistyötä ja tietojen vaihtamista. Sen on myös kannustettava rekisterinpitäjien tai henkilötietojen käsittelijöiden yhdistyksiä laatimaan käytännesääntöjä sekä luomaan tietosuojaa koskevia sertifiointimekanismeja ja sinettejä.

523 *Ibid.*, 68 artiklan 4 ja 5 kohta.

524 *Ibid.*, 73 ja 75 artikla.

525 *Ibid.*, 65 artikla.

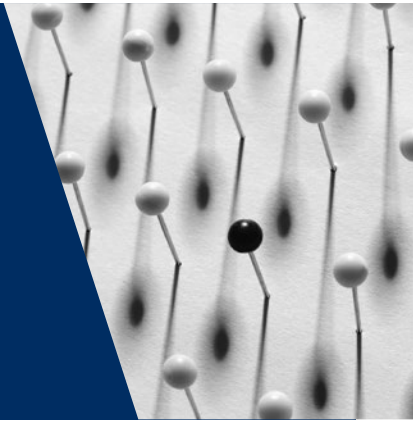
Tietosuojaneuvoston päätökset voidaan riitauttaa Euroopan unionin tuomioistuimessa.

5.5 Yleisen tietosuoja-asetuksen yhdenmukaisuusmekanismi

Yleisellä tietosuoja-asetuksella perustetaan yhdenmukaisuusmekanismi, jotta voidaan edistää asetuksen yhdenmukaista soveltamista kaikissa jäsenvaltioissa, ja valvontaviranomaiset tekevät sen puitteissa yhteistyötä toistensa ja tarvittaessa komission kanssa. Yhdenmukaisuusmekanismia käytetään kahdessa tilanteessa. Ensimmäinen koskee tietosuojaneuvoston lausuntoja tapauksissa, joissa toimivaltainen valvontaviranomainen aikoo toteuttaa toimenpiteitä, kuten hyväksyä luettelon toimista, joilta edellytetään tietosuojaa koskevaa vaikutustenarviointia, tai määrittää vakiosopimuslausekkeet. Toinen koskee tietosuojaneuvoston sitovia päätöksiä valvontaviranomaisille yhden luukun järjestelmän tapauksissa tai kun valvontaviranomainen ei noudata tietosuojaneuvoston lausuntoa tai ei pyydä sitä.

6

Rekisteröityjen oikeudet ja niiden valvonta



EU	Käsiteltävät asiat	EN
Oikeus saada ilmoitus		
Yleinen tietosuoja-asetus, 12 artikla EUT, C-473/12, *Institut professionnel des agents immobiliers (IPI) vastaan Englebert*, 2013 EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 2015	**Tietojen läpinäkyvyys**	Uudistettu yleissopimus 108, 8 artikla
Yleinen tietosuoja-asetus, 13 artiklan 1 ja 2 kohta ja 14 artiklan 1 ja 2 kohta	**Tietojen sisältö**	Uudistettu yleissopimus 108, 8 artiklan 1 kohta
Yleinen tietosuoja-asetus, 13 artiklan 1 kohta ja 14 artiklan 3 kohta	**Tietojen toimittamisen ajankohta**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan b alakohta
Yleinen tietosuoja-asetus, 12 artiklan 1, 5 ja 7 kohta	**Tietojen toimittamisen tavat**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan b alakohta
Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan d alakohta ja 14 artiklan 2 kohdan e alakohta, 77, 78 ja 79 artikla	**Oikeus tehdä valitus**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan f alakohta

EU	Käsiteltävät asiat	EN
Oikeus saada pääsy tietoihin		
Yleinen tietosuoja-asetus, 15 artiklan 1 kohta EUT, C-553/07, *College van burgemeester en wethouders van Rotterdam vastaan E. E. Rijkeboer*, 2009 EUT, yhdistetyt asiat C-141/12 ja C- 372/12, *YS vastaan Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vastaan M ja S*, 2014 EUT, C-434/16, *Peter Nowak v. Data Protection Commissioner*, 2017	**Oikeus saada pääsy omiin tietoihin**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan b alakohta EIT, *Leander v. Ruotsi*, nro 9248/81, 1987
Oikeus tietojen oikaisemiseen		
Yleinen tietosuoja-asetus, 16 artikla	**Epätarkkojen ja virheellisten henkilötietojen oikaisu**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan e alakohta EIT, *Cemalettin Canli v. Turkki*, nro 22427/04, 2008 EIT, *Ciubotaru v. Moldova*, nro 27138/04, 2010
Oikeus tietojen poistamiseen		
Yleinen tietosuoja-asetus, 17 artiklan 1 kohta	**Henkilötietojen poistaminen**	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan e alakohta EIT, *Segerstedt-Wiberg ym. v. Ruotsi*, nro 62332/00, 2006
EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 2014 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	**Oikeus tulla unohdetuksi**	

EU	Käsiteltävät asiat	EN
Oikeus käsittelyn rajoittamiseen		
Yleinen tietosuoja-asetus, 18 artiklan 1 kohta	Oikeus henkilötietojen käytön rajoittamiseen	
Yleinen tietosuoja-asetus, 19 artikla	Ilmoitusvelvollisuus	
Oikeus siirtää tiedot järjestelmästä toiseen		
Yleinen tietosuoja-asetus, 20 artikla	Oikeus siirtää tiedot järjestelmästä toiseen	
Vastustamisoikeus		
Yleinen tietosuoja-asetus, 21 artiklan 1 kohta EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 2017	Oikeus vastustaa tietojenkäsittelyä rekisteröidyn erityisen tilanteen vuoksi	Profilointia koskeva suositus, 5 artiklan 3 kohta Uudistettu yleissopimus 108, 9 artiklan 1 kohdan d alakohta
Yleinen tietosuoja-asetus, 21 artiklan 2 kohta	Oikeus vastustaa tietojen käyttöä markkinointitarkoituksiin	Suoramarkkinointia koskeva suositus, 4 artiklan 1 kohta
Yleinen tietosuoja-asetus, 21 artiklan 5 kohta	Oikeus vastustaa henkilötietojen automaattista käsittelyä	
Automaattiseen päätöksentekoon ja profilointiin liittyvät oikeudet		
Yleinen tietosuoja-asetus, 22 artikla	Automaattiseen päätöksentekoon ja profilointiin liittyvät oikeudet	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan a alakohta
Yleinen tietosuoja-asetus, 21 artikla	Oikeus vastustaa automaattista päätöksentekoa	
Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta	Oikeus saada ymmärrettävä selitys	Uudistettu yleissopimus 108, 9 artiklan 1 kohdan c alakohta

EU	Käsiteltävät asiat	EN
Oikeussuojakeinot, vastuu, seuraamukset ja korvaukset		
Perusoikeuskirja, 47 artikla EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 2015 Yleinen tietosuoja-asetus, 77–84 artikla	**Kansallisen tietosuoja-lainsäädännön rikkomukset**	EIT, 13 artikla (vain Euroopan neuvoston jäsenvaltioille) Uudistettu yleissopimus 108, 9 artiklan 1 kohdan f alakohta, 12, 15 ja 16–21 artikla EIT, *K.U. v. Suomi*, nro 2872/02, 2008 EIT, *Biriuk v. Liettua*, nro 23373/03, 2008
EU:n toimielinten tietosuoja-asetus, 34 ja 49 artikla EUT, C-28/08 P, *Euroopan komissio vastaan The Bavarian Lager Co. Ltd* [suuri jaosto], 2010	**EU:n oikeuden rikkomukset EU:n toimielimissä ja elimissä**	

Yleisesti oikeussääntöjen ja erityisesti rekisteröityjen oikeuksien vaikuttavuus riippuu merkittävässä määrin asianmukaisten valvontamekanismien olemassaolosta. Digitaaliaikana tietojenkäsittelyä on kaikkialla, ja ihmisten on entistä vaikeampaa ymmärtää sitä. Rekisteröityjen ja rekisterinpitäjien välisen vallan epätasapainon lieventämiseksi yksilöille on annettu tiettyjä oikeuksia, jotta he voivat valvoa aiempaa paremmin henkilötietojensa käsittelyä. Euroopan unionin perusoikeuskirjan 8 artiklan 2 kohdassa vahvistetaan oikeus tutustua omiin tietoihin ja oikeus saada ne oikaistuiksi. Perusoikeuskirja kuuluu EU:n primaarilainsäädäntöön ja sillä on perustavanlaatuinen arvo EU:n oikeusjärjestyksessä. EU:n johdetussa oikeudessa – erityisesti yleisessä tietosuoja-asetuksessa – on vahvistettu johdonmukainen oikeudellinen kehys, jonka nojalla rekisteröityjen valtuuksia lisätään antamalla heille rekisterinpitäjiä koskevia oikeuksia. Tietoihin pääsyä ja oikaisua koskevien oikeuksien lisäksi yleisessä tietosuoja-asetuksessa tunnustetaan useita muita oikeuksia, kuten oikeus tietojen poistamiseen (oikeus tulla unohdetuksi), oikeus vastustaa tai rajoittaa tietojenkäsittelyä sekä automaattiseen päätöksentekoon ja profilointiin liittyvät oikeudet. Myös uudistetussa yleissopimuksessa 108 on samanlaisia takeita, joiden nojalla rekisteröidyt voivat valvoa tehokkaasti omia tietojaan. Sen 9 artiklassa luetellaan oikeudet, joita yksilöillä pitäisi olla heidän henkilötietojensa käsittelyn osalta. Sopimuspuolten on varmistettava, että nämä oikeudet ovat kaikkien rekisteröityjen käytettävissä niiden oikeudenkäyttöalueella ja että niitä tuetaan tehokkailla oikeudellisilla ja käytännön keinoilla, jotta rekisteröidyt voivat käyttää niitä.

Sen lisäksi, että yksilöille annetaan oikeuksia, on myös tärkeää perustaa mekanismeja, joiden avulla rekisteröidyt voivat riitauttaa oikeuksiensa rikkomukset, saada rekisterinpitäjät vastuuseen ja vaatia korvauksia. Ihmisoikeussopimuksessa ja perusoikeuskirjassa taattu oikeus tehokkaaseen oikeussuojakeinoon edellyttää vielä, että jokaisella on käytettävissään oikeussuojakeinoja.

6.1 Rekisteröityjen oikeudet

Keskeiset kohdat

- Jokaisella rekisteröidyllä on oikeus saada kaikilta rekisterinpitäjiltä tietoa siitä, käsitteleekö rekisterinpitäjä hänen henkilötietojaan. Tähän sovelletaan tiettyjä poikkeuksia.
- Rekisteröidyillä on oltava oikeus
  - saada pääsy omiin tietoihinsa ja saada tiettyjä tietoja käsittelystä
  - saada henkilötietoja käsittelevä rekisterinpitäjä oikaisemaan hänen tietonsa, jos ne ovat virheelliset
  - saada rekisterinpitäjä tarvittaessa poistamaan hänen tietonsa, jos rekisterinpitäjä käsittelee niitä laittomasti
  - rajoittaa käsittelyä väliaikaisesti
  - saada tietonsa siirretyksi toiselle rekisterinpitäjälle tietyin ehdoin.
- Lisäksi rekisteröidyllä on oltava oikeus vastustaa omien henkilötietojensa käsittelyä
  - erityiseen tilanteeseensa liittyvistä syistä
  - suoramarkkinointitarkoituksissa.
- Rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin, ja jolla on häntä koskevia oikeusvaikutuksia tai joka vaikuttaa häneen vastaavalla tavalla merkittävästi. Rekisteröidyillä on myös oikeus
  - vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö
  - esittää kantansa ja riitauttaa päätös, joka perustuu automaattiseen käsittelyyn.

6.1.1 Oikeus saada ilmoitus

Sekä **Euroopan neuvoston** että **EU:n oikeuden** mukaan käsittelytoimien rekisterinpitäjien on ilmoitettava rekisteröidyille suunnitellusta käsittelystä, kun henkilötietoja kerätään. Tämä velvollisuus ei edellytä rekisteröidyn esittämää pyyntöä, vaan rekisterinpitäjän on noudatettava sitä ennakoivasti riippumatta siitä, osoittaako rekisteröity olevansa kiinnostunut tiedoista vai ei.

Euroopan neuvoston oikeudessa uudistetun yleissopimuksen 108 8 artiklan mukaan sopimuspuolten on taattava, että rekisterinpitäjät ilmoittavat rekisteröidyille henkilöllisyytensä ja tavanomaisen sijaintipaikkansa, käsittelyn oikeusperustan ja tarkoituksen, käsiteltävät henkilötietoryhmät, henkilötietojen (mahdolliset) vastaanottajat ja sen, miten rekisteröidyt voivat käyttää 9 artiklan mukaisia oikeuksiaan, kuten oikeutta saada omat tiedot ja oikaista ne sekä oikeutta oikeussuojakeinoihin. Rekisteröidyille on lisäksi ilmoitettava kaikki muut lisätiedot, joiden katsotaan olevan tarpeen oikeudenmukaisen ja läpinäkyvän henkilötietojen käsittelyn varmistamiseksi. Uudistetun yleissopimuksen 108 selitysmuistiossa täsmennetään, että tiedot on esitettävä rekisteröidyille helposti saatavilla, luettavissa olevalla, ymmärrettävällä ja asianomaisten rekisteröityjen mukaan mukautetulla tavalla[526].

EU:n oikeudessa läpinäkyvyyden periaate edellyttää, että kaiken henkilötietojen käsittelyn on oltava yleisesti läpinäkyvää luonnollisille henkilöille. Luonnollisilla henkilöillä on oikeus tietää, miten ja mitä henkilötietoja kerätään, käytetään tai muutoin käsitellään, ja heille on tiedotettava käsittelyyn liittyvistä riskeistä, suojatoimista ja oikeuksista.[527] Yleisen tietosuoja-asetuksen 12 artiklassa vahvistetaankin rekisterinpitäjille laaja ja kattava velvollisuus antaa läpinäkyvää tietoa ja/tai ilmoittaa, miten rekisteröidyt voivat käyttää oikeuksiaan[528]. Tiedot on esitettävä tiiviisti, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa selkeällä ja yksinkertaisella kielellä. Tiedot on toimitettava kirjallisesti, tapauksen mukaan myös sähköisessä muodossa, ja ne voidaan antaa suullisestikin, jos rekisteröity sitä pyytää ja jos rekisteröidyn henkilöllisyys on vahvistettu muulla tavoin. Tiedot on annettava ilman aiheetonta viivytystä ja kuluitta.[529]

526 Uudistettu yleissopimus 108, selitysmuistio, 68 kohta.

527 Yleinen tietosuoja-asetus, johdanto-osan 39 kappale.

528 *Ibid.*, 13 ja 14 artikla; uudistettu yleissopimus 108, 8 artiklan 1 kohdan b alakohta.

529 Yleinen tietosuoja-asetus, 12 artiklan 5 kohta; uudistettu yleissopimus 108, 9 artiklan 1 kohdan b alakohta.

Yleisen tietosuoja-asetuksen 13 artiklassa käsitellään rekisteröityjen oikeutta saada ilmoitus, kun henkilötiedot kerätään suoraan rekisteröidyiltä, ja 14 artiklassa silloin, kun henkilötietoja ei ole saatu rekisteröidyiltä.

Ilmoituksen saamista koskevan oikeuden soveltamisalaa ja sen rajoituksia EU:n oikeudessa on selvennetty Euroopan unionin tuomioistuimen oikeuskäytännössä.

Esimerkki: Asiassa *Institut professionnel des agents immobiliers (IPI) vastaan Englebert*[530] Euroopan unionin tuomioistuinta pyydettiin tulkitsemaan direktiivin 95/46/EY 13 artiklan 1 kohtaa. Artiklan nojalla jäsenvaltiot voivat toteuttaa lainsäädännöllisiä toimenpiteitä, joilla pyritään rajoittamaan rekisteröityjen oikeutta saada ilmoitus, kun se on tarpeen muun muassa muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi ja rikosten tai, säännellyn ammattitoiminnan osalta, ammattietiikan rikkomusten torjumiseksi ja tutkimiseksi. IPI on Belgiassa kiinteistönvälittäjien ammatillinen elin, joka vastaa kiinteistönvälittäjien ammatin moitteettoman harjoittamisen varmistamisesta. Se vaati kansallista tuomioistuinta toteamaan, että vastaajat olivat rikkoneen ammatin harjoittamisen sääntöjä ja määräämään ne lopettamaan useita kiinteistönvälitykseen liittyviä toimintoja. Kanne perustui IPI:n käyttämien yksityisetsivien keräämiin tosiseikkoihin.

Kansallisella tuomioistuimella oli epäilyksiä yksityisetsivien keräämien todisteiden arvosta, kun otettiin huomioon se mahdollisuus, että ne oli hankittu noudattamatta yksilöiden suojaa henkilötietojen käsittelyssä koskevia Belgian lainsäädännön vaatimuksia ja erityisesti velvollisuutta informoida rekisteröityjä heidän henkilötietojensa käsittelystä etukäteen ennen kyseisten tietojen keräämistä. Euroopan unionin tuomioistuin totesi, että 13 artiklan 1 kohdan mukaan jäsenvaltioilla ei ole velvollisuutta vaan mahdollisuus panna täytäntöön kansallisessa lainsäädännössä poikkeuksia velvollisuudesta informoida rekisteröityjä heidän henkilötietojensa käsittelystä. Koska 13 artiklan 1 kohta sisältää rikosten tai, säännellyn ammattitoiminnan osalta, ammattietiikan rikkomusten torjunnan, tutkinnan, selvittämisen ja syyteharkinnan syinä, joiden perusteella jäsenvaltiot voivat rajoittaa yksilöiden oikeuksia, IPI:n kaltaisen elimen ja sen puolesta toimivien yksityisetsivien toiminnassa voidaan vedota tähän säännökseen. Jos taas jäsenvaltio ei ole säätänyt tällaisesta poikkeuksesta, rekisteröityjä on informoitava.

530 EUT, C-473/12, *Institut professionnel des agents immobiliers (IPI) vastaan Geoffrey Englebert* ym., 7.11.2013.

Esimerkki: Asiassa *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*[531] Euroopan unionin tuomioistuin selvitti, onko EU:n lainsäädäntö esteenä sille, että jäsenvaltion viranomainen voi siirtää henkilötietoja toiselle viranomaiselle myöhempää käsittelyä varten ilman, että rekisteröidyille on ilmoitettu tästä siirrosta sekä käsittelystä. Kyseessä olevassa asiassa kansallinen hallintoviranomainen ei ollut ilmoittanut kantajille siirtäneensä heidän tietojaan kansalliselle sairausvakuutuskassalle ennen siirtoa.

Euroopan unionin tuomioistuin totesi, että EU:n lainsäädännön vaatimus ilmoittaa rekisteröidyille heidän henkilötietojensa käsittelystä on "sitäkin tärkeämpi, sillä se on välttämätön edellytys sille, että kyseiset henkilöt käyttävät [...] oikeuttaan tutustua käsiteltäviin tietoihin ja oikaista niitä sekä [...] oikeuttaan vastustaa mainittujen tietojen käsittelyä". Asianmukaisen tietojenkäsittelyn periaate edellyttää, että rekisteröidyille ilmoitetaan heidän tietojensa siirtämisestä toiselle viranomaiselle sen tekemää myöhempää käsittelyä varten. Direktiivin 95/46/EY 13 artiklan 1 kohdan mukaan jäsenvaltiot voivat rajoittaa oikeutta saada ilmoitus valtiolle tärkeän taloudellisen edun turvaamiseksi, myös verotusta koskevissa asioissa. Tällaisista rajoituksista on kuitenkin säädettävä lainsäädännöllä. Koska siirrettävien tietojen määritelmästä tai siirtämisen yksityiskohtaisista järjestelyistä ei ollut säädetty lainsäädännöllä vaan ainoastaan kahden viranomaisen välisessä pöytäkirjassa, EU:n oikeudessa tarkoitettuja poikkeusta koskevia ehtoja ei täytetty. Kantajia olisi pitänyt informoida etukäteen heidän tietojensa siirtämisestä kansalliselle sairausvakuutuskassalle ja kyseisen viranomaisen suorittamasta näiden tietojen myöhemmästä käsittelystä.

Tietojen sisältö

Uudistetun yleissopimuksen 108 8 artiklan 1 kohdan mukaan rekisterinpitäjän on annettava rekisteröidylle kaikki tiedot, joilla varmistetaan asianmukainen ja avoin henkilötietojen käsittely, muun muassa

- rekisterinpitäjän henkilöllisyys ja tavanomainen kotipaikka tai toimipaikka
- suunnitellun käsittelyn oikeusperusta ja tarkoitukset
- käsiteltävät henkilötietoryhmät

531 EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 1.10.2015.

- henkilötietojen vastaanottajat tai mahdolliset vastaanottajaryhmät
- tavat, joilla rekisteröidyt voivat käyttää oikeuksiaan.

Yleisen tietosuoja-asetuksen mukaan kerättäessä rekisteröidyltä häntä koskevia henkilötietoja rekisterinpitäjän on silloin, kun henkilötietoja saadaan, toimitettava rekisteröidylle kaikki seuraavat tiedot:[532]

- rekisterinpitäjän ja tapauksen mukaan tämän mahdollisen edustajan sekä tietosuojavastaavan identiteetti ja yhteystiedot
- henkilötietojen käsittelyn tarkoitukset sekä oikeusperuste eli sopimus tai lakisääteinen velvollisuus
- rekisterinpitäjän oikeutetut edut, jos ne ovat käsittelyn perusteena
- henkilötietojen vastaanottajat tai vastaanottajaryhmät
- tieto siitä, siirretäänkö henkilötietoja kolmanteen maahan tai kansainväliselle järjestölle, ja siitä, perustuuko se tietosuojan riittävyyttä koskevaan päätökseen vai käytetäänkö asianmukaisia suojatoimia
- henkilötietojen säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- rekisteröidyn käsittelyä koskevat oikeudet, kuten oikeus saada pääsy häntä itseään koskeviin henkilötietoihin sekä oikeus pyytää kyseisten tietojen oikaisemista tai poistamista ja oikeus pyytää käsittelyn rajoittamista tai vastustaa käsittelyä
- tieto siitä, onko henkilötietojen antaminen lakisääteinen tai sopimukseen perustuva vaatimus, sekä siitä, onko rekisteröidyn pakko toimittaa henkilötiedot, ja tällaisten tietojen antamatta jättämisen mahdolliset seuraukset
- automaattisen päätöksenteon, muun muassa profiloinnin, olemassaolo
- oikeus tehdä valitus valvontaviranomaiselle
- oikeus peruuttaa suostumus.

532 Yleinen tietosuoja-asetus, 13 artiklan 1 kohta.

Kun kyse on automaattisesta päätöksenteosta, muun muassa profiloinnista, rekisteröityjen on saatava merkityksselliset tiedot profilointiin liittyvästä logiikasta sekä sen merkittävyydestä ja mahdollisista seurauksista rekisteröidylle.

Jos tietoja ei saada suoraan rekisteröidyltä, rekisterinpitäjän on ilmoitettava rekisteröidyille henkilötietojen alkuperä. Rekisterinpitäjän on joka tapauksessa ilmoitettava rekisteröidyille muun muassa siitä, käytetäänkö automaattista päätöksentekoa, esimerkiksi profilointia.[533] Jos rekisterinpitäjä lisäksi aikoo käsitellä henkilötietoja edelleen muuhun tarkoitukseen kuin siihen, johon henkilötiedot kerättiin, käyttötarkoitussidonnaisuuden periaate ja läpinäkyvyys edellyttävät, että rekisterinpitäjä antaa rekisteröidylle tietoa uudesta tarkoituksesta. Rekisterinpitäjien on annettava tiedot ennen kaikkea jatkokäsittelyä. Toisin sanoen tapauksissa, joissa rekisteröity on antanut suostumuksensa henkilötietojen käsittelyyn, rekisterinpitäjän on saatava rekisteröidyltä uusi suostumus, jos tietojenkäsittelyn tarkoitus muuttuu tai jos lisätään muita tarkoituksia.

Tietojen toimittamisen ajankohta

Yleisessä tietosuoja-asetuksessa erotetaan kaksi tilannetta ja kaksi ajankohtaa, jolloin rekisterinpitäjän on annettava tietoa rekisteröidyille:

- Kun henkilötiedot saadaan suoraan rekisteröidyltä, rekisterinpitäjän on ilmoitettava rekisteröidylle kaikista tähän liittyvistä tiedoista ja yleisen tietosuoja-asetuksen mukaisista oikeuksista silloin, kun henkilötietoja saadaan[534]. Jos rekisterinpitäjä aikoo käsitellä henkilötietoja eri tarkoitukseen, sen on annettava kaikki asiaankuuluvat tiedot ennen käsittelyn suorittamista.

- Silloin, kun henkilötietoja ei ole saatu suoraan rekisteröidyltä, rekisterinpitäjän on annettava rekisteröidylle tietoa käsittelystä ”kohtuullisen ajan kuluttua mutta viimeistään kuukauden kuluessa henkilötietojen saamisesta” tai ennen kuin tietoja luovutetaan kolmannelle osapuolelle[535].

533 Yleinen tietosuoja-asetus, 13 artiklan 2 kohta ja 14 artiklan 2 kohdan f alakohta.

534 *Ibid.*, 13 artiklan 1 ja 2 kohta, johdannon sanamuoto, jossa yleisessä tietosuoja-asetuksessa viitataan velvollisuuteen antaa tietoja ”silloin, kun henkilötietoja saadaan”.

535 *Ibid.*, 13 artiklan 3 kohta ja 14 artiklan 3 kohta; ks. myös uudistetun yleissopimuksen 108 8 artiklan 1 kohdan b alakohdan viittaus tietojen toimittamisesta kohtuullisessa määräajassa ja ilman aiheetonta viivytystä.

Uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että jos rekisteröidyille ei voida antaa tietoja ennen käsittelyn aloittamista, se voidaan tehdä myöhemmin, esimerkiksi silloin, kun rekisterinpitäjä ottaa yhteyttä rekisteröityyn mistä tahansa syystä[536].

Erilaisia tapoja toimittaa tietoja

Sekä Euroopan neuvoston että EU:n oikeuden mukaan tiedot, jotka rekisterinpitäjän on annettava, on esitettävä tiiviisti, läpinäkyvässä, helposti ymmärrettävässä ja saatavilla olevassa muodossa. Tiedot on toimitettava kirjallisesti, tapauksen mukaan myös sähköisessä muodossa selkeällä, yksinkertaisella ja helposti ymmärrettävällä kielellä. Tietoja toimittaessaan rekisterinpitäjä voi käyttää standardoituja kuvakkeita tietojen esittämiseksi helposti näkyvässä ja ymmärrettävässä muodossa[537]. Esimerkiksi lukkoa esittävää kuvaketta voitaisiin käyttää osoittamaan, että tiedot on kerätty suojatusti ja/tai salattu. Rekisteröidyt voivat myös pyytää, että tiedot annetaan suullisesti. Tietojen on oltava maksuttomia, paitsi jos rekisteröidyn pyynnöt ovat ilmeisen perusteettomia tai kohtuuttomia (esimerkiksi toistuvia).[538] Tietojen vaivaton saatavuus on ratkaisevan tärkeää rekisteröidyn kyvylle käyttää hänen EU:n tietosuojalainsäädännössä säädettyjä oikeuksiaan.

Asianmukaisen käsittelyn periaate edellyttää, että rekisteröidyt ymmärtävät tiedot vaivatta. Käytettävän kielen on sovelluttava sen vastaanottajille. Käytettävässä kielessä on oltava eri tasoja ja tyyppejä sen mukaan, onko sen kohteena esimerkiksi aikuinen vai lapsi, suuri yleisö vai akateeminen asiantuntija. Tietosuojatyöryhmä käsitteli kysymystä tämän ymmärrettäviä tietoja koskevan näkökohdan tasapainottamisesta lausunnossaan yhtenäisemmistä informointia koskevista säännöksistä. Siinä edistetään ajatusta niin sanotuista monitasoisista ilmoituksista[539], joiden ansiosta rekisteröity voisi päättää, miten yksityiskohtaista tietoa hän haluaa. Tämä tietojen esittämisen tapa ei kuitenkaan vapauta rekisterinpitäjää sen yleisen tietosuoja-asetuksen 13 ja 14 artiklan mukaisesta velvollisuudesta. Rekisterinpitäjän on edelleen annettava rekisteröidylle kaikki tiedot.

536 Uudistettu yleissopimus 108, selitysmuistio, 70 kohta.

537 Euroopan komissio kehittää delegoitujen säädösten avulla edelleen kuvakkeilla annettavia tietoja ja menettelyjä, joilla standardoituja kuvakkeita tarjotaan käyttöön, ks. yleinen tietosuoja-asetus, 12 artiklan 8 kohta.

538 Yleinen tietosuoja-asetus, 12 artiklan 1, 5 ja 7 kohta; uudistettu yleissopimus 108, 9 artiklan 1 kohdan b alakohta.

539 Tietosuojatyöryhmä (2004), *lausunto 10/2004 yhtenäisemmistä informointia koskevista säännöksistä*, WP 100, Bryssel, 25.11.2004.

Yksi tehokkaimmista tavoista tarjota tietoa on esittää rekisterinpitäjän kotisivulla asianmukaiset tiedotuslausekkeet, kuten sivuston tietosuojaseloste. Yrityksen tai viranomaisen on kuitenkin tiedotuskäytäntöä laatiessaan otettava huomioon, että osa väestöstä ei käytä internetiä.

Verkkosivuston henkilötietojen käsittelyä koskeva tietosuojaseloste voisi näyttää esimerkiksi tältä:

Tietoa meistä

Tietoja käsittelevä ”rekisterinpitäjä” on Bed and Breakfast C&U, jonka toimipaikka on osoitteessa [osoite: xxx]. Puhelinnumero: xxx; faksinumero: xxx; ja sähköpostiosoite info@c&u.com. Tietosuojavastaavan yhteystiedot: [xxx].

Henkilötietoja koskeva ilmoitus kuuluu hotellipalveluja sääntelevіin ehtoihin.

Mitä henkilötietoja kerätään?

Me keräämme seuraavat henkilötiedot: nimi, postiosoite, puhelinnumero, sähköpostiosoite, tiedot oleskelusta, pankki- ja luottokortin numero sekä niiden tietokoneiden IP-osoitteet tai verkkotunnukset, joita käytit yhteyden muodostamiseen verkkosivustollemme.

Miksi henkilötietoja kerätään?

Tietojasi kerätään suostumuksesi perusteella ja varausten täytäntöönpanoa varten, tarjoamiimme palveluihin liittyvien sopimusten tekemistä ja täytäntöönpanoa varten sekä laissa säädettyjen vaatimusten noudattamiseksi. Siitä on esimerkki paikallisista maksuista annettu laki, jonka mukaan henkilötiedot on kerättävä kaupungin majoitusveron maksamiseksi.

Miten tietoja käsitellään?

Henkilötietojasi säilytetään kolmen kuukauden ajan. Tietosi eivät joudu automaattisten päätöksentekomenettelyjen kohteeksi.

Bed and Breakfast C&U noudattaa tiukasti turvallisuusmenettelyjä, joilla varmistetaan, että henkilötietosi eivät vahingoitu, niitä ei tuhota eikä luovuteta kolmannelle osapuolelle ilman lupaasi ja että niihin ei pääse luvatta. Tietokoneita, joihin tiedot tallennetaan, pidetään turvallisessa ympäristössä, johon on rajoitettu fyysinen pääsy. Sähköisen pääsyn rajoittamiseksi käytetään palomuureja ja muita toimenpiteitä. Jos tietoja on siirrettävä kolmannelle osapuolelle, siltä edellytetään samanlaisia toimenpiteitä henkilötietojen suojaamiseksi.

Kaikkia keräämiämme ja tallentamiamme tietoja käsitellään vain toimistoissamme. Vain henkilöille, jotka tarvitsevat tietoja tehtäviensä täyttämiseksi tämän sopimuksen mukaisesti, annetaan pääsy henkilötietoihin. Sinulta kysytään nimenomaisesti, kun tarvitsemme tietoja tunnistamistasi varten. Voimme pyytää sinua tekemään yhteistyötä turvatarkastajiemme kanssa ennen kuin luovutamme tietoja sinulle. Voit saattaa meille antamasi tiedot ajan tasalle milloin tahansa ottamalla meihin yhteyttä suoraan.

Mitä oikeuksia sinulla on?

Sinulla on oikeus tutustua tietoihisi, saada jäljennös tiedoistasi, pyytää tietojesi poistamista tai oikaisua tai pyytää siirtämään tietosi toiselle rekisterinpitäjälle.

Voit osoittaa pyyntösi meille osoitteeseen info@c&u.com. Meidän on vastattava pyyntöösi kuukauden kuluessa, mutta jos pyyntösi on liian monimutkainen tai jos saamme liian monta pyyntöä, ilmoitamme, että vastausaikaa voidaan jatkaa kahdella kuukaudella.

Omiin henkilötietoihin tutustuminen

Sinulla on oikeus tutustua omiin tietoihisi, ja ne annetaan sinulle pyynnöstä yhdessä tietojenkäsittelyn perustaa koskevien tietojen kanssa. Sinulla on myös oikeus pyytää niiden poistamista tai oikaisemista ja oikeus olla joutumatta automaattisen päätöksenteon kohteeksi, joka tehtäisiin ilman, että näkemyksiäsi otettaisiin huomioon. Voit osoittaa pyyntösi meille osoitteeseen info@c&u.com. Sinulla on myös oikeus vastustaa käsittelyä, peruuttaa suostumuksesi ja esittää valitus kansalliselle valvontaviranomaiselle, jos katsot, että tämä tietojenkäsittely rikkoo lakia, ja vaatia korvausta vahingoista, jotka johtuvat lainvastaisesta tietojenkäsittelystä.

Oikeus tehdä valitus

Yleisen tietosuoja-asetuksen mukaan rekisterinpitäjän on ilmoitettava rekisteröidyille kansallisen ja EU:n lainsäädännön mukaisesti täytäntöönpanomekanismeista henkilötietojen tietoturvaloukkausta koskevan ilmoituksen yhteydessä. Rekisterinpitäjän on ilmoitettava rekisteröidyille näiden oikeudesta tehdä henkilötietojen tietoturvaloukkauksesta valitus valvontaviranomaiselle ja tarvittaessa kansalliselle tuomioistuimelle[540]. Myös Euroopan neuvoston oikeudessa säädetään rekisteröityjen oikeudesta saada tietoa oikeuksiensa käyttämistä koskevista tavoista, muun muassa oikeudesta 9 artiklan 1 kohdan f alakohdassa tarkoitettuun oikeussuojakeinoon.

Poikkeukset informointivelvollisuuteen

Yleisessä tietosuoja-asetuksessa säädetään poikkeuksesta informointivelvollisuuteen. Yleisen tietosuoja-asetuksen 13 artiklan 4 kohdan ja 14 artiklan 5 kohdan mukaan velvollisuutta ilmoittaa rekisteröidyille ei sovelleta, jos rekisteröidyllä jo on kaikki asiaankuuluvat tiedot[541]. Jos taas henkilötietoja ei ole saatu rekisteröidyltä, informointivelvollisuutta ei sovelleta, jos tietojen antaminen on mahdotonta tai kohtuutonta, erityisesti, jos henkilötietoja käsitellään yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä ja historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten[542].

Jäsenvaltiot voivat lisäksi yleisen tietosuoja-asetuksen nojalla oman harkintansa mukaan rajoittaa asetuksen mukaisia velvollisuuksia ja yksilöille annettuja oikeuksia, jos se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide, jotta voidaan esimerkiksi taata kansallinen ja yleinen turvallisuus, puolustus, rikostutkinnan ja oikeudenkäyntien suojelu tai taloudellisten ja rahoituksellisten etujen suojelu sekä sellaisten yksityisten etujen suojelu, jotka ovat tärkeämpiä kuin tietosuojaa koskevat edut[543].

Kaikkien poikkeusten tai rajoitusten on oltava välttämättömiä demokraattisessa yhteiskunnassa ja oikeasuhteisia tavoitteeseen nähden. Erittäin poikkeuksellisissa

540 Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan d alakohta ja 14 artiklan 2 kohdan e alakohta; uudistettu yleissopimus 108, 8 artiklan 1 kohdan f alakohta.

541 *Ibid.*, 13 artiklan 4 kohta ja 14 artiklan 5 kohdan a alakohta.

542 *Ibid.*, 14 artiklan 5 kohdan b–e alakohta.

543 Yleinen tietosuoja-asetus, 23 artiklan 1 kohta.

tapauksissa, esimerkiksi lääketieteellisessä käytössä, rekisteröidyn suojelu itsessään voi edellyttää läpinäkyvyyden rajoittamista. Se koskee erityisesti jokaisen rekisteröidyn oikeutta tutustua tietoihin.[544] Suojan vähimmäistaso edellyttää, että kansallisessa lainsäädännössä on noudatettava keskeisiltä osin EU:n oikeudessa suojeltuja perusoikeuksia ja -vapauksia[545]. Tämä puolestaan edellyttää, että kansallisessa oikeudessa on erityisiä säännöksiä, joissa selkeytetään käsittelyn tarkoitusta, siihen kuuluvia henkilötietoryhmiä, suojatoimia ja muita menettelyyn liittyviä vaatimuksia[546].

Kun henkilötietoja kerätään yleisen edun mukaisia tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan säätää poikkeuksista informointivelvollisuuteen, jos se todennäköisesti estää erityisten tarkoitusten saavuttamisen tai vaikeuttaa sitä suuresti[547].

Euroopan neuvoston oikeudessa on samanlaisia rajoituksia. Sen mukaan rekisteröidyille uudistetun yleissopimuksen 108 9 artiklan nojalla myönnettyjä oikeuksia voidaan rajoittaa uudistetun yleissopimuksen 108 11 artiklan nojalla tiukoin ehdoin. Lisäksi uudistetun yleissopimuksen 108 8 artiklan 2 kohdan mukaan rekisterinpitäjille säädettyä velvollisuutta käsittelyn läpinäkyvyydestä ei sovelleta, kun rekisteröidyllä jo on tiedot.

Oikeus saada pääsy omiin tietoihin

Euroopan neuvoston oikeudessa oikeus saada pääsy omiin tietoihin tunnustetaan yksiselitteisesti uudistetun yleissopimuksen 108 9 artiklassa. Sen nojalla kaikilla henkilöillä on oikeus saada pyynnöstä tietoa omien henkilötietojensa käsittelystä, ja tiedot on annettava ymmärrettävällä tavalla. Tietojensaantioikeus on tunnustettu uudistetun yleissopimuksen 108 lisäksi myös Euroopan ihmisoikeustuomioistuimen oikeuskäytännössä. Ihmisoikeustuomioistuin on toistuvasti todennut, että yksilöllä on oikeus saada pääsy omiin henkilötietoihinsa ja että tämä oikeus perustuu siihen, että yksityiselämää on kunnioitettava[548]. Oikeutta päästä julkisten tai yksityisten

544 Yleinen tietosuoja-asetus, 15 artikla.

545 Yleinen tietosuoja-asetus, 23 artiklan 1 kohta.

546 *Ibid.*, 23 artiklan 2 kohta.

547 *Ibid.*, 89 artiklan 2 ja 3 kohta.

548 EIT, *Gaskin v. Yhdistynyt kuningaskunta*, nro 10454/83, 7.7.1989; EIT, *Odièvre v. Ranska*[suuri jaosto], nro 42326/98, 13.2.2003; EIT, *K.H. ym. v. Slovakia*, nro 32881/04, 28.4.2009; EIT, *Godelli v. Italia*, nro 33783/09, 25.9.2012.

organisaatioiden tallentamiin henkilötietoihin voidaan kuitenkin tietyissä olosuhteissa rajoittaa[549].

EU:n oikeudessa oikeus saada pääsy omiin tietoihin tunnustetaan yksiselitteisesti yleisen tietosuoja-asetuksen 15 artiklassa. Se esitetään myös henkilötietojen suojaa koskevan perusoikeuden osana EU:n perusoikeuskirjan 8 artiklan 2 kohdassa[550]. Yksilön oikeus saada pääsy omiin henkilötietoihinsa on keskeinen osa Euroopan tietosuojalainsäädäntöä[551].

Yleisen tietosuoja-asetuksen mukaan jokaiselle rekisteröidyllä on oikeus saada pääsy omiin henkilötietoihinsa sekä tiettyjä käsittelyä koskevia tietoja, jotka rekisterinpitäjien on annettava[552]. Jokaisella rekisteröidyllä on erityisesti oikeus saada (rekisterinpitäjältä) vahvistus siitä, että häntä koskevia henkilötietoja käsitellään tai että niitä ei käsitellä, ja tiedot ainakin seuraavista:

- käsittelyn tarkoitukset
- kyseessä olevat henkilötietoryhmät
- vastaanottajat tai vastaanottajaryhmät, joille henkilötietoja on luovutettu tai on tarkoitus luovuttaa
- henkilötietojen suunniteltu säilytysaika tai jos se ei ole mahdollista, tämän ajan määrittämiskriteerit
- oikeus pyytää henkilötietojen oikaisemista tai poistamista taikka henkilötietojen käsittelyn rajoittamista
- oikeus tehdä valitus valvontaviranomaiselle

549 EIT, *Leander v. Ruotsi*, nro 9248/81, 26.3.1987.

550 Ks. myös EUT, yhdistetyt asiat C-141/12 ja C-372/12, *YS vastaan Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vastaan M ja S*, 17.7.2014; CJEU, C-615/13 P, *ClientEarth ja Pesticide Action Network Europe (PAN Europe) vastaan Euroopan elintarviketurvallisuusviranomainen, Euroopan komissio*, 16.7.2015.

551 EUT, yhdistetyt asiat C-141/12 ja C-372/12, *YS vastaan Minister voor Immigratie, Integratie en Asiel* ja *Minister voor Immigratie, Integratie en Asiel vastaan M ja S*, 17.7.2014.

552 Yleinen tietosuoja-asetus, 15 artiklan 1 kohta.

- kaikki käsiteltävien tietojen alkuperästä käytettävissä olevat tiedot, jos tietoja ei kerätä rekisteröidyltä

- automaattisen päätöksenteon tapauksessa automaattiseen tietojenkäsittelyyn liittyvä logiikka.

Rekisterinpitäjän on toimitettava rekisteröidylle jäljennös käsiteltävistä henkilötiedoista. Kaikki rekisteröidyille toimitettavat tiedot on annettava helposti ymmärrettävässä muodossa, mikä tarkoittaa, että rekisterinpitäjän on varmistettava, että rekisteröity pystyy ymmärtämään annetut tiedot. Vastaukseksi pääsyä koskevaan pyyntöön eivät esimerkiksi tavallisesti riitä tekniset lyhenteet, koodatut termit tai akronyymit, paitsi jos niiden merkitys selitetään. Kun käytetään automaattista päätöksentekoa, muun muassa profilointia, automaattiseen päätöksentekoon liittyvä yleinen logiikka on selitettävä, samoin kuin rekisteröidyn arvioinnissa käytetyt perusteet. **Euroopan neuvoston oikeudessa** on olemassa samanlaisia vaatimuksia[553].

Esimerkki: Henkilötietoihin pääsyä koskevaa oikeutta käyttämällä rekisteröity voi varmistaa, että tiedot pitävät paikkansa. Siksi on olennaisen tärkeää, että rekisteröidyille ilmoitetaan helposti ymmärrettävällä tavalla käsiteltävien henkilötietojen lisäksi myös ryhmät, joissa henkilötietoja käsitellään, kuten nimi, IP-osoite, geopaikannuksen koordinaatit, luottokortin numero jne.

Kun tietoja ei ole kerätty rekisteröidyltä, tietoihin pääsyä koskevaan pyyntöön annettavassa vastauksessa on kerrottava tietojen alkuperä, jos se vain on mahdollista. Tässä yhteydessä on otettava huomioon kohtuullisuuden, läpinäkyvyyden ja osoitusvelvollisuuden periaatteet. Rekisterinpitäjä ei saa tuhota tietoa henkilötietojen alkuperästä välttyäkseen sen paljastamiselta – ellei niitä olisi tuhottu ilman pääsyä koskevaa pyyntöäkin – eikä laiminlyödä oman alansa tavanomaisia vaatimuksia ”vastuullisuudesta”.

Kuten Euroopan unionin tuomioistuimen oikeuskäytännössä on korostettu, oikeutta tutustua omiin henkilötietoihin ei voi perusteettomasti rajoittaa ajallisesti. Rekisteröidyillä on myös oltava kohtuulliset mahdollisuudet saada tietoa aiemmista henkilötietojen käsittelytoimista.

553 Ks. uudistettu yleissopimus 108, 8 artiklan 1 kohdan c alakohta.

Esimerkki: Asiassa *Rijkeboer*[554] Euroopan unionin tuomioistuinta pyydettiin selvittämään, voidaanko henkilön oikeus saada tietoja häntä koskevien henkilötietojen vastaanottajista tai vastaanottajaryhmistä sekä tietojen sisällöstä rajoittaa hänen tiedonsaantihakemustaan edeltävään vuoden jaksoon.

Sen ratkaisemiseksi, mahdollistetaanko EU:n lainsäädännössä tällainen ajallinen rajoittaminen, tuomioistuin päätti tulkita kyseistä artiklaa direktiivin tarkoituksia vasten. Tuomioistuin totesi ensinnäkin, että tiedonsaantioikeus on välttämätön, jotta rekisteröity voi käyttää oikeuttaan saada rekisterinpitäjä oikaisemaan, poistamaan tai suojaamaan hänen tietonsa tai ilmoittamaan sivullisille, joille tietoja on luovutettu, näistä oikaisuista, poistamisista tai suojaamisista. Tehokas tiedonsaantioikeus on myös välttämätön, jotta rekisteröity voi käyttää oikeuttaan vastustaa henkilötietojensa käsittelyä tai tehdä valitus ja vaatia korvauksia.[555]

Euroopan unionin tuomioistuin totesi, että rekisteröidyille annettujen oikeuksien käytännön vaikutuksen varmistamiseksi ”tämän oikeuden on välttämättä koskettava mennyttä aikaa. Jos näin ei olisi, rekisteröity ei voisi tehokkaalla tavalla käyttää oikeuttaan saada laittomiksi tai paikkansapitämättömiksi oletettuja tietoja oikaistuksi, poistetuksi tai suojatuksi tai käyttää oikeussuojakeinoa ja saada korvausta kärsimästään vahingosta.”

6.1.2 Oikeus tietojen oikaisemiseen

EU:n oikeudessa ja **Euroopan neuvoston oikeudessa** rekisteröidyillä on oikeus saada henkilötietonsa oikaistuiksi. Henkilötietojen paikkansapitävyys on keskeistä rekisteröityjen korkeatasoisen tietosuojan varmistamisessa[556].

Esimerkki: Asiassa *Ciubotaru v. Moldova*[557] kantajan pyyntö hänen etnistä alkuperäänsä koskevan merkinnän muuttamisesta virallisissa rekistereissä moldovalaisesta romanialaiseksi oli evätty sillä perusteella, ettei hän ollut

554 EUT, C-553/07, *College van burgemeester en wethouders van Rotterdam vastaan E. E. Rijkeboer*, 7.5.2009.

555 Yleinen tietosuoja-asetus, 15 artiklan 1 kohdan c ja f alakohta, 16 artikla, 17 artiklan 2 kohta ja 21 artikla sekä VIII luku.

556 *Ibid.*, 16 artikla ja johdanto-osan 65 kappale; uudistettu yleissopimus 108, 9 artiklan 1 kohdan e alakohta.

557 EIT, *Ciubotaru v. Moldova*, nro 27138/04, 27.4.2010, 51 ja 59 kohta.

esittänyt todisteita pyyntönsä tueksi. Euroopan ihmisoikeustuomioistuin piti hyväksyttävänä sitä, että valtio pyytää rekisteröintiä varten objektiivista näyttöä henkilön etnisestä alkuperästä. Viranomaiset voisivat evätä pyynnön, joka perustuisi puhtaasti subjektiivisiin ja toteennäyttämättömiin väitteisiin. Kantajan pyyntö oli kuitenkin perustunut muuhunkin kuin subjektiiviseen näkemykseen omasta etnisyydestä; hän oli pystynyt esittämään objektiivisesti varmistettavissa olevia yhteyksiä romanialaisten etniseen ryhmään, kuten kielen, nimen ja yhteenkuuluvuuden tunteen. Kansallisen lain mukaan kantajan olisi kuitenkin pitänyt esittää todisteita siitä, että hänen vanhempansa olivat kuuluneet romanialaisten etniseen ryhmään. Moldovan historiallisen tilanteen takia tämä vaatimus oli muodostunut ylitsepääsemättömäksi esteeksi muun etnisen alkuperän rekisteröimiselle kuin sen, jonka Neuvostoliiton viranomaiset olivat kirjanneet kantajan vanhemmille. Epäämällä kantajalta mahdollisuuden hänen pyyntönsä tarkastelemiseen objektiivisesti varmistettavissa olevien todisteiden valossa valtio oli jättänyt noudattamatta positiivista velvollisuuttaan varmistaa kantajalle yksityiselämän kunnioitus. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Joissakin tapauksissa riittää, että rekisteröity pyytää esimerkiksi nimen kirjoitusasun oikaisemista tai osoitteen tai puhelinnumeron muuttamista. **EU:n oikeuden** ja **Euroopan neuvoston oikeuden** mukaan virheelliset henkilötiedot on oikaistava ilman tarpeetonta tai liiallista viivytystä[558]. Jos tällaiset pyynnöt liittyvät oikeudellisesti merkittäviin kysymyksiin, kuten rekisteröidyn oikeushenkilöllisyyteen tai oikeaan asuinpaikkaan oikeusasiakirjojen toimittamista varten, pelkkä oikaisupyyntö ei kuitenkaan välttämättä riitä ja rekisterinpitäjällä voi olla oikeus pyytää näyttöä väitetystä virheestä. Tällaisesta pyynnöstä ei saa aiheutua rekisteröidylle kohtuutonta todistustaakkaa, joka estäisi rekisteröityä saamasta tietojaan oikaistuiksi. Euroopan ihmisoikeustuomioistuin on todennut, että ihmisoikeussopimuksen 8 artiklaa on rikottu monessa sellaisessa tapauksessa, jossa kantaja ei ole pystynyt kyseenalaistamaan salaisten rekisterien sisältämien tietojen täsmällisyyttä[559].

558 Yleinen tietosuoja-asetus, 16 artikla, uudistettu yleissopimus 108, 9 artiklan 1 kohta.

559 EIT, *Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000.

Esimerkki: Asiassa *Cemalettin Canli v. Turkki*[560] Euroopan ihmisoikeustuomioistuin totesi, että poliisin virheellinen raportointi rikosoikeudenkäynnissä oli rikkonut ihmisoikeussopimuksen 8 artiklaa.

Kantaja oli ollut kaksi kertaa syytettynä laittoman järjestön jäsenyydestä, mutta häntä ei ollut koskaan tuomittu. Kun kantaja jälleen kerran pidätettiin ja asetettiin syytteeseen uudesta rikoksesta, poliisi toimitti rikostuomioistuimelle raportin, jonka otsikkona oli "*tietoja muista rikoksista*" ja jossa kantaja esitettiin kahden laittoman järjestön jäsenenä. Kantajan pyyntö saada raportti ja poliisin rekisteritiedot muutettua evättiin. Euroopan ihmisoikeustuomioistuin katsoi, että poliisin raportin tiedot kuuluivat ihmisoikeussopimuksen 8 artiklan soveltamisalaan, sillä julkisetkin tiedot voivat kuulua "yksityiselämän" piiriin, kun viranomaiset ovat keränneet ja säilyttäneet niitä järjestelmällisesti. Lisäksi poliisin raportti oli virheellinen ja se oli laadittu ja toimitettu rikostuomioistuimelle kansallisen lainsäädännön vastaisesti. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Siviiliriita-asioissa tai viranomaiskäsittelyissä, joissa päätetään, pitävätkö tiedot paikkansa, rekisteröity voi pyytää merkitsemään tietoihinsa, että niiden paikkansapitävyys on riitautettu ja että virallista päätöstä odotetaan[561]. Rekisterinpitäjä ei saa sillä aikaa esittää tietoja oikeina tai muuttumattomina, etenkään kolmansille osapuolille.

6.1.3 Oikeus tietojen poistamiseen ("oikeus tulla unohdetuksi")

Rekisteröityjen oikeus saada omat tietonsa poistetuksi on erityisen tärkeää tietosuojaperiaatteiden ja etenkin tietojen minimoinnin periaatteen (henkilötietojen on rajoituttava siihen, mikä on välttämätöntä tietojen käsittelyn tarkoituksen saavuttamiseksi) tehokasta soveltamista varten. Oikeudesta tietojen poistamiseen säädetään siksi sekä Euroopan neuvoston että EU:n säädöksissä[562].

560 EIT, *Cemalettin Canli v. Turkki*, nro 22427/04, 18.11.2008, 33 ja 42–43 kohta; EIT, *Dalea v. Ranska*, nro 964/07, 2.2.2010.

561 Yleinen tietosuoja-asetus, 18 artikla ja johdanto-osan 67 kappale.

562 *Ibid.*, 17 artikla.

Esimerkki: Asiassa *Segerstedt-Wiberg ym. v. Ruotsi*[563] kantajat olivat kuuluneet tiettyihin liberaaleihin ja kommunistisiin puolueisiin. He epäilivät, että heitä koskevia tietoja oli kirjattu turvallisuuspoliisin rekisteriin, ja pyysivät niiden poistamista. Euroopan ihmisoikeustuomioistuin totesi, että tietojen tallentamisella oli ollut oikeudellinen peruste ja laillinen tarkoitus. Tuomioistuin kuitenkin katsoi, että joidenkin kantajien kohdalla tietojen säilyttäminen edelleen loukkasi suhteettomasti heidän yksityiselämäänsä. Yksi kantaja esimerkiksi oli viranomaisten tietojen mukaan vuonna 1969 kannattanut poliisin väkivaltaista vastustamista mielenosoituksissa. Tuomioistuimen mielestä tällaisella tiedolla ei voinut olla suurta merkitystä kansalliselle turvallisuudelle, etenkään sen historiallisen luonteen vuoksi. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu neljän kantajan kohdalla viidestä, sillä heidän tiedoillaan ei ollut merkitystä, koska niitä koskevista toimista oli kulunut kauan aikaa.

Esimerkki: Asiassa *Brunet v. Ranska*[564] kantajat vaativat kieltämään heidän henkilötietojensa säilyttämisen poliisin tietokannassa, jossa oli tietoa tuomituista henkilöistä, syytetyistä henkilöistä ja uhreista. Kantajan tiedot olivat edelleen tietokannassa, vaikka rikosoikeudenkäynti häntä vastaan oli keskeytetty. Euroopan ihmisoikeustuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu. Johtopäätöksen aikaansaamiseksi tuomioistuin otti huomioon, että käytännössä kantajalla ei ollut mahdollisuutta saada henkilötietojaan poistetuksi tietokannasta. Tuomioistuin otti huomioon tietokannassa olevien tietojen luonteen ja katsoi, että ne loukkasivat kantajan yksityisyyttä, koska ne sisälsivät yksityiskohtia hänen henkilöllisyydestään ja persoonallisuudestaan. Se totesi lisäksi, että henkilötietojen 20 vuoden säilyttämisaika tietokannassa oli liian pitkä etenkin, kun kantajaa ei ollut ikinä tuomittu oikeudessa.

Uudistetussa yleissopimuksessa 108 tunnustetaan nimenomaisesti, että jokaisella henkilöllä on oikeus virheellisten, valheellisten tai lainvastaisesti käsiteltyjen tietojen poistamiseen[565].

563 EIT, *Segerstedt-Wiberg ym. v. Ruotsi*, nro 62332/00, 6.6.2006, 89 ja 90 kohta; ks. myös esim., EIT, *M.K. v. Ranska*, nro 19522/09, 18.4.2013.

564 EIT, *Brunet v. Ranska*, nro 21010/10, 18.9.2014.

565 Uudistettu yleissopimus 108, 9 artiklan 1 kohdan e alakohta.

EU:n oikeudessa yleisen tietosuoja-asetuksen 17 artiklan vahvistetaan rekisteröidyn oikeus pyytää tietojensa poistamista. Oikeutta saada omat henkilötiedot poistetuksi ilman aiheetonta viivytystä sovelletaan, kun

- henkilötietoja ei enää tarvita niihin tarkoituksiin, joita varten ne kerättiin tai joita varten niitä muutoin käsiteltiin
- rekisteröity peruuttaa suostumuksen, johon käsittely on perustunut, eikä käsittelyyn ole muuta laillista perustetta
- rekisteröity vastustaa käsittelyä eikä käsittelyyn ole olemassa perusteltua syytä
- henkilötietoja on käsitelty lainvastaisesti
- henkilötiedot on poistettava unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan rekisterinpitäjään sovellettavan lakisääteisen velvoitteen noudattamiseksi
- henkilötiedot on kerätty yleisen tietosuoja-asetuksen 8 artiklassa tarkoitetun tietoyhteiskunnan palvelujen tarjoamisen yhteydessä[566].

Todistustaakka henkilötietojen käsittelyn laillisuudesta on rekisterinpitäjillä, koska ne ovat vastuussa käsittelyn lainmukaisuudesta[567]. Osoitusvelvollisuuden periaatteen mukaan rekisterinpitäjän on pystyttävä milloin tahansa osoittamaan, että sen suorittamalle henkilötietojen käsittelylle on pätevä oikeusperusta, tai käsittely on lopetettava[568]. Yleisessä tietosuoja-asetuksessa määritetään poistamisoikeutta koskevat poikkeukset, muun muassa silloin kuin henkilötietojen käsittely on tarpeen

- sananvapautta ja tiedonvälityksen vapautta koskevan oikeuden käyttämiseksi
- rekisterinpitäjään sovellettavaan unionin oikeuteen tai jäsenvaltion lainsäädäntöön perustuvan, käsittelyä edellyttävän lakisääteisen velvoitteen noudattamiseksi tai jos käsittely tapahtuu yleistä etua koskevan tehtävän suorittamista tai rekisterinpitäjälle kuuluvan julkisen vallan käyttämistä varten

566 Yleinen tietosuoja-asetus, 17 artiklan 1 kohta.

567 *Ibid.*

568 *Ibid.*, 5 artiklan 2 kohta.

- kansanterveyteen liittyvää yleistä etua koskevista syistä
- yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten
- oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi[569].

Euroopan unionin tuomioistuin on vahvistanut poistamisoikeuden merkityksen korkeatasoisen tietosuojan varmistamisessa.

Esimerkki: Asiassa *Google Spain*[570] Euroopan unionin tuomioistuin pohti, pitikö Googlen poistaa kantajan taloudellisia vaikeuksia koskevat vanhentuneet tiedot hakutulosten luettelostaan. Google riitautti muun muassa vastuunsa ja väitti vain antavansa linkin julkaisijan verkkosivustolle, jolla tiedot ovat, tässä tapauksessa sanomalehteen, joka kertoi kantajan maksukyvyttömyysongelmista[571]. Google katsoi, että pyyntö vanhentuneiden tietojen poistamiseen verkkosivulta pitäisi tehdä verkkosivun ylläpitäjälle eikä Googlelle, joka vain antaa linkin alkuperäiselle sivulle. Euroopan unionin tuomioistuin totesi, että kun Google hakee verkosta tietoa ja verkkosivuja ja indeksoi sisällön hakutulosten antamiseksi, siitä tulee rekisterinpitäjä, johon sovelletaan EU:n oikeuden mukaisia vastuita ja velvollisuuksia.

Euroopan unionin tuomioistuin selvensi, että internetin hakukoneiden ja henkilötietoja antavien hakutulosten avulla voidaan laatia yksityiskohtainen profiili yksilöstä[572]. Hakukoneiden avulla hakutulosten luetteloihin sisältyvistä tiedoista tulee sellaisia, että niitä voidaan katsella kaikkialla. Tämän puuttumisen potentiaalisen vakavuuden vuoksi sitä ei voida perustella hakukoneen ylläpitäjällä tällaiseen käsittelyyn olevalla pelkällä taloudellisella

569 *Ibid.*, 17 artiklan 3 kohta.

570 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 55–58 kohta.

571 Google riitautti myös EU:n tietosuojasääntöjen soveltamisen sillä perusteella, että Google Inc. on sijoittautunut Yhdysvaltoihin ja että myös kyseessä olevien henkilötietojen käsittely tehtiin Yhdysvalloissa. Toinen perustelu EU:n tietosuojalainsäädännön soveltamattomuudesta liittyi väitteeseen siitä, että hakukoneita ei voida pitää ”rekisterinpitäjinä” niiden tuloksissa näkyvien tietojen osalta, koska niillä ei ole tietämystä mainituista tiedoista eikä niillä ole niihin määräysvaltaa. Euroopan unionin tuomioistuin hylkäsi molemmat perustelut, koska se katsoi, että direktiivi 95/46/EY oli sovellettavissa kyseisessä asiassa, ja jatkoi sen takaamien oikeuksien, erityisesti henkilötietojen poistamista koskevan oikeuden, soveltamisalan tutkimista.

572 *Ibid.*, 36, 38, 80–81 ja 97 kohta.

intressillä. On pyrittävä löytämään oikeudenmukainen tasapaino internetin käyttäjien tietojen saamista koskevan oikeutetun intressin ja rekisteröidyllä perusoikeuskirjan 7 ja 8 artiklan nojalla olevien perusoikeuksien välillä. Koska yhteiskunta digitalisoituu jatkuvasti enemmän, vaatimus siitä, että henkilötiedot ovat täsmällisiä ja että niiden osalta ei mennä pidemmälle kuin on välttämätöntä (eli annetaan tiedot yleisölle), on olennainen yksilöiden tietosuojan korkean tason varmistamisessa. Hakukoneen ylläpitäjän on ”rekisterinpitäjänä varmistettava vastuidensa, valtuuksiensa ja mahdollisuuksiensa yhteydessä se, että käsittely täyttää [EU:n lainsäädännön] vaatimukset”, jotta takeet saavat täyden vaikutuksensa.[573] Tämä tarkoittaa sitä, että oikeus saada omat henkilötietonsa poistetuiksi, kun käsittely on vanhentunut tai se ei ole enää tarpeen, koskee myös rekisterinpitäjiä, jotka julkaisevat tiedot muilla sivustoilla.[574]

Tutkiessaan, pitääkö Googlen poistaa kantajaan liittyvät linkit, Euroopan unionin tuomioistuin katsoi, että tietyissä olosuhteissa yksilöillä on oikeus pyytää henkilötietojensa poistamista. Tähän oikeuteen voidaan vedota, kun yksilöön liittyvät tiedot ovat virheellisiä, epäasianmukaisia tai epäolennaisia tai ne ovat liian laajoja siihen tarkoitukseen, jossa niitä käsitellään. Euroopan unionin tuomioistuin tunnusti, että tämä oikeus ei ole ehdoton. Sitä on punnittava suhteessa muihin oikeuksiin ja etuihin, erityisesti suuren yleisön tietojen saamista koskevaan etuun. Kaikki poistamispyynnöt on arvioitava tapauskohtaisesti, jotta saadaan tasapaino aikaan toisaalta rekisteröidyn henkilötietojen suojaa ja yksityis- ja perhe-elämän kunnioitusta koskevien perusoikeuksien ja toisaalta kaikkien internetin käyttäjien, myös julkaisijoiden, oikeutettujen etujen välillä. Tuomioistuin antoi ohjeita tekijöistä, jotka on otettava punninnassa huomioon. Kyseessä olevien tietojen luonne on erityisen tärkeä tekijä. Jos tiedot liittyvät yksilön yksityiselämään ja jos tietojen saatavuus ei ole yleisen edun mukaista, tietosuoja ja yksityisyydensuoja ohittaisivat suuren yleisön tiedonsaantioikeuden. Jos taas osoittautuu, että rekisteröity on julkisuuden henkilö tai että tietojen luonne oikeuttaa niiden

573 *Ibid.*, 81–83 kohta.

574 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 88 kohta. Ks. myös tietosuojatyöryhmä (2014), *Guidelines on the implementation of the CJEU judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González” C-131/12*, WP 225, Bryssel, 26.11.2014 ja ministerikomitean suositus CM/Rec 2012(3) jäsenvaltioille ihmisoikeuksien suojelusta hakukoneiden osalta, 4.4.2012.

antamisen suuren yleisön saataville, silloin suuren yleisön ensisijaisella intressillä saada tietoa voidaan oikeuttaa puuttuminen rekisteröidyn tietosuojaa ja yksityisyydensuojaa koskeviin perusoikeuksiin.

Tietosuojatyöryhmä antoi tuomion perusteella ohjeet Euroopan unionin tuomioistuimen päätöksen täytäntöönpanosta[575]. Ohjeissa on luettelo yleisistä kriteereistä, joita valvontaviranomaiset voivat käyttää käsitellessään kanteluita, jotka liittyvät yksilöiden esittämiin poistamispyyntöihin, ja niissä selitetään, mitä poistamisoikeuteen sisältyy. Viranomaiset voivat käyttää kriteereitä myös ohjeina oikeuksien punninnassa. Ohjeissa toistetaan, että arviointi on tehtävä tapauskohtaisesti. Koska oikeus tulla unohdetuksi ei ole ehdoton, pyynnön tulos voi eri tapauksissa olla erilainen. Tätä havainnollistaa myös Euroopan unionin tuomioistuimen oikeuskäytäntö Googlen tapauksen jälkeen.

Esimerkki: Asiassa *Camera di Commercio di Lecce vastaan Manni*[576] Euroopan unionin tuomioistuimen piti tutkia, oliko yksilöllä oikeus saada henkilötietonsa poistetuksi julkisesta yhtiörekisteristä, kun hänen yhtiönsä oli purkautunut. Salvatore Manni oli pyytänyt Leccen kauppakamaria poistamaan hänen henkilötietonsa kyseisestä rekisteristä, kun hän oli havainnut, että mahdolliset asiakkaat tutustuisivat rekisteriin ja näkisivät, että hän oli ollut aiemmin konkurssipesän hoitaja yhtiössä, joka oli julistettu konkurssiin yli kymmenen vuotta sitten. Kantaja katsoi, että nämä tiedot karkottaisivat mahdolliset asiakkaat.

Punnitessaan Mannin oikeutta henkilötietojen suojaan ja suuren yleisön tietojen saamista koskevaa intressiä Euroopan unionin tuomioistuin tutki ensin julkisen yhtiörekisterin tarkoitusta. Se huomautti, että tietojen julkistamisesta säädettiin lailla ja erityisesti EU:n direktiivillä, jonka tavoitteena on edesauttaa yhtiöitä koskevien tietojen saamista ulkopuolisten henkilöiden saataville helpommin. Yhtiön perusasiakirjojen ja muiden yhtiötä koskevien tietojen pitäisi siis olla kolmansien osapuolien käytettävissä, ja näiden pitäisi pystyä tutustumaan tietoihin ”erityisesti siitä, keillä on oikeus edustaa yhtiötä”.

575 Tietosuojatyöryhmä (2014), *Guidelines on the implementation of the CJEU judgment on “Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González”* C-131/12, WP 225, Bryssel, 26.11.2014.

576 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9.3.2017.

Julkistamisen tarkoituksena oli myös turvata oikeusvarmuus jäsenvaltioiden välisten liiketoimien lisääntyessä varmistamalla, että kolmansilla osapuolilla on käytettävissään kaikki merkitykselliset tiedot yhtiöistä koko EU:ssa.

Euroopan unionin tuomioistuin pani lisäksi merkille, että tietyn ajan kuluttua ja yhtiön purkautumisen jälkeenkin yhtiötä koskevia oikeuksia ja oikeussuhteita voi edelleen olla olemassa. Purkautumista koskevat kiistat voivat olla pitkiä, ja yhtiötä, sen johtajia ja selvitysmiehiä koskevia kysymyksiä voi tulla esiin vielä useita vuosia kyseisen yhtiön olemassaolon lakkaamisen jälkeen. Euroopan unionin tuomioistuin totesi, että lukuisten mahdollisten tilanteiden ja kussakin jäsenvaltiossa säädettyjen vanhentumisaikojen erojen vuoksi ”vaikuttaa siltä, että tällä hetkellä on mahdotonta yksilöidä yhtä ainoaa yhtiön purkautumisesta laskettavaa määräaikaa, jonka päätyttyä henkilötietojen merkitseminen rekisteriin ja niiden julkistaminen eivät olisi enää tarpeen”. Koska julkaisemisella on perusteltu tarkoitus ja koska on vaikeaa määrittää aikaa, jonka päätyttyä henkilötiedot voitaisiin poistaa rekisteristä aiheuttamatta haittaa kolmansien osapuolien eduille, Euroopan unionin tuomioistuin totesi, että EU:n tietosuojasäännöt eivät takaa oikeutta henkilöiden henkilötietojen poistamiseen Salvatore Mannin tilanteessa.

Kun rekisterinpitäjä on antanut henkilötiedot julkisesti saataville ja sen on poistettava tiedot, rekisterinpitäjän on toteutettava ”kohtuulliset” toimenpiteet ilmoittaakseen muille samoja henkilötietoja käsitteleville rekisterinpitäjille rekisteröidyn poistamispyynnöstä. Rekisterinpitäjän toimissa on otettava huomioon käytettävissä oleva teknologia ja toteuttamiskustannukset[577].

6.1.4 Oikeus käsittelyn rajoittamiseen

Yleisen tietosuoja-asetuksen 18 artiklassa annetaan rekisteröidyille oikeus rajoittaa rekisterinpitäjän suorittamaa heidän henkilötietojensa käsittelyä tilapäisesti. Rekisteröidyt voivat pyytää rekisterinpitäjää rajoittamaan käsittelyä, kun

- henkilötietojen paikkansapitävyys kiistetään
- käsittely on lainvastaista ja rekisteröity vaatii henkilötietojen käytön rajoittamista niiden poistamisen sijaan

577 Yleinen tietosuoja-asetus, 17 artiklan 2 kohta ja johdanto-osan 66 kappale.

- tiedot on säilytettävä oikeudellisen vaateen esittämiseksi tai puolustamiseksi
- käsiteltävänä on päätös siitä, syrjäyttävätkö rekisterinpitäjän oikeutetut perusteet rekisteröidyn perusteet[578].

Menetelmiä, joilla rekisterinpitäjä voi rajoittaa henkilötietojen käsittelyä, voivat olla muun muassa valittujen tietojen väliaikainen siirtäminen toiseen käsittelyjärjestelmään, käyttäjien pääsyn estäminen henkilötietoihin tai henkilötietojen väliaikainen poistaminen[579]. Rekisterinpitäjän on ilmoitettava rekisteröidylle ennen kuin käsittelyä koskeva rajoitus poistetaan[580].

Henkilötietojen oikaisua tai poistoa tai käsittelyn rajoitusta koskeva ilmoitusvelvollisuus

Rekisterinpitäjän on ilmoitettava kaikenlaisista henkilötietojen oikaisuista, poistoista tai käsittelyn rajoituksista jokaiselle vastaanottajalle, jolle henkilötietoja on luovutettu, mikäli se ei ole mahdotonta tai vaadi kohtuutonta vaivaa[581]. Jos rekisterinpitäjä pyytää tietoa kyseisistä vastaanottajista, rekisterinpitäjän on annettava hänelle kyseiset tiedot[582].

6.1.5 Oikeus siirtää tiedot järjestelmästä toiseen

Yleisen tietosuoja-asetuksen mukaan rekisteröidyillä on oikeus siirtää tiedot järjestelmästä toiseen, kun heidän rekisterinpitäjälle toimittamiaan henkilötietoja käsitellään automaattisesti suostumuksen perusteella tai kun henkilötietojen käsittely on tarpeen sopimuksen täytäntöönpanemiseksi ja käsittely suoritetaan automaattisesti. Tämä tarkoittaa, että oikeutta siirtää tiedot järjestelmästä toiseen ei sovelleta tilanteissa, joissa henkilötietoja käsitellään muun laillisen perusteen kuin suostumuksen tai sopimuksen nojalla.[583]

Jos oikeutta siirtää tiedot järjestelmästä toiseen sovelletaan, rekisteröidyillä on oikeus saada henkilötietonsa siirrettyä suoraan rekisterinpitäjältä toiselle, jos se on

578 *Ibid.*, 18 artiklan 1 kohta.
579 *Ibid.*, johdanto-osan 67 kappale.
580 *Ibid.*, 18 artiklan 3 kohta.
581 *Ibid.*, 19 artikla.
582 *Ibid.*
583 *Ibid.*, johdanto-osan 68 kappale ja 20 artiklan 1 kohta.

teknisesti mahdollista[584]. Tämän helpottamiseksi rekisterinpitäjien olisi kehitettävä yhteentoimivia muotoja, jotka mahdollistavat rekisteröityjen tietojen siirtämisen[585]. Yleisessä tietosuoja-asetuksessa täsmennetään, että näiden muotojen on oltava jäsenneltyjä, yleisesti käytettyjä ja koneellisesti luettavia yhteentoimivuuden helpottamiseksi[586]. Yhteentoimivuus voidaan määritellä laajasti mahdollisuudeksi vaihtaa ja jakaa tietoja tietojärjestelmien välillä[587]. Vaikka käytettävien muotojen tarkoituksena on saada aikaan yhteentoimivuus, yleisessä tietosuoja-asetuksessa ei anneta nimenomaisia suosituksia erityisestä muodosta: muodot voivat vaihdella aloittain[588].

Tietosuojatyöryhmän ohjeiden mukaan oikeus siirtää tiedot järjestelmästä toiseen ”lisää käyttäjän valinta-, valvonta- ja vaikutusmahdollisuuksia”, ja sen tavoitteena on antaa rekisteröidyille määräysvaltaa omiin henkilötietoihinsa[589]. Ohjeissa selvennetään tietojen siirrettävyyden keskeiset osatekijät, joita ovat muun muassa

- rekisteröityjen oikeus saada itseään koskevat rekisterinpitäjän käsittelemät henkilötiedot jäsennellyssä, yleisesti käytetyssä, koneellisesti luettavassa ja yhteentoimivassa muodossa

- oikeus siirtää henkilötietoja rekisterinpitäjältä toiselle rekisterinpitäjän esteettä, jos se on teknisesti mahdollista

- rekisterinpitojärjestelmä – kun rekisterinpitäjä vastaa tietojen siirtämistä koskevaan pyyntöön, se toimii rekisteröidyn ohjeiden mukaisesti eli se ei ole vastuussa siitä, että vastaanottaja noudattaa tietosuojalainsäädäntöä, koska rekisteröity valitsee, kenelle tiedot siirretään

- oikeus siirtää tietoja järjestelmästä toiseen ei rajoita minkään muun oikeuden käyttöä, kuten on myös yleisen tietosuoja-asetuksen muiden oikeuksien tapauksessa.

584 *Ibid.*, 20 artiklan 2 kohta.

585 *Ibid.*, johdanto-osan 68 kappale ja 20 artiklan 1 kohta.

586 *Ibid.*, johdanto-osan 68 kappale.

587 Euroopan komissio, Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi, COM(2016) 205 final, 6.4.2016.

588 Tietosuojatyöryhmä (2016), *oikeutta tietojen siirtämiseen järjestelmästä toiseen koskevat ohjeet*, WP 242, 13.12.2016, viimeksi tarkistettu ja hyväksytty 5.4.2017, s. 13.

589 *Ibid.*

6.1.6 Vastustamisoikeus

Rekisteröidyllä on oikeus vastustaa häntä koskevien henkilötietojen käsittelyä henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella tai jos tietoja käsitellään suoramarkkinointitarkoituksia varten. Vastustamisoikeutta voi käyttää automaattisesti.

Oikeus vastustaa tietojenkäsittelyä rekisteröidyn erityiseen tilanteeseen liittyvällä perusteella

Rekisteröidyillä ei ole yleistä oikeutta vastustaa henkilötietojensa käsittelyä[590]. Yleisen tietosuoja-asetuksen 21 artiklan 1 kohdassa rekisteröidylle annetaan oikeus esittää vastalauseita henkilökohtaiseen erityiseen tilanteeseensa liittyvällä perusteella, kun käsittelyn oikeusperusta on se, että rekisterinpitäjä käsittelee tietoja yleistä etua koskevan tehtävän suorittamiseksi tai se, että käsittely perustuu rekisterinpitäjän oikeutettuihin etuihin[591]. Vastustamisoikeus koskee profilointitoimia. Uudistetussa yleissopimuksessa 108 on tunnustettu samanlainen oikeus[592].

Rekisteröidyn erityiseen tilanteeseen perustuvalla vastustamisoikeudella pyritään saattamaan tasapainoon rekisteröidyn tietosuojaa koskevat oikeudet ja muiden lailliset oikeudet käsitellä rekisteröidyn henkilötietoja. Euroopan unionin tuomioistuin on kuitenkin selventänyt, että rekisteröidyn oikeudet syrjäyttävät ”pääsääntöisesti” rekisterinpitäjän taloudelliset intressit. Se riippuu ”kyseessä olevien tietojen luonteesta ja niiden arkaluonteisuudesta rekisteröidyn yksityiselämän kannalta sekä yleisöllä olevasta intressistä saada kyseiset tiedot käyttöönsä”[593]. Yleisen tietosuoja-asetuksen mukaan todistustaakka on rekisterinpitäjillä, joiden on osoitettava, että käsittelyn jatkamiselle on huomattavan tärkeä syy[594]. Myös uudistetun yleissopimuksen 108 selitysmuistiossa selvennetään, että tietojenkäsittelylle on

590 Ks. myös EIT, *M.S. v. Ruotsi*, nro 20837/92, 27.8.1997 (jossa potilastietoja luovutettiin ilman suostumusta tai vastustamismahdollisuutta); EIT, *Leander v. Ruotsi*, nro 9248/81, 26.3.1987; EIT, *Mosley v. Yhdistynyt kuningaskunta*, nro 48009/08, 10.5.2011.

591 Yleinen tietosuoja-asetus, johdanto-osan 69 kappale, 6 artiklan 1 kohdan e ja f alakohta.

592 Uudistettu yleissopimus 108, 9 artiklan 1 kohdan d alakohta; profilointia koskeva suositus 5 artiklan 3 kohta.

593 EUT, C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014, 81 kohta.

594 Ks. myös uudistettu yleissopimus 108, 98 artiklan 1 kohdan d alakohta, jonka mukaan rekisteröity voi vastustaa henkilötietojensa käsittelyä, paitsi jos rekisterinpitäjä osoittaa käsittelylle perustellut syyt, jotka syrjäyttävät rekisteröidyn edut ja perusvapaudet.

esitettävä perustellut syyt (jotka voivat syrjäyttää rekisteröityjen vastustamisoikeuden) tapauskohtaisesti[595].

Esimerkki: Asiassa *Manni*[596] Euroopan unionin tuomioistuin totesi, että koska henkilötietojen julkaisemiseen yhtiörekisterissä oli perusteltu syy, erityisesti se, että oli suojeltava ulkopuolisten henkilöiden etuja ja turvattava oikeusvarmuus, Salvatore Mannilla ei ollut oikeutta saa henkilötietojaan poistetuksi yhtiörekisteristä. Se kuitenkin tunnusti, että on olemassa oikeus vastustaa käsittelyä, toteamalla, että ”ei voida [...] sulkea pois sitä, että saattaa olla erityisiä tilanteita, joissa kyseisen henkilön konkreettiseen tilanteeseen liittyvien huomattavan tärkeiden ja perusteltujen syiden vuoksi on poikkeuksellisesti oikeutettua, että oikeus saada yhtiörekisteriin merkittyjä häntä koskevia henkilötietoja annetaan riittävän pitkän ajan kuluttua [...] käytettäviksi vain ulkopuolisille, joilla on erityinen intressi tutustua niihin”.

Euroopan unionin tuomioistuin katsoi, että kansallisten tuomioistuinten vastuulla on arvioida kukin tapaus ja ottaa huomioon kaikki yksilön kannalta merkitykselliset olosuhteet ja se, onko olemassa sellaisia huomattavan tärkeitä ja perusteltuja syitä, joiden vuoksi voi olla poikkeuksellisesti oikeutettua rajoittaa kolmansien osapuolten oikeutta saada yhtiörekisteriin merkittyjä tietoja. Se selvensi kuitenkin, että kantaja Mannin tapauksessa pelkästään se seikka, että on väitetty, että hänen henkilötietojensa julkistaminen rekisterissä vaikutti hänen asiakaskuntaansa, ei voi riittää tällaiseksi huomattavan tärkeäksi ja perustelluksi syyksi. Salvatore Mannin mahdollisilla asiakkailla on oikeutettu intressi hänen entisen yhtiönsä konkurssia koskevien tietojen saamiseen.

Jos vastalause hyväksytään, rekisterinpitäjä ei voi enää käsitellä kyseisiä tietoja. Ennen vastalausetta rekisteröidyn osalta suoritetut käsittelytoimet ovat kuitenkin edelleen laillisia.

595 Uudistettu yleissopimus 108, selitysmuistio, 78 kohta.

596 EUT, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9.3.2017, 47 ja 60 kohta.

Oikeus vastustaa tietojen käyttöä markkinointitarkoituksiin

Yleisen tietosuoja-asetuksen 21 artiklan 2 kohdassa säädetään erityisestä oikeudesta vastustaa henkilötietojen käyttöä suoramarkkinointitarkoituksiin. Sillä selvennetään entisestään sähköisen viestinnän tietosuojadirektiivin 13 artiklaa. Tämä oikeus vahvistetaan myös uudistetussa yleissopimuksessa 108 sekä Euroopan neuvoston suoramarkkinointia koskevassa suosituksessa[597]. Uudistetun yleissopimuksen 108 selitysmuistiossa selvennetään, että suoramarkkinointitarkoituksiin tehtävän tietojenkäsittelyn kiellon perusteella kyseiset henkilötiedot on poistettava ehdottomasti[598].

Rekisteröidyllä on oikeus vastustaa henkilötietojensa käyttöä suoramarkkinointitarkoituksiin milloin tahansa maksutta. Rekisteröidyille on ilmoitettava tästä oikeudesta selkeästi ja muista tiedoista erillään.

Oikeus vastustaa henkilötietojen käsittelyä automaattisesti

Kun henkilötietoja käytetään ja käsitellään tietoyhteiskunnan palveluja varten, rekisteröity voi käyttää oikeuttaan vastustaa henkilötietojensa käsittelyä automaattisesti.

Tietoyhteiskunnan palveluilla tarkoitetaan kaikkia palveluja, toisin sanoen kaikkia etäpalveluina sähköisessä muodossa palvelun vastaanottajan henkilökohtaisesta pyynnöstä toimitettavia palveluja, joista tavallisesti maksetaan korvaus[599].

Tietoyhteiskunnan palveluja tarjoavilla rekisterinpitäjillä on oltava käytössä asianmukaiset tekniset järjestelyt ja menettelyt sen varmistamiseksi, että automaattista vastustamisoikeutta voidaan käyttää tehokkaasti[600]. Siihen voi kuulua esimerkiksi evästeiden estäminen verkkosivuilla tai seurannan ottaminen pois käytöstä verkkohaussa.

597 Euroopan neuvoston ministerikomitea (1985), suositus Rec(85)20 jäsenvaltioille suoramarkkinointiin käytettävien henkilötietojen suojasta, 25.10.1985, 4 artiklan 1 kohta.

598 Uudistettu yleissopimus 108, selitysmuistio, 79 kohta.

599 Teknisiä standardeja ja määräyksiä koskevien tietojen toimittamisessa noudatettavasta menettelystä annetun direktiivin 98/34/EY, sellaisena kuin se on muutettuna direktiivillä 98/48/EY, 1 artiklan 2 kohta.

600 Yleinen tietosuoja-asetus, 21 artiklan 5 kohta.

Oikeus vastustaa tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten tehtävää käsittelyä

EU:n oikeudessa tieteellisiä tutkimustarkoituksia olisi tulkittava laajasti niin, että ne tarkoittavat myös teknologian kehittämistä ja esittelyä, perustutkimusta, soveltavaa tutkimusta ja yksityisin varoin rahoitettua tutkimusta[601]. Historiantutkimukseen kuuluu myös sukututkimustarkoituksiin tehty tutkimus ottaen huomioon, että yleistä tietosuoja-asetusta ei sovelleta kuolleisiin henkilöihin[602]. Tilastollisilla tarkoituksilla tarkoitetaan mitä tahansa henkilötietojen keräämis- ja käsittelytoimenpidettä, joka on tarpeen tilastotutkimuksia varten tai tilastollisten tulosten tuottamiseksi[603]. Rekisteröidyn henkilökohtainen tilanne on tässäkin oikeusperusta oikeudelle vastustaa henkilötietojen käsittelyä tutkimustarkoituksiin[604]. Ainoa poikkeus on, että käsittely on tarpeen yleistä etua koskevan tehtävän suorittamiseksi. Poistamisoikeutta ei kuitenkaan sovelleta, kun käsittely on tarpeen (yleisen edun mukaisista syistä tai ilman niitä) tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten[605].

Yleisessä tietosuoja-asetuksessa luodaan tasapaino tieteellisen, tilastollisen tai historiallisen tutkimuksen vaatimusten ja rekisteröidyn oikeuksien välille 89 artiklan erityisillä suojatoimilla ja poikkeuksilla. Unionin oikeudessa tai jäsenvaltioiden lainsäädännössä voidaan näin ollen säätää poikkeuksista vastustamisoikeuteen, jos tällainen oikeus todennäköisesti estää erityisten tutkimustarkoitusten saavuttamisen tai vaikeuttaa sitä suuresti ja jos tällaiset poikkeukset ovat tarpeen näiden tarkoitusten täyttämiseksi.

Euroopan neuvoston oikeudessa, uudistetun yleissopimuksen 108 9 artiklan 2 kohdassa vahvistetaan, että laissa voidaan säätää rajoituksista rekisteröityjen oikeuksiin, myös vastustamisoikeuteen, kun tietojenkäsittely tehdään yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten, kun rekisteröityjen oikeuksien ja perusvapauksien rikkomiseen ei ole tunnistettavaa riskiä.

601 *Ibid.*, johdanto-osan 159 kappale.

602 *Ibid.*, johdanto-osan 160 kappale.

603 *Ibid.*, johdanto-osan 162 kappale.

604 *Ibid.*, 21 artiklan 6 kohta.

605 *Ibid.*, 17 artiklan 3 kohdan d alakohta.

Selitysmuistiossa (41 kohta) tunnustetaan kuitenkin myös, että rekisteröidyillä pitäisi olla oikeus antaa suostumuksensa vain tietyille tutkimusaloille tai tutkimushankkeiden osille, mikäli se on mahdollista suunnitellun tarkoituksen perusteella, ja vastustaa, jos käsittelyllä heidän mielestään kajotaan liiallisesti heidän oikeuksiinsa ja vapauksiinsa ilman perusteltua syytä.

Toisin sanoen tällainen käsittely katsottaisiin siksi etukäteen yhteensopivaksi, mikäli käytössä on muita suojatoimia ja mikäli toimilla periaatteessa suljetaan pois kaikkien sellaisten tietojen käyttö, jotka on saatu tiettyä henkilöä koskevia päätöksiä tai toimenpiteitä varten.

6.1.7 Automatisoidut yksittäispäätökset, profilointi mukaan luettuna

Automatisoidut päätökset ovat päätöksiä, jotka on tehty käsittelemällä henkilötietoja ainoastaan automaattisesti ilman ihmisen osallistumista. **EU:n oikeuden** mukaan rekisteröityjen ei tarvitse joutua sellaisten automaattisen päätösten kohteeksi, joilla on heitä koskevia oikeusvaikutuksia tai jotka vaikuttavat heihin vastaavalla tavalla merkittävästi. Jos tällaiset päätökset todennäköisesti vaikuttavat yksilöiden elämään merkittävällä tavalla, koska ne liittyvät esimerkiksi luottokelpoisuuteen, sähköiseen rekrytointiin, työsuoritukseen tai käytöksen tai luotettavuuden arviointiin, tarvitaan erityistä suojaa kielteisten seurausten välttämiseksi. Automaattinen päätöksenteko sisältää profiloinnin, jossa missä tahansa muodossa arvioidaan automaattisesti ”luonnollisen henkilön tiettyjä henkilökohtaisia ominaisuuksia, erityisesti analysoidaan tai ennakoidaan piirteitä, jotka liittyvät kyseisen luonnollisen henkilön työsuoritukseen, taloudelliseen tilanteeseen, terveyteen, henkilökohtaisiin mieltymyksiin, kiinnostuksen kohteisiin, luotettavuuteen, käyttäytymiseen, sijaintiin tai liikkeisiin”[606].

Esimerkki: Tulevan asiakkaan luottokelpoisuuden nopeaa selvittämistä varten luottotietoyritykset keräävät tiettyjä tietoja, esimerkiksi asiakkaan luotto- ja palvelu-/hyödyketilien hallintaa koskevia tietoja, asiakkaan aiempia osoitetietoja sekä tietoa julkisista lähteistä, kuten vaaliluettelosta, julkisista rekistereistä (myös oikeuden tuomioista) tai vararikko- ja maksukyvyttömyystietoja. Nämä henkilötiedot syötetään pisteytysalgoritmiin, joka laskee mahdollisen asiakkaan luottokelpoisuutta kuvastavan kokonaisarvon.

606 *Ibid.*, johdanto-osan 71 kappale, 4 artiklan 4 kohta ja 22 artikla.

Tietosuojatyöryhmän mukaan pääsääntönä on, että sellaiset täysin automatisoidut yksittäispäätökset, mukaan luettuna profilointi, ovat yleisesti kiellettyjä, kun niillä on rekisteröityä koskevia oikeusvaikutuksia tai ne vaikuttavat häneen vastaavalla tavalla merkittävästi, eikä rekisteröidyn tarvitse aktiivisesti vastustaa kyseistä päätöstä[607].

Yleisen tietosuoja-asetuksen mukaan automatisoitu päätöksenteko, jolla on oikeusvaikutuksia tai vastaavia merkittäviä vaikutuksia yksilöille, voi olla hyväksyttävissä, jos se on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten tai jos rekisteröity on antanut nimenomaisen suostumuksen. Automatisoitu päätöksenteko voidaan hyväksyä myös, jos se on hyväksytty lainsäädännössä ja jos rekisteröidyn oikeudet, vapaudet ja oikeutetut edut suojataan asianmukaisesti.[608]

Yleisessä tietosuoja-asetuksessa säädetään myös, että kun henkilötietoja kerätään rekisteröidyltä, rekisterinpitäjien toimitettavia tietoja koskeviin velvollisuuksiin kuuluu kertoa rekisteröidyille automatisoidun päätöksenteon, muun muassa profiloinnin, olemassaolosta[609]. Tämä ei vaikuta oikeuteen saada pääsy rekisterinpitäjän käsittelemiin henkilötietoihin[610]. Sen lisäksi, että tiedoissa ilmoitetaan profiloinnin suorittamisesta, niihin pitäisi sisältyä myös merkitykselliset tiedot profilointiin liittyvästä logiikasta ja mahdolliset seuraukset rekisteröidylle[611]. Esimerkiksi sairausvakuutusyhtiön, joka käyttää hakemuksissa automatisoitua päätöksentekoa, olisi annettava rekisteröidyille yleistä tietoa algoritmin toiminnasta sekä siitä, mitä tekijöitä algoritmi käyttää heidän vakuutusmaksujensa laskemiseen. Myös käyttäessään ”oikeuttaan saada pääsy tietoihin” rekisteröidyt voivat pyytää rekisterinpitäjältä tietoa automatisoidun päätöksenteon olemassaolosta ja merkityksellisiä tietoja käsittelyyn liittyvästä logiikasta[612].

Rekisteröidyille annettavien tietojen tarkoituksena on taata läpinäkyvyys ja antaa rekisteröidyille mahdollisuus tapauksen mukaan antaa tietoinen suostumus tai vaatia, että tiedot käsittelee luonnollinen henkilö. Rekisterinpitäjän on toteutettava asianmukaiset toimenpiteet rekisteröidyn oikeuksien ja vapauksien sekä

607 Tietosuojatyöryhmä, *suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi*, WP 251, 3.10.2017, s. 21.

608 Yleinen tietosuoja-asetus, 22 artiklan 2 kohta.

609 *Ibid.*, 12 artikla.

610 *Ibid.*, 15 artikla.

611 *Ibid.*, 13 artiklan 2 kohdan f alakohta.

612 *Ibid.*, 15 artiklan 1 kohdan h alakohta.

oikeutettujen etujen suojaamiseksi. Siihen sisältyy vähintään oikeus vaatia, että tiedot käsittelee rekisterinpitäjän puolesta luonnollinen henkilö, sekä rekisteröidyn mahdollisuus esittää kantansa ja riitauttaa päätös henkilötietojensa automaattisen käsittelyn perusteella.[613]

Tietosuojatyöryhmä on antanut lisäohjeita automatisoidun päätöksenteon käytöstä yleisen tietosuoja-asetuksen mukaisesti.[614]

Euroopan neuvoston oikeuden mukaan yksilöillä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka vaikuttaa heihin huomattavasti ja joka perustuu ainoastaan automaattiseen käsittelyyn, jossa ei ole otettu huomioon heidän näkemyksiään[615]. Vaatimus rekisteröidyn näkemysten huomioon ottamisesta, kun päätökset perustuvat ainoastaan automaattiseen käsittelyyn, tarkoittaa, että rekisteröidyllä on oikeus riitauttaa kyseiset päätökset ja että hänen pitäisi voida kiistää kaikki virheellisyydet rekisterinpitäjän käyttämissä henkilötiedoissa ja kyseenalaistaa häneen sovelletun profiilin merkityksellisyys[616]. Henkilö ei kuitenkaan voi käyttää tätä oikeutta, jos automatisoitu päätöksenteko sallitaan rekisterinpitäjään sovellettavassa lainsäädännössä, jossa myös säädetään asianmukaisista toimenpiteistä rekisteröityjen oikeuksien, vapauksien ja oikeutettujen etujen suojaamiseksi. Rekisteröidyillä on myös oikeus saada pyynnöstä tietoja suoritetun tietojenkäsittelyn perustasta.[617] Uudistetun yleissopimuksen 108 selitysmuistiossa annetaan esimerkki luottopisteytyksestä. Sen lisäksi, että henkilöillä on oikeus saada tietää, onko pisteytyspäätös myönteinen vai kielteinen, heidän pitäisi voida saada tietoonsa myös kyseiseen päätökseen johtaneen henkilötietojen käsittelyn taustalla oleva *logiikka*. Näiden tekijöiden ymmärtäminen edistää muiden keskeisten suojatoimien, kuten vastustamisoikeuden ja toimivaltaiselle viranomaiselle valittamista koskevan oikeuden, tehokasta käyttöä[618].

Vaikka profilointia koskeva suositus ei ole oikeudellisesti sitova, siinä yksilöidään henkilötietojen keräämistä ja käsittelyä profiloinnin yhteydessä koskevat ehdot[619].

613 *Ibid.*, 22 artiklan 3 kohta.

614 Tietosuojatyöryhmä, *suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi*, WP 251, 3.10.2017.

615 Uudistettu yleissopimus 108, 9 artiklan 1 kohdan a alakohta.

616 Uudistettu yleissopimus 108, selitysmuistio, 75 kohta.

617 Uudistettu yleissopimus 108, 9 artiklan 1 kohdan c alakohta.

618 Uudistettu yleissopimus 108, selitysmuistio, 77 kohta.

619 Euroopan neuvosto, ministerikomitea (2010), suositus Rec(2010)13 jäsenvaltioille yksilöiden suojelusta profiloinnin yhteydessä tapahtuvassa automaattisessa henkilötietojen käsittelyssä, 5 artiklan 5 kohta.

Sen säännösten mukaan on varmistettava, että profiloinnin yhteydessä tehtävä käsittely on kohtuullista, oikeasuhteista ja määriteltyä ja lainmukaista tarkoitusta varten. Siihen kuuluu myös säännöksiä tiedoista, joita rekisterinpitäjien on annettava rekisteröidyille. Suosituksessa esitetään myös tietojen laatua koskeva periaate, jonka mukaan rekisterinpitäjien on ryhdyttävä toimenpiteisiin tietojen virheellisyyttä koskevien tekijöiden oikaisemiseksi ja profilointiin mahdollisesti liittyvien riskien tai virheiden rajoittamiseksi sekä arvioitava säännöllisesti tietojen ja käytettyjen algoritmien laatua.

6.2 Oikeussuojakeinot, vastuu, seuraamukset ja korvaukset

Keskeiset kohdat

- Uudistetun yleissopimuksen 108 mukaan sopimuspuolten kansallisessa lainsäädännössä on säädettävä asianmukaisista oikeussuojakeinoista ja seuraamuksista tietosuojaa koskevan oikeuden rikkomusten varalta.
- EU:ssa yleisessä tietosuoja-asetuksessa säädetään rekisteröityjen oikeussuojakeinoista, jos heidän oikeuksiaan loukataan, sekä seuraamuksista rekisterinpitäjille ja henkilötietojen käsittelijöille, jotka eivät noudata asetuksen säännöksiä. Siinä säädetään myös oikeudesta korvauksiin ja vastuuseen.
    - Rekisteröidyillä on oikeus tehdä valitus valvontaviranomaiselle asetuksen väitetystä rikkomisesta sekä oikeus tehokkaisiin oikeussuojakeinoihin ja oikeus saada korvausta.
    - Kun yksityishenkilöt käyttävät oikeuttaan tehokkaisiin oikeussuojakeinoihin, heitä voivat edustaa tietosuojan alalla toimivat voittoa tavoittelemattomat järjestöt.
    - Rekisterinpitäjä tai henkilötietojen käsittelijä on vastuussa kaikesta rikkomisesta johtuvasta aineellisesta tai aiheettomasta vahingosta.
    - Valvontaviranomaiset voivat määrätä asetuksen rikkomisesta hallinnollisen sakon, joka on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.
- Rekisteröidyt voivat viimeisenä keinona ja tietyin edellytyksin saattaa henkilötietojen suojaa koskevat rikkomukset myös Euroopan ihmisoikeustuomioistuimen käsiteltäväksi.

- Kaikilla luonnollisilla henkilöillä ja oikeushenkilöillä on oikeus tehdä valitus mistä tahansa Euroopan tietosuojaneuvoston tekemästä päätöksestä Euroopan unionin tuomioistuimelle perussopimuksissa säädetyin ehdoin.

Säädösten antaminen ei riitä varmistamaan henkilötietojen suojaa Euroopassa. Euroopan tietosuojasääntöjen tehokkuuden varmistamiseksi on luotava mekanismeja, joiden avulla yksityishenkilöt voivat torjua oikeuksiensa loukkauksia ja hakea korvausta kärsitystä vahingosta. Tärkeää on myös, että valvontaviranomaisilla on valtuudet määrätä tehokkaita, varoittavia ja oikeasuhteisia seuraamuksia kyseessä olevasta rikkomuksesta.

Tietosuojalainsäädännön mukaisia oikeuksia voi käyttää henkilö, jonka oikeudet ovat kyseessä, eli henkilö, joka on rekisteröity. Muut henkilöt – jotka täyttävät kansallisen lainsäädännön mukaiset tarvittavat vaatimukset – voivat kuitenkin myös edustaa rekisteröityjä näiden oikeuksien käytössä. Useiden kansallisten lainsäädäntöjen mukaan lasten ja kehitysvammaisten edustajan on oltava heidän holhoojansa[620]. EU:n tietosuojalainsäädännön mukaan yhdistys – jonka lainmukaisena tavoitteena on tietosuojaoikeuksien edistäminen – voi edustaa rekisteröityjä valvontaviranomaisessa tai tuomioistuimessa[621].

6.2.1 Oikeus tehdä valitus valvontaviranomaiselle

Sekä **Euroopan neuvoston** että **EU:n oikeuden** mukaan yksilöillä on oikeus tehdä pyyntöjä ja valituksia toimivaltaiselle valvontaviranomaiselle, jos he katsovat, että heidän henkilötietojaan käsitellään lainvastaisesti.

Uudistetussa yleissopimuksessa 108 tunnustetaan rekisteröityjen oikeus saada valvontaviranomaiselta apua, kun he käyttävät yleissopimuksen mukaisia oikeuksiaan, kansalaisuudesta tai asuinpaikasta riippumatta[622]. Avunpyyntö voidaan torjua vain poikkeuksellisissa olosuhteissa, eikä rekisteröidyille pitäisi koitua kustannuksia tai maksuja avusta[623].

620 FRA (2015), Käsikirja Euroopan lapsen oikeuksia koskevasta oikeudesta, Luxemburg, EU:n julkaisutoimisto; FRA (2013), Kehitysvammaisten ja mielenterveysongelmaisten henkilöiden oikeuskelpoisuus, Luxemburg, EU:n julkaisutoimisto.

621 Yleinen tietosuoja-asetus, 80 artikla.

622 Uudistettu yleissopimus 108, 18 artikla.

623 *Ibid.*, 16–17 artikla.

EU:n oikeusjärjestelmässä on samanlaisia säännöksiä. Yleisen tietosuoja-asetuksen mukaan valvontaviranomaisten on helpotettava valitusten jättämistä toimenpitein, kuten luomalla sähköinen valituslomake[624]. Rekisteröity voi tehdä valituksen valvontaviranomaiselle jäsenvaltiossa, jossa hänen vakinainen asuinpaikkansa tai työpaikkansa on taikka jossa väitetty rikkominen on tapahtunut[625]. Valitukset on tutkittava, ja valvontaviranomaisen on ilmoitettava kyseessä olevalle henkilölle valituksen etenemisestä ja ratkaisusta[626].

EU:n toimielinten tai elinten mahdolliset rikkomukset voidaan esittää Euroopan tietosuojavaltuutetulle[627]. Jos tietosuojavaltuutettu ei vastaa kuuden kuukauden kuluessa, valitus katsotaan hylätyksi. Euroopan tietosuojavaltuutetun päätöksiä koskevat muutoksenhaut voidaan saattaa Euroopan unionin tuomioistuimen käsiteltäväksi asetuksen (EY) N:o 45/2001 nojalla. Siinä säädetään EU:n toimielinten ja elinten velvollisuudesta noudattaa tietosuojasääntöjä.

Kansallisen valvontaviranomaisen päätöksiin on voitava hakea muutosta tuomioistuimista. Tämä koskee rekisteröityjä sekä rekisterinpitäjiä ja henkilötietojen käsittelijöitä, jotka ovat olleet osapuolina valvontaviranomaisen menettelyssä.

Esimerkki: Espanjan tietosuojaviranomainen antoi syyskuussa 2017 sakot Facebookille useiden tietosuojamääräysten rikkomisesta. Valvontaviranomainen tuomitsi verkkoyhteisön henkilötietojen, myös erityisten henkilötietoryhmien, keräämisestä, tallentamisesta ja käsittelemisestä mainontatarkoituksiin ja ilman rekisteröidyn suostumusta. Päätös perustui valvontaviranomaisen omasta aloitteesta tehtyyn tutkimukseen.

6.2.2 Oikeus tehokkaisiin oikeussuojakeinoihin

Sen lisäksi, että yksityishenkilöillä on oikeus tehdä valitus valvontaviranomaiselle, heillä on oltava myös oikeus tehokkaisiin oikeussuojakeinoihin ja oikeus saattaa asiansa tuomioistuimen käsiteltäväksi. Oikeus oikeussuojakeinoihin on vakiintunut Euroopan oikeusperinteeseen. Se tunnustetaan perusoikeudeksi

624 Yleinen tietosuoja-asetus, 57 artiklan 2 kohta.

625 *Ibid.*, 77 artiklan 1 kohta.

626 *Ibid.*, 77 artiklan 2 kohta.

627 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001, L 8.

sekä EU:n perusoikeuskirjan 47 artiklassa että Euroopan ihmisoikeussopimuksen 13 artiklassa.[628]

EU:n oikeudessa rekisteröityjen käytettävissä olevien tehokkaiden oikeussuojakeinojen merkitys heidän oikeuksiaan rikottaessa käy selkeästi ilmi sekä yleisen tietosuoja-asetuksen säännöksistä – joissa vahvistetaan oikeus tehokkaisiin oikeussuojakeinoihin valvontaviranomaisia, rekisterinpitäjiä ja henkilötietojen käsittelijöitä vastaan – että Euroopan unionin tuomioistuimen oikeuskäytännöstä.

Esimerkki: Asiassa *Schrems*[629] Euroopan unionin tuomioistuin totesi tietosuojan tason riittävyyttä koskevan safe harbor -päätöksen olevan pätemätön. Päätöksellä sallitaan kansainväliset tietosiirrot EU:sta Yhdysvalloissa sijaitseville organisaatioille, jotka ilmoittavat noudattavansa safe harbor -järjestelmää. Euroopan unionin tuomioistuin katsoi, että safe harbor -järjestelmässä oli useita puutteita, jotka vaaransivat EU:n kansalaisten perusoikeudet yksityisyyden suojaan ja henkilötietojen suojaan sekä oikeuden tehokkaisiin oikeussuojakeinoihin.

Yksityiselämän suojaa ja tietosuojaa koskevan oikeuden rikkomisesta Euroopan unionin tuomioistuin toi esiin, että tietyt viranomaiset pystyivät Yhdysvaltojen lainsäädännön nojalla saamaan jäsenvaltioista Yhdysvaltoihin siirrettyjä henkilötietoja ja käsittelemään niitä siirron alkuperäisten tarkoitusten vastaisella tavalla ja laajemmin kuin on ehdottomasti tarpeen ja oikeasuhteista kansallisen turvallisuuden suojelemisen kannalta. Oikeudesta tehokkaisiin oikeussuojakeinoihin se pani merkille, ettei rekisteröidyillä ollut mahdollisuutta hakea hallinto- tai oikeusteitse oikeussuojaa, jonka avulla he muun muassa voisivat saada tutustua itseään koskeviin tietoihin ja saada ne tarvittaessa oikaistuiksi tai poistetuiksi. Euroopan unionin tuomioistuin totesi, että säännöstö, jossa ei anneta mitään mahdollisuutta käyttää oikeussuojakeinoja henkilötietoihin tutustumista tai niiden oikaisemista tai poistamista varten, ”ei ole tehokasta oikeussuojaa koskevan perusoikeuden, sellaisena kuin se vahvistetaan perusoikeuskirjan 47 artiklassa, keskeisen sisällön mukainen”. Se korosti, että oikeuden määräysten ja säännösten noudattamisen varmistamiseen tarkoitetun tehokkaan tuomioistuinvalvonnan itse olemassaolo kuuluu erottamattomana osana oikeusvaltioon.

628 Ks. esim. EIT, *Karabeyoğlu v. Turkki*, nro 30083/10, 7.6.2016; EIT, *Mustafa Sezgin Tanrıkulu v. Turkki*, nro 27473/06, 18.7.2017.

629 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

Yksityishenkilöt, rekisterinpitäjät tai henkilötietojen käsittelijät, jotka haluavat riitauttaa valvontaviranomaisen oikeudellisesti sitovan päätöksen, voivat nostaa kanteen tuomioistuimessa[630]. Päätöksen käsitettä olisi tulkittava laajasti siten, että se koskee valvontaviranomaisen tutkintavaltuuksien, seuraamusten määräämistä koskevien valtuuksien ja hyväksymisvaltuuksien käyttöä sekä valitusten käsittelemättä jättämistä tai hylkäämistä koskevia päätöksiä. Tuomioistuimessa esitettävän kanteen kohteena eivät voi kuitenkaan olla toimenpiteet, jotka eivät ole oikeudellisesti sitovia, kuten valvontaviranomaisen antamat lausunnot tai neuvot[631]. Kanne valvontaviranomaista vastaan on nostettava sen jäsenvaltion tuomioistuimissa, johon valvontaviranomainen on sijoittautunut[632].

Jos rekisterinpitäjä tai henkilötietojen käsittelijä rikkoo rekisteröidyn oikeuksia, rekisteröidyllä on oikeus tehdä valitus tuomioistuimelle[633]. Rekisterinpitäjää tai henkilötietojen käsittelijää vastaan nostettavissa kanteissa on erityisen tärkeää, että rekisteröidyt voivat valita, missä kanne nostetaan. Kanne voidaan ostaa sen jäsenvaltion tuomioistuimissa, jossa rekisterinpitäjällä tai henkilötietojen käsittelijällä on toimipaikka, tai sen jäsenvaltion tuomioistuimissa, jossa rekisteröidyn vakinainen asuinpaikka on.[634] Toinen mahdollisuus helpottaa huomattavasti rekisteröityjen oikeuksien käyttöä, koska he voivat nostaa kanteen asuinvaltiossaan, jonka oikeudenkäyttö on heille tuttua. Jos kanteen nostaminen rekisterinpitäjiä ja henkilötietojen käsittelijöitä vastaan rajoitettaisiin jäsenvaltioon, jossa niillä on toimipaikka, se voisi estää toisissa jäsenvaltioissa oleskelevia rekisteröityjä nostamasta kannetta, koska siihen kuuluisi matkustamista ja lisäkustannuksia, ja oikeudenkäynti voisi olla vieraalla kielellä ja oikeudenkäyttöalueella. Ainoa poikkeus koskee tapauksia, joissa rekisterinpitäjä tai henkilötietojen käsittelijä on jäsenvaltion viranomainen ja käsittely liittyy sen julkisen vallan käyttöön. Siinä tapauksessa kanne voidaan nostaa vain kyseisen viranomaisen valtion tuomioistuimissa.[635]

Vaikka useimmissa tapauksissa tietosuojasääntöjä koskevat päätökset tehdään jäsenvaltioiden tuomioistuimissa, jotkin tapaukset voidaan saattaa Euroopan unionin tuomioistuimen käsiteltäväksi. Ensimmäinen mahdollisuus koskee tapausta, jossa rekisteröity, rekisterinpitäjä, henkilötietojen käsittelijä tai valvontaviranomainen

630 Yleinen tietosuoja-asetus, 78 artikla.

631 *Ibid.*, johdanto-osan 143 kappale.

632 *Ibid.*, 78 artiklan 3 kohta.

633 *Ibid.*, 79 artikla.

634 *Ibid.*, 79 artiklan 2 kohta.

635 *Ibid.*

nostaa kumoamiskanteen Euroopan tietosuojaneuvoston päätöstä vastaan. Tähän kanteeseen sovelletaan kuitenkin SEUT-sopimuksen 263 artiklan ehtoja, joiden mukaan kanteen käsiteltäväksi ottaminen edellyttää, että yksityishenkilöt ja yhteisöt osoittavat, että päätös koskee heitä tai niitä suoraan ja erikseen.

Toinen mahdollinen tilanne koskee tapauksia, joissa EU:n toimielimet tai elimet käsittelevät henkilötietoja lainvastaisesti. Tapauksissa, joissa EU:n toimielimet rikkovat tietosuojalainsäädäntöä, rekisteröidyt voivat esittää kanteen suoraan unionin yleiselle tuomioistuimelle (yleinen tuomioistuin on osa Euroopan unionin tuomioistuinta). Yleinen tuomioistuin vastaa ensimmäisessä oikeusasteessa EU:n toimielinten tekemien EU:n lainsäädännön rikkomista koskevien kanteiden käsittelystä. Näin ollen myös kantelut Euroopan tietosuojavaltuutettua – joka on EU:n toimielin – vastaan voidaan esittää yleiselle tuomioistuimelle.[636]

Esimerkki: Asiassa *Bavarian Lager*[637] yhtiö oli pyytänyt Euroopan komissiolta täydellisen pöytäkirjan komission pitämästä kokouksesta, jonka se väitti liittyneen yritystä koskeneisiin oikeudellisiin kysymyksiin. Komissio oli hylännyt pyynnön yksityiselämän- ja henkilötietojen suojaan liittyvien ensisijaisten etujen perusteella[638]. Bavarian Lager valitti tästä päätöksestä EU:n toimielinten tietosuoja-asetuksen 32 artiklan nojalla ensimmäisen oikeusasteen tuomioistuimeen (joka oli unionin yleisen tuomioistuimen edeltäjä). Päätöksessään (asia T194/04, *The Bavarian Lager Co. Ltd vastaan Euroopan yhteisöjen komissio*) ensimmäisen oikeusasteen tuomioistuin kumosi päätöksen, jolla komissio hylkäsi asiakirjapyynnön. Euroopan komissio valitti päätöksestä unionin tuomioistuimeen.

Unionin tuomioistuin (suuri jaosto) kumosi ensimmäisen oikeusasteen tuomioistuimen tuomion ja vahvisti Euroopan komission kokouksen täydellisen pöytäkirjan saamista koskevan pyynnön hylkäyksen kokoukseen osallistuneiden henkilöiden henkilötietojen suojaamiseksi. Euroopan unionin tuomioistuin katsoi, että komissio oli oikeassa kieltäytyessään luovuttamasta kyseisiä tietoja, koska osallistujat eivät olleet antaneet suostumustaan henkilötietojensa luovuttamiseen. Bavarian Lager ei myöskään ollut osoittanut, että tietojen saaminen oli tarpeen.

636 Asetus (EY) N:o 45/2001, 32 artiklan 3 kohta.

637 EUT, C-28/08 P, *Euroopan komissio vastaan The Bavarian Lager Co. Ltd* [suuri jaosto], 2010.

638 Ks. perustelujen analyysi asiakirjassa EDPS (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bryssel, EDPS.

Rekisteröidyt, valvontaviranomaiset, rekisterinpitäjät tai henkilötietojen käsittelijät voivat lisäksi kansallisten menettelyjen yhteydessä esittää, että kansallinen tuomioistuin pyytää unionin tuomioistuinta selventämään EU:n perussopimusten tulkintaa sekä ottamaan kantaa EU:n toimielinten, elinten, laitosten tai virastojen toimien pätevyyteen. Tällaisia selvennyksiä kutsutaan ennakkoratkaisuiksi. Kyseessä ei ole valituksen tekijän näkökulmasta välitön oikeuskeino, mutta näin kansalliset tuomioistuimet voivat varmistaa, että ne tulkitsevat oikein EU:n lainsäädäntöä. Ennakkoratkaisujärjestelmän avulla Euroopan unionin tuomioistuimen käsiteltäväksi on saatettu merkittäviä asioita, jotka ovat vaikuttaneet huomattavasti EU:n tietosuojalainsäädännön kehittymiseen. Tällaisia asioita ovat muun muassa *Digital Rights Ireland* ja *Kärntner Landesregierung ym.*[639] ja *Schrems*[640].

Esimerkki: Asiassa *Digital Rights Ireland* ja *Kärntner Landesregierung ym.*[641] oli kyse yhteisestä asiasta, jossa Irish High Court ja Itävallan perustuslakituomioistuin esittivät ennakkoratkaisupyynnön direktiivin 2006/24/EY (tietojen säilyttämistä koskeva direktiivi) EU:n tietosuojalainsäädännön mukaisuudesta. Itävallan perustuslakituomioistuin kysyi Euroopan unionin tuomioistuimelta, oliko direktiivin 2006/24/EY 3–9 artiklaa pidettävä pätevinä perusoikeuskirjan 7, 9 ja 11 artiklan valossa. Se kysyi muun muassa, olivatko tietyt Itävallan liittovaltion televiestintälain säännökset, joilla tietojen säilyttämistä koskeva direktiivi oli saatettu osaksi kansallista lainsäädäntöä, yhdenmukaisia tiettyjen tietosuojadirektiivin ja EU:n toimielinten tietosuoja-asetuksen näkökohtien kanssa.

Asiassa *Kärntner Landesregierung ym.* yksi perustuslakituomioistuimen menettelyn kantajista, Seitlinger, totesi, että hän käyttää puhelinta, internetiä ja sähköpostia sekä työssään että yksityiselämässään. Tiedot, joita hän lähettää ja vastaanottaa, kulkevat julkisten televiestintäverkkojen kautta. Itävallan vuoden 2003 televiestintälain nojalla hänen televiestintäpalvelujen tarjoajallaan on lakisääteinen velvollisuus kerätä ja säilyttää tietoja hänen verkon käytöstään. Seitlinger katsoi, ettei tällainen hänen henkilötietojensa keruu ja säilytys ollut mitenkään välttämätöntä siihen tekniseen

639 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

640 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

641 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

tarkoitukseen, joka oli lähettäminen ja vastaanottaminen. Henkilötietojen keruu ja säilytys ei ollut mitenkään tarpeellista edes laskutustarkoituksiin. Seitlinger ei totisesti ollut antanut suostumustaan tällaiseen henkilötietojensa käyttöön. Ainoa syy kaikkien ylimääräisten tietojen keruulle ja säilytykselle oli Itävallan vuoden 2003 televiestintälaki.

Seitlinger nosti näin ollen Itävallan perustuslakituomioistuimessa kanteen, jossa hän väitti, että televiestintäpalvelujen tarjoajan lakisääteiset velvollisuudet rikkoivat hänen EU:n perusoikeuskirjan 8 artiklan mukaisia perusoikeuksiaan. Koska kyseisellä Itävallan lailla saatettiin EU:n lainsäädäntöä (silloinen tietojen säilyttämistä koskeva direktiivi) osaksi kansallista lainsäädäntöä, Itävallan perustuslakituomioistuin pyysi Euroopan unionin tuomioistuinta päättämään, onko direktiivi EU:n perusoikeuskirjassa vahvistettujen yksityisyyden suojaa ja tietosuojaa koskevien oikeuksien mukainen.

Euroopan unionin tuomioistuin (suuri jaosto) teki asiassa päätöksen, jolla kumottiin EU:n tietojen säilyttämistä koskeva direktiivi. Tuomioistuin katsoi, että direktiivi sisältää erityisen vakavan puuttumisen yksityisyyden suojaa ja tietosuojaa koskeviin perusoikeuksiin ilman, että tällainen puuttuminen rajoitetaan täysin välttämättömään. Direktiivillä oli hyväksyttävä tavoite, koska se antoi kansallisille viranomaisille lisämahdollisuuksia selvittää vakavia rikoksia ja tehdä niiden syyteharkintaa. Tältä osin se siis oli hyödyllinen väline rikostutkinnassa. Euroopan unionin tuomioistuin kuitenkin totesi, että perusoikeuksia pitäisi rajoittaa vain, kun se on ehdottoman välttämätöntä, ja niiden tukena olisi oltava selvät ja täsmälliset rajoittamisen laajuutta ja soveltamista koskevat säännöt sekä riittävät takeet yksityishenkilöille.

Tuomioistuimen mukaan direktiivi ei läpäissyt tätä välttämättömyystestiä. Siinä ei ensinnäkään säädetty selvistä ja täsmällisistä säännöistä, joilla säädellään puuttumisen laajuutta. Sen sijaan, että direktiivissä vaadittaisiin yhteyttä säilytettävien tietojen ja vakavan rikollisuuden välillä, direktiiviä sovellettiin kaikkien sähköisten viestintämuotojen kaikkien käyttäjien kaikkiin metatietoihin. Näin ollen se merkitsi puuttumista käytännöllisesti katsoen koko EU:n väestön yksityisyyden suojaa ja tietosuojaa koskeviin oikeuksiin, mikä voidaan katsoa suhteettomaksi. Direktiivissä ei säädetty perusteesta, jolla voitaisiin rajoittaa niiden henkilöiden määrää, joilla on oikeus saada tietoja, eikä tietojen saamiseen sovellettu menettelyllisiä edellytyksiä, kuten vaatimusta saada hallinnollisen yksikön tai tuomioistuimen lupa ennen tietojen saamista. Direktiivissä ei myöskään säädetty selvistä

takeista säilytettävien tietojen suojaamiseksi. Siinä ei näin ollen varmistettu tietojen tehokasta suojaa väärinkäytön vaaraa vastaan eikä näiden tietojen kaikenlaista laitonta saantia ja käyttöä vastaan.[642]

Euroopan unionin tuomioistuimen on periaatteessa vastattava sille esitettyihin kysymyksiin. Se ei voi kieltäytyä antamasta ennakkoratkaisua sillä perusteella, että sen vastaus ei olisi merkityksellinen eikä oikea-aikainen pääasian kannalta. Se voi kuitenkin jättää vastaamatta, jos kysymys ei kuulu sen toimivaltaan[643]. Euroopan unionin tuomioistuin antaa päätöksen vain ennakkoratkaisupyynnön pääasiasta, ja kansallinen tuomioistuin on toimivaltainen tekemään päätöksen alkuperäisestä asiasta[644].

EU:n oikeuden mukaan sopimuspuolten on otettava käyttöön asianmukaiset oikeudelliset ja muut kuin oikeudelliset suojakeinot uudistetun yleissopimuksen 108 säännösten rikkomista vastaan[645]. Tietosuojaoikeuksien rikkomukset, joiden väitetään olevan paitsi ihmisoikeussopimuksen sopimuspuolen kansallisen lainsäädännön vastaisia myös ihmisoikeussopimuksen 8 artiklan vastaisia, voidaan lisäksi saattaa Euroopan ihmisoikeustuomioistuimen käsiteltäviksi sen jälkeen, kun kaikki kansalliset oikeuskeinot on käytetty. Jotta ihmisoikeustuomioistuin voisi ratkaista ihmisoikeussopimuksen 8 artiklan rikkomisen, on muidenkin tutkittavaksi ottamisen edellytysten täytyttävä (ihmisoikeussopimuksen 34–37 artikla)[646].

Kanteen voi ihmisoikeustuomioistuimessa nostaa vain sopimuspuolta vastaan, mutta asioissa voidaan välillisesti käsitellä myös yksityisten osapuolten toimia tai laiminlyöntejä, siinä määrin kuin sopimuspuoli on jättänyt noudattamatta positiivisia velvoitteitaan eikä ole vahvistanut kansallisessa lainsäädännössä riittävää turvaa tietosuojaoikeuksien rikkomisia vastaan.

642 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014, 69 kohta.

643 EUT, C-244/80, *Pasquale Foglia vastaan Mariella Novello (nro 2)*, 16.12.1981; EUT, C-467/04, *Rikosoikeudenkäynti vastaan Gasparini ym.*, 28.9.2006.

644 EUT, C-438/05, *International Transport Workers' Federation ja Finnish Seamen's Union vastaan Viking Line ABP ja OÜ Viking Line Eesti* [suuri jaosto], 11.12.2007, 85 kohta.

645 Uudistettu yleissopimus 108, 12 artikla.

646 EIT, 34–37 artikla.

Esimerkki: Asiassa *K.U. v. Suomi*[647] kantajana ollut alaikäinen henkilö valitti, että hänestä oli julkaistu internetin seuranhakupalstalla seksuaalisluonteinen ilmoitus. Palveluntarjoaja kieltäytyi paljastamasta tiedon julkaisseen henkilön henkilöllisyyttä vedoten Suomen lain mukaiseen salassapitovelvollisuuteen. Kantaja väitti, että Suomen laki ei tarjonnut riittävää suojaa tilanteessa, jossa yksityishenkilö julkaisi laittomasti tietoja internetissä. Euroopan ihmisoikeustuomioistuin katsoi, että valtioilla on paitsi velvollisuus olla puuttumatta mielivaltaisesti ihmisten yksityiselämään myös positiivisia velvoitteita, joihin kuuluu yksityiselämää suojaavien toimenpiteiden toteuttaminen myös yksilöiden välisten suhteiden alalla. Kantajan tapauksessa hänen tosiasiallinen ja tehokas suojaamisensa edellytti toimia rikoksentekijän tunnistamiseksi ja asettamiseksi syytteeseen. Valtio ei kuitenkaan ollut tarjonnut tällaista suojaa, ja siksi tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Köpke v. Saksa*[648] kantajaa oli epäilty varkaudesta hänen työpaikallaan ja siksi hänet oli asetettu salaa videovalvontaan. Euroopan ihmisoikeustuomioistuin katsoi, ettei mikään viitannut siihen, että kansalliset viranomaiset eivät olisi harkintavaltansa puitteissa pyrkineet saattamaan kantajan 8 artiklan mukaista oikeutta nauttia yksityiselämän kunnioitusta tasapainoon työnantajan omistusoikeuden suojaamiseen liittyvien etujen ja asianmukaista oikeudenkäyttöä koskevan yleisen edun kanssa. Kanne jätettiin näin ollen tutkimatta.

Jos Euroopan ihmisoikeustuomioistuin toteaa, että sopimuspuoli on rikkonut jotain ihmisoikeussopimuksella suojattua oikeutta, sopimusvaltion on pantava täytäntöön tuomioistuimen tuomio (ihmisoikeussopimuksen 46 artikla). Täytäntöönpanotoimenpiteiden ensisijaisena vaikutuksena on oltava kyseessä olevan rikkomuksen lopettaminen ja sen jälkeen mahdollisuuksien mukaan kantajalle aiheutuneiden haitallisten seurauksien korjaaminen. Tuomioiden täytäntöönpano saattaa edellyttää myös yleisiä toimenpiteitä, joilla ehkäistään tuomioistuimen toteamien rikkomusten toistumista lainsäädännön muutosten, oikeuskäytännön tai muiden toimenpiteiden kautta.

647 EIT, *K.U. v. Suomi*, nro 2872/02, 2.12.2008.

648 EIT, *Köpke v. Saksa* (päätös), nro 420/07, 5.10.2010.

Kun ihmisoikeustuomioistuin toteaa, että ihmisoikeussopimusta on rikottu, se voi ihmisoikeussopimuksen 41 artiklan nojalla määrätä sopimusvaltion maksamaan kantajalle hyvityksen.

Oikeus valtuuttaa voittoa tavoittelematon elin, järjestö tai yhdistys

Kun yksityishenkilöt tekevät valituksen valvontaviranomaiselle tai nostavat kanteen oikeudessa, heillä on yleisen tietosuoja-asetuksen mukaan oikeus valtuuttaa voittoa tavoittelematon elin, järjestö tai yhdistys edustamaan itseään[649]. Näiden voittoa tavoittelemattomien yhteisöjen sääntömääräisten tavoitteiden on oltava yleisen edun mukaisia, ja niiden on toimittava tietosuojan alalla. Ne voivat tehdä rekisteröityjen puolesta valituksen tai käyttää heidän puolestaan oikeutta oikeussuojakeinoihin. Asetuksessa annetaan jäsenvaltioille mahdollisuus säätää – kansallisen lainsäädännön mukaisesti – siitä, voiko elin tehdä valituksia rekisteröityjen puolesta ilman kyseisten rekisteröityjen valtuutusta.

Yksityishenkilöt pystyvät tämän edustamisoikeuden ansiosta hyötymään kyseisten voittoa tavoittelemattomien yhteisöjen asiantuntemuksesta sekä organisatorisista ja taloudellisista valmiuksista, mikä helpottaa huomattavasti heidän oikeuksien käyttöään. Yleisen tietosuoja-asetuksen mukaan nämä yhteisöt voivat esittää ryhmäkanteita useiden rekisteröityjen puolesta. Se on hyödyksi myös oikeusjärjestelmän toiminnalle ja tehokkuudelle, koska samanlaiset kanteet voidaan koota tutkittavaksi yhdessä.

6.2.3 Vastuu ja oikeus korvauksen saamiseen

Yksityishenkilöiden täytyy tehokkaita oikeussuojakeinoja koskevan oikeuden nojalla pystyä vaatimaan korvausta kaikista vahingoista, joita heille aiheutuu heidän henkilötietojensa käsittelystä, jossa on rikottu sovellettavaa lainsäädäntöä. Yleisessä tietosuoja-asetuksessa tunnustetaan yksiselitteisesti rekisterinpitäjien ja henkilötietojen käsittelijöiden vastuu lainvastaisesta käsittelystä[650]. Asetuksessa annetaan yksilöille oikeus saada rekisterinpitäjältä tai henkilötietojen käsittelijältä korvausta sekä aineellisista että aineettomista vahingoista, ja sen johdanto-osassa säädetään, että ”[v]ahingon käsite olisi tulkittava laajasti unionin tuomioistuimen oikeuskäytännön perusteella ja tavalla, jossa tämän asetuksen tavoitteet otetaan kaikilta

649 Yleinen tietosuoja-asetus, 80 artikla.

650 *Ibid.*, 82 artikla.

osin huomioon"[651]. Rekisterinpitäjät ovat vastuussa, ja niiltä voidaan vaatia vahingonkorvausta, jos ne eivät täytä asetuksen mukaisia velvollisuuksiaan. Henkilötietojen käsittelijät ovat vastuussa käsittelystä aiheutuneesta vahingosta vain, jos ne eivät ole noudattaneet nimenomaisesti henkilötietojen käsittelijöille osoitettuja tämän asetuksen velvoitteita tai jos ne ovat toimineet rekisterinpitäjän lainmukaisen ohjeistuksen ulkopuolella tai sen vastaisesti. Jos rekisterinpitäjä tai henkilötietojen käsittelijä on maksanut täyden korvauksen aiheutuneesta vahingosta, rekisterinpitäjällä tai henkilötietojen käsittelijällä on yleisen tietosuoja-asetuksen mukaan oikeus periä muilta samaan tietojenkäsittelyyn osallistuneilta rekisterinpitäjiltä tai henkilötietojen käsittelijöiltä se osuus korvauksesta, joka vastaa vastuuta aiheutuneesta vahingosta.[652] Vastuuta koskevat poikkeukset ovat puolestaan erittäin tiukkoja, ja ne edellyttävät todistetta siitä, että rekisterinpitäjä tai henkilötietojen käsittelijä ei ole millään tavalla vastuussa vahingon aiheuttaneesta tapahtumasta.

Korvauksen on oltava "täysi ja tosiasiallinen" aiheutuneeseen vahinkoon nähden. Jos vahinko johtuu useiden rekisterinpitäjien ja henkilötietojen käsittelijöiden suorittamasta käsittelystä, ne kaikki on katsottava vastuuvelvollisiksi koko vahingosta. Tämän säännön tarkoituksena on varmistaa, että rekisteröity saa tosiasiallisen korvauksen ja että käsittelytoimissa mukana olevilla rekisterinpitäjillä ja henkilötietojen käsittelijöillä on yhdenmukainen lähestymistapa sääntöjen noudattamiseen.

Esimerkki: Rekisteröityjen ei tarvitse esittää kannetta ja vaatia korvausta kaikilta vahingosta vastuussa olevilta yhteisöiltä, koska se voisi johtaa pitkiin ja kalliisiin oikeudenkäynteihin. Kanteen voi esittää pelkästään yhdestä yhteisrekisterinpitäjistä, ja tämän katsotaan olevan vastuussa koko vahingosta. Tällaisissa tapauksissa korvauksen maksavalla rekisterinpitäjällä tai henkilötietojen käsittelijällä on oikeus periä muilta samaan tietojenkäsittelyyn osallistuneilta ja rikkomuksesta vastuussa olevilta yhteisöiltä se osuus korvauksesta, joka vastaa niiden vastuuta aiheutuneesta vahingosta. Nämä menettelyt eri yhteisrekisterinpitäjien ja henkilötietojen käsittelijöiden kesken käydään sen jälkeen, kun rekisteröity on saanut korvauksen, eikä rekisteröity osallistu niihin.

Euroopan neuvoston oikeudellisessa kehyksessä, uudistetun yleissopimuksen 108 12 artiklassa edellytetään, että sopimuspuolet ottavat käyttöön asianmukaiset

651 *Ibid.*, johdanto-osan 146 kappale.

652 *Ibid.*, 82 artiklan 2 ja 5 kohta.

oikeussuojakeinot yleissopimuksen vaatimukset täytäntöönpanevan kansallisen lainsäädännön rikkomisen varalta. Uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että oikeussuojakeinoihin täytyy kuulua mahdollisuus riitauttaa oikeudessa päätös tai käytäntö ja että myös tuomioistuimen ulkopuolisia oikeussuojakeinoja on annettava saataville[653]. Kukin sopimuspuoli voi päättää oman harkintansa mukaan näiden oikeussuojakeinojen saatavuuteen liittyvistä yksityiskohtaisista ehdoista ja eri säännöistä sekä noudatettavasta menettelystä. Sopimuspuolten ja kansallisten tuomioistuinten olisi myös harkittava taloudellisia korvauksia käsittelyn aiheuttamista aineellisista ja aineettomista vahingoista sekä mahdollisuutta esittää ryhmäkanteita.[654]

6.2.4 Seuraamukset

Euroopan neuvoston oikeudessa uudistetun yleissopimuksen 108 12 artiklassa määrätään, että kunkin sopimuspuolen on toteutettava asianmukaiset seuraamukset ja oikeussuojakeinot sen kansallisen lainsäädännön rikkomisesta, jolla yleissopimuksessa 108 mainitut tietosuojan perusperiaatteet toteutetaan. Yleissopimuksessa ei määrätä erityisistä seuraamuksista. Sitä vastoin siinä todetaan selkeästi, että kukin sopimuspuoli voi oman harkintansa mukaan määrittää oikeudellisten tai muiden kuin oikeudellisten seuraamusten luonteen ja että ne voivat olla rikosoikeudellisia, hallinnollisia tai siviilioikeudellisia. Uudistetun yleissopimuksen 108 selitysmuistiossa todetaan, että seuraamusten on oltava tehokkaita, varoittavia ja oikeasuhteisia[655]. Sopimuspuolten on noudatettava tätä periaatetta määrittäessään kansallisessa oikeusjärjestyksessä käytettävissä olevien seuraamusten luonteen ja vakavuuden.

EU:n oikeudessa yleisen tietosuoja-asetuksen 83 artiklassa annetaan jäsenvaltioiden valvontaviranomaiselle valtuudet määrätä hallinnollisia sakkoja asetuksen rikkomisesta. Kyseisessä 83 artiklassa säädetään myös sakkojen tasosta ja seikoista, jotka kansallisten viranomaisten on otettava huomioon päättäessään sakon määräämisestä, sekä kyseisen sakon suurimmasta kokonaismäärästä. Seuraamusjärjestelmä on siis yhdenmukainen koko EU:ssa.

Yleisessä tietosuoja-asetuksessa noudatetaan porrastettua sakottamismallia. Valvontaviranomaiset voivat määrätä asetuksen rikkomisesta hallinnollisen sakon,

653 Uudistettu yleissopimus 108, selitysmuistio, 100 kohta.

654 *Ibid.*

655 *Ibid.*

joka on enintään 20 000 000 euroa, tai jos kyseessä on yritys, neljä prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi. Rikkomuksia, joista voidaan määrätä tämän tason sakko, ovat muun muassa käsittelyn perusperiaatteiden ja suostumuksen edellytysten rikkominen, rekisteröityjen oikeuksien rikkominen ja henkilötietojen siirtoa vastaanottajille kolmansissa maissa koskevien asetuksen säännösten rikkominen. Muista rikkomuksista valvontaviranomaiset voivat määrätä sakkoja, jotka ovat enintään 10 000 000 euroa, tai jos kyseessä on yritys, kaksi prosenttia sen edeltävän tilikauden vuotuisesta maailmanlaajuisesta kokonaisliikevaihdosta sen mukaan, kumpi näistä määristä on suurempi.

Valvontaviranomaisten on hallinnollista sakkoa ja sakon määrää määrätessään otettava huomioon useita seikkoja[656]. Niiden on esimerkiksi otettava asianmukaisesti huomioon rikkomisen luonne, vakavuus ja kesto, henkilötietoryhmät, joihin rikkominen vaikuttaa, ja rikkomisen tahallisuus tai tuottamuksellisuus. Jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut toimenpiteitä rekisteröityneille aiheutuneiden vahinkojen lieventämiseksi, sekin on otettava huomioon. Myös yhteistyön aste valvontaviranomaisen kanssa rikkomisen korjaamiseksi ja tapa, jolla rikkominen tuli valvontaviranomaisen tietoon (esimerkiksi se, ilmoittiko siitä käsittelystä vastaava yhteisö vai rekisteröity, jonka oikeuksia loukattiin) ovat muita tärkeitä seikkoja, jotka ohjaavat valvontaviranomaisten päätöstä.[657]

Sen lisäksi, että valvontaviranomaiset voivat määrätä hallinnollisia sakkoja, niillä on käytössään myös laaja valikoima muita korjaavia toimivaltuuksia. Valvontaviranomaisten korjaavista toimivaltuuksista säädetään yleisen tietosuoja-asetuksen 58 artiklassa. Niitä ovat muun muassa rekisterinpitäjille ja henkilötietojen käsittelijöille annettavat määräykset, varoitukset ja huomautukset sekä väliaikaisten tai jopa pysyvien käsittelykieltojen määrääminen.

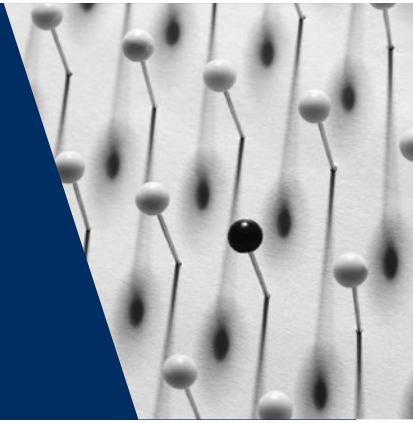
EU:n toimielinten tietosuoja-asetuksen erityisen soveltamisalan vuoksi EU:n toimielinten tai elinten tekemistä EU:n oikeuden rikkomuksista voidaan määrätä seuraamuksia kurinpitotoimina. Tämän asetuksen 49 artiklan mukaan ”[j]os Euroopan yhteisöjen palveluksessa oleva virkamies tai muu toimihenkilö tahallaan tai tuottamuksellisesti jättää täyttämättä tämän asetuksen mukaiset velvollisuutensa, hänelle voidaan määrätä kurinpitoseuraamus”.

656 Yleinen tietosuoja-asetus, 83 artiklan 2 kohta.

657 Tietosuojatyöryhmä (2017), *asetuksessa 2016/679 tarkoitettujen hallinnollisten sakkojen soveltamista ja määräämistä koskevat suuntaviivat*, WP 253, 3.10.2017.

7

Kansainväliset henkilötietojen siirrot



EU	Käsiteltävät asiat	EN
Henkilötietojen siirrot		
Yleinen tietosuoja-asetus, 44 artikla	Määritelmä	Uudistettu yleissopimus 108, 14 artiklan 1 ja 2 kohta
Henkilötietojen vapaa liikkuvuus		
Yleinen tietosuoja-asetus, 1 artiklan 3 kohta ja johdanto-osan 170 kappale	EU:n jäsenvaltioiden välillä	
	Yleissopimuksen 108 sopimuspuolten välillä	Uudistettu yleissopimus 108, 14 artiklan 1 kohta
Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille		
Yleinen tietosuoja-asetus, 45 artikla C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 2015	Tietosuojan tason riittävyyttä koskeva päätös / kolmannet maat tai kansainväliset järjestöt, joissa on riittävä tietosuojan taso	Uudistettu yleissopimus 108, 14 artiklan 2 kohta
Yleinen tietosuoja-asetus, 46 artiklan 1 ja 2 kohta	Asianmukaiset suojatoimet, muun muassa rekisteröityjen täytäntöönpanokelpoiset oikeudet ja oikeussuojakeinot, jotka on taattu tietosuojaa koskevilla vakiolausekkeilla, yritystä koskevat sitovat säännöt, käytännesäännöt ja sertifiointimekanismit	Uudistettu yleissopimus 108, 14 artiklan 2, 3, 5 ja 6 kohta

EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus, 46 artiklan 3 kohta	Toimivaltaisen valvontaviranomaisen luvalla: sopimuslausekkeet tai viranomaisten välisiin hallinnollisiin järjestelyihin sisältyvät säännökset	
Yleinen tietosuoja-asetus, 46 artiklan 5 kohta	Direktiivin 95/46/EY perusteella olemassa olevat luvat	
Yleinen tietosuoja-asetus, 47 artikla	Yritystä koskevat sitovat säännöt	
Yleinen tietosuoja-asetus, 49 artikla	Erityistilanteita koskevat poikkeukset	Uudistettu yleissopimus 108, 14 artiklan 4 kohta
Esimerkkejä: EU:n ja Yhdysvaltojen PNR-sopimus EU:n ja Yhdysvaltojen SWIFT-sopimus	Kansainväliset sopimukset	Uudistettu yleissopimus 108, 14 artiklan 3 kohdan a alakohta

EU:n oikeudessa yleisessä tietosuoja-asetuksessa säädetään tietojen vapaasta liikkuvuudesta Euroopan unionissa. Siinä on kuitenkin erityisiä vaatimuksia henkilötietojen siirroille EU:n ulkopuolisiin kolmansiin maihin ja kansainvälisille järjestöille. Asetuksessa tunnustetaan kyseisten siirtojen merkitys erityisesti kansainvälisen kaupan ja yhteistyön kannalta, mutta siinä tunnustetaan myös henkilötietoja koskevan riskin kasvaminen. Asetuksella pyritään siksi tarjoamaan kolmansiin maihin siirrettäville henkilötiedoille sama suojan taso kuin EU:ssa.[658] Myös Euroopan neuvoston oikeudessa tunnustetaan rajat ylittävää tietojensiirtoa koskevien täytäntöönpanosääntöjen merkitys. Se perustuu vapaaseen liikkuvuuteen osapuolten välillä ja siirtoja muille kuin sopimuspuolille koskeviin erityisvaatimuksiin.

7.1 Henkilötietojen siirtojen luonne

Keskeiset kohdat

- Sekä EU:n että Euroopan neuvoston oikeudessa on sääntöjä henkilötietojen siirroista vastaanottajille kolmansissa maissa tai kansainvälisille järjestöille.
- Kun varmistetaan, että rekisteröityjen oikeudet suojataan, kun tietoja siirretään EU:n ulkopuolelle, EU:n oikeudessa taattu suoja voi seurata EU:sta peräisin olevia henkilötietoja.

658 Yleinen tietosuoja-asetus, johdanto-osan 101 ja 116 kappale.

Euroopan neuvoston oikeudessa rajan yli tapahtuva tietojen siirto määritellään henkilötietojen siirroksi vastaanottajille, jotka ovat vieraan lainkäyttövallan alaisia[659]. Rajan yli tapahtuvat tietojen siirrot vastaanottajalle, joka ei kuulu sopimuspuolen lainkäyttövaltaan, sallitaan vain, jos niissä on asianmukainen suojan taso[660].

EU:n oikeudessa säännellään sellaisten henkilötietojen siirtoa, ”joita käsitellään tai joita on tarkoitus käsitellä kolmanteen maahan tai kansainväliselle järjestölle siirtämisen jälkeen”[661]. Ne sallitaan vain, jos niissä noudatetaan yleisen tietosuoja-asetuksen V luvussa asetettuja sääntöjä.

Henkilötietojen rajat ylittävät siirrot sallitaan Euroopan neuvoston oikeuden mukaan vain vastaanottajalle, joka on sopimuspuolen lainkäyttövallan alainen, ja EU:n oikeuden mukaan vastaanottajalle, joka on jäsenvaltion lainkäyttövallan alainen. Molemmissa oikeusjärjestelmissä sallitaan tietojen siirto maahan, joka ei ole sopimuspuoli tai jäsenvaltio, jos tietyt edellytykset täytetään.

7.2 Henkilötietojen vapaa liikkuminen/siirto jäsenvaltioiden tai sopimuspuolten välillä

Keskeiset kohdat

- Henkilötietojen liikkumista koko EU:ssa sekä henkilötietojen siirtoja uudistetun yleissopimuksen 108 sopimuspuolten välillä ei saa rajoittaa. Koska kaikki uudistetun yleissopimuksen 108 sopimuspuolet eivät kuitenkaan ole EU:n jäsenvaltioita, siirtoja EU:n jäsenvaltiosta kolmanteen maahan, joka kuitenkin on yleissopimuksen 108 sopimuspuoli, ei voida tehdä, elleivät siirrot täytä yleisessä tietosuoja-asetuksessa asetettuja edellytyksiä.

Euroopan neuvoston oikeuden mukaan henkilötietoja on voitava siirtää vapaasti uudistetun yleissopimuksen 108 osapuolina olevien valtioiden välillä. Siirto voidaan kuitenkin kieltää, jos on todellinen ja vakava riski siitä, että siirto toiseen sopimuspuoleen voisi johtaa yleissopimuksen säännösten kiertämiseen tai jos sopimuspuolen on tehtävä niin alueelliseen kansainväliseen järjestöön kuuluvien valtioiden yhteisten suojaa koskevien yhdenmukaistettujen sääntöjen nojalla[662].

659 Uudistettu yleissopimus 108, selitysmuistio, 102 kohta.

660 Uudistettu yleissopimus 108, 14 artiklan 2 kohta.

661 Yleinen tietosuoja-asetus, 44 artikla.

662 Uudistettu yleissopimus 108, 14 artiklan 1 kohta.

EU:n oikeuden mukaan henkilötietojen vapaata liikkuvuutta EU:n jäsenvaltioiden välillä ei saa rajoittaa eikä kieltää syistä, jotka liittyvät luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä[663]. Vapaan liikkuvuuden aluetta on laajennettu sopimuksella Euroopan talousalueesta[664], joka tuo Islannin, Liechtensteinin ja Norjan sisämarkkinoille.

Esimerkki: Jos sellaisen kansainvälisen yritysryhmän tytäryhtiö, jolla on toimipaikkoja useissa EU:n jäsenvaltioissa, muun muassa Sloveniassa ja Ranskassa, siirtää henkilötietoja Sloveniasta Ranskaan, tällaista tietojen siirtoa ei saa rajoittaa eikä kieltää Slovenian kansallisessa lainsäädännössä luonnollisten henkilöiden suojeluun henkilötietojen käsittelyssä liittyvistä syistä.

Mutta jos sama slovenialainen tytäryhtiö haluaa siirtää samat henkilötiedot emoyhtiölleen Malesiaan, slovenialaisen tietojen viejän on otettava huomioon yleisen tietosuoja-asetuksen V luvussa esitetyt säännöt. Näiden säännösten tarkoituksena on suojata EU:n lainkäyttövaltaan kuuluvien rekisteröityjen henkilötietoja.

EU:n oikeudessa rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten ETA:n jäsenvaltioihin tehtyihin henkilötietoihin siirtoihin sovelletaan direktiiviä (EU) 2016/680[665]. Näin myös varmistetaan, että toimivaltaisten viranomaisten unionissa suorittamaa henkilötietojen vaihtoa ei rajoiteta tai kielletä tietosuojaan liittyvistä syistä. Euroopan neuvoston oikeudessa kaikkien henkilötietojen käsittely (myös niiden rajat ylittävät siirrot yleissopimuksen 108 muihin sopimuspuoliin) ilman tarkoituksiin tai toiminta-aloihin perustuvia poikkeuksia kuuluvat yleissopimuksen 108 soveltamisalaan, joskin sopimuspuolet voivat määrätä poikkeuksia. Kaikki ETA:n jäsenvaltiot ovat myös yleissopimuksen 108 osapuolia.

663 Yleinen tietosuoja-asetus, 1 artiklan 3 kohta.

664 Neuvoston ja komission päätös, tehty 13 päivänä joulukuuta 1993, Euroopan yhteisöjen ja niiden jäsenvaltioiden sekä Itävallan tasavallan, Suomen tasavallan, Islannin tasavallan, Liechtensteinin ruhtinaskunnan, Norjan kuningaskunnan, Ruotsin kuningaskunnan ja Sveitsin valaliiton välisen Euroopan talousaluetta koskevan sopimuksen tekemisestä, EYVL 1994, L 1.

665 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta, EUVL 2016, L 119.

7.3 Henkilötietojen siirrot kolmansiin maihin / muihin kuin sopimuspuoliin tai kansainvälisille järjestöille

Keskeiset kohdat

- Sekä **Euroopan neuvosto** että **EU** sallivat henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille, mikäli henkilötietojen suoja täyttää tietyt edellytykset.
  - **Euroopan neuvoston oikeuden** mukaan tietosuojan riittävä taso voidaan saada aikaan valtion tai kansainvälisen järjestön lain nojalla tai ottamalla käyttöön asianmukaisia vaatimuksia.
  - **EU:n oikeuden** mukaan siirtoja voidaan tehdä, jos kolmas maa varmistaa riittävän suojan tason tai jos rekisterinpitäjä tai henkilötietojen käsittelijä tarjoaa asianmukaiset suojatoimet, muun muassa täytäntöönpanokelpoiset rekisteröidyn oikeudet ja oikeussuojakeinot, esimerkiksi tietosuojaa koskevilla vakiolausekkeilla tai yritystä koskevilla sitovilla säännöillä.
- **Sekä Euroopan neuvoston että EU:n oikeudessa** säädetään poikkeuslausekkeista, joiden nojalla henkilötietoja voidaan siirtää erityisolosuhteissa silloinkin, kun suojan taso ei ole riittävä tai käytössä ei ole asianmukaisia suojatoimia.

Vaikka sekä Euroopan neuvoston että EU:n oikeudessa sallitaan tietojen siirtäminen kolmansiin maihin tai kansainvälisille järjestöille, niissä asetetaan erilaisia edellytyksiä. Molempien järjestöjen edellytyksissä otetaan huomioon ne asettaneen järjestön erilainen rakenne ja tarkoitukset.

EU:n oikeuden mukaan on periaatteessa kaksi tapaa sallia henkilötietojen siirto kolmansiin maihin tai kansainvälisille järjestöille. Henkilötietojen siirtoja voidaan toteuttaa Euroopan komission tietosuojan tason riittävyyttä koskevan päätöksen perusteella[666] tai, jollei päätöstä tietosuojan tason riittävyydestä ole tehty, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet, muun muassa rekisteröidyn täytäntöönpanokelpoiset oikeudet ja oikeussuojakeinot[667]. Jos päätöstä tietosuojan tason riittävyydestä ei ole tehty eikä asianmukaisia suojatoimia ole, käytettävissä on useita poikkeuksia.

666 Yleinen tietosuoja-asetus, 45 artikla.

667 *Ibid.*, 46 artikla.

Euroopan neuvoston oikeudessa tietojen vapaa siirtäminen muille kuin yleissopimuksen osapuolille on kuitenkin sallittua vain, kun se perustuu

- kyseisen valtion tai kansainvälisen järjestön lakiin, muun muassa sovellettaviin kansainvälisiin valtiosopimuksiin tai asianmukaiset suojatoimet takaaviin sopimuksiin

- tapauskohtaisiin tai hyväksyttyihin vakiosuojatoimiin, joista on säädetty oikeudellisesti sitovilla ja täytäntöönpanokelpoisilla säädöksillä, jotka on antanut ja pannut täytäntöön siirtoon ja myöhempään käsittelyyn osallistuva henkilö[668].

EU:n oikeuden tapaan käytettävissä on useita poikkeuksia, jos tietosuojan taso ei ole asianmukainen.

7.3.1 Siirrot tietosuojan riittävyyttä koskevan päätöksen perusteella

EU:n oikeudessa henkilötietojen vapaasta siirrosta kolmansiin maihin, joissa on riittävä tietosuojan taso, säädetään yleisen tietosuoja-asetuksen 45 artiklassa. Euroopan unionin tuomioistuin on selventänyt, että ”tietosuojan riittävä taso” edellyttää, että kolmas maa tosiasiallisesti takaa perusoikeuksien suojan sellaisen tason, joka ”pääosiltaan vastaa”[669] unionin oikeusjärjestyksessä taattua suojaa. Keinot, joita kyseinen kolmas maa voi käyttää taatakseen tällaisen suojan tason, voivat poiketa niistä, joita unionissa käytetään, ja jotta tietosuojan taso olisi riittävä, kolmannen maan ei ole tarpeen kopioida EU:n sääntöjä kohta kohdalta[670].

Euroopan komissio arvioi tietosuojan tasoa ulkomailla tarkastelemalla maiden kansallista lainsäädäntöä ja sovellettavia kansainvälisiä velvollisuuksia. Huomioon on otettava myös maan osallistuminen monenvälisiin tai alueellisiin järjestelmiin, erityisesti henkilötietojen suojaa koskeviin. Jos Euroopan komissio havaitsee, että kolmas maa tai kansainvälinen järjestö takaa tietosuojan riittävän tason, se voi antaa

668 Uudistettu yleissopimus 108, 14 artiklan 3 kohdan a ja b alakohta.

669 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015, 96 kohta.

670 *Ibid.*, 74 kohta. Ks. myös Euroopan komissio (2017), komission tiedonanto Euroopan parlamentille ja neuvostolle ”Henkilötietojen vaihtaminen ja suojaaminen globalisoituneessa maailmassa”, COM(2017) 7 final, 10.1.2017, s. 6.

tietosuojan riittävyyttä koskevan päätöksen, joka on sitova.[671] Euroopan unionin tuomioistuin on kuitenkin todennut, että kansallisilla valvontaviranomaisilla on edelleen toimivalta tutkia henkilön vaatimus sellaisten henkilötietojensa suojasta, jotka on siirretty kolmanteen maahan, jonka komissio on katsonut takaavan riittävän suojan tason, kun henkilön mukaan kolmannessa maassa voimassa olevat oikeussäännöt ja käytännöt eivät takaa tietosuojan riittävää tasoa[672].

Euroopan komissio voi myös arvioida kolmannen maan alueen tietosuojan riittävyyttä tai keskittyä vain tiettyihin aloihin, kuten tapauksessa Kanadan yksityisestä kauppalainsäädännöstä[673]. Lisäksi on paljon tietosuojan riittävyyden toteavia päätöksiä, jotka perustuvat EU:n ja kolmansien maiden välisiin sopimuksiin. Nämä päätökset koskevat yksinomaan tietyntyyppistä tietojen siirtoa, kuten matkustajarekisterien siirtoa lentoyhtiöiltä muiden maiden rajavalvontaviranomaisille silloin, kun lentoyhtiö lentää EU:sta tiettyihin ulkomaankohteisiin (ks. 7.3.4 kohta).

Tietosuojan riittävyyttä koskevia päätöksiä seurataan jatkuvasti. Komissio seuraa jatkuvasti kehitystä, joka saattaa vaikuttaa päätösten asemaan. Jos siis Euroopan komissio havaitsee, että kolmas maa tai kansainvälinen järjestö ei enää täytä tietosuojan riittävyyttä koskevan päätöksen perustana olevia edellytyksiä, komissio voi muuttaa päätöstä, lykätä sen voimaantuloa tai kumota sen. Komissio voi myös aloittaa neuvottelut kyseessä olevan kolmannen maan tai kansainvälisen järjestön kanssa korjatakseen tilanteen, jonka vuoksi päätös annettiin.

Komission direktiivin 95/46/EY nojalla antamat tietosuojan riittävyyttä koskevat päätökset pysyvät voimassa, kunnes niitä muutetaan, ne korvataan tai kumotaan yleisen tietosuoja-asetuksen 45 artiklan mukaisesti annetulla komission päätöksellä.

Tähän mennessä Euroopan komissio on tunnustanut, että Andorra, Argentiina, Färsaaret, Guernsey, Israel, Jersey, Kanada (tietosuojasta ja sähköisistä asiakirjoista annetun lain – PIPEDA – soveltamisalaan kuuluvat kaupalliset järjestöt), Mansaari, Sveitsi, Uruguay ja Uusi-Seelanti tarjoavat tietosuojan riittävän tason. Euroopan komissio antoi vuonna 2000 tietojen siirroista Yhdysvaltoihin päätöksen tietosuojan

671 Maista, joista on tehty tietosuojan riittävyyttä koskeva päätös, on jatkuvasti päivitettävä luettelo Euroopan komission oikeusasioiden pääosaston kotisivulla.

672 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015, 63 ja 65–66 kohta.

673 Euroopan komissio (2002), 20 päivänä joulukuuta 2001 tehty päätös 2002/2/EY henkilötietojen suojaa ja sähköisiä asiakirjoja koskevan Kanadassa voimassa olevan lain tarjoaman tietosuojan riittävyydestä Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti, EYVL 2002, L 2.

tason riittävyydestä. Sen nojalla tietoja pystyttiin siirtämään yhdysvaltalaisille yrityksille, jotka ilmoittavat suojaavansa EU:sta siirrettyjä henkilötietoja ja noudattavansa niin sanottuja safe harbor -periaatteita[674]. Euroopan unionin tuomioistuin totesi tämän päätöksen pätemättömäksi vuonna 2015, ja uusi päätös annettiin heinäkuussa 2016. Sitä voitiin alkaa soveltaa yhtiöihin 1. elokuuta 2016 alkaen.

Esimerkki: Asiassa *Schrems*[675] Maximillian Schrems, joka on Itävallan kansalainen, on ollut Facebookin käyttäjä useiden vuosien ajan. Joitakin Schremsin Facebookille antamia tietoja siirrettiin Facebookin irlantilaisesta tytäryhtiöstä Yhdysvalloissa sijaitseville palvelimille, joissa niitä käsiteltiin. Schrems teki Irlannin tietosuojaviranomaiselle kantelun, jossa hän katsoi, että yhdysvaltalaisen väärinkäytösten paljastajan Edward Snowdenin Yhdysvaltojen tiedustelupalvelujen valvontatoimista tekemien paljastusten vuoksi Yhdysvalloissa voimassa olevat oikeussäännöt ja käytännöt eivät takaa riittävää suojaa maahan siirretyille tiedoille. Irlannin viranomainen hylkäsi kantelun, koska komissio oli katsonut 26. heinäkuuta 2000 antamassaan päätöksessä, että Yhdysvallat takaa safe harbor -järjestelmällä siirrettyjen henkilötietojen riittävän suojan. Asia saatettiin Irlannin High Courtin käsiteltäväksi, ja se teki siitä Euroopan unionin tuomioistuimelle ennakkoratkaisupyynnön.

Euroopan unionin tuomioistuin totesi, että komission päätös safe harbor -järjestelmän riittävyydestä on pätemätön. Euroopan unionin tuomioistuin pani ensin merkille, että päätöksen mukaan safe harbor -tietosuojaperiaatteiden sovellettavuutta voitiin rajoittaa kansallisen turvallisuuden, yleisen edun tai lainsäädännön vaatimusten vuoksi sekä Yhdysvaltain kansallisen lainsäädännön perusteella. Näin ollen päätöksellä sallittiin puuttuminen niiden henkilöiden perusoikeuksiin, joiden henkilötietoja siirretään tai voitaisiin siirtää Yhdysvaltoihin.[676] Se huomautti myös, että päätös ei sisältänyt mitään toteamusta siitä, että Yhdysvalloissa olisi sääntöjä, joilla olisi tarkoitus rajoittaa kyseistä puuttumista, eikä tehokasta oikeussuojaa tällaista puuttumista vastaan[677]. Euroopan unionin tuomioistuin korosti, että unionissa taattu

674 Komission päätös 2000/520/EY, tehty 26 päivänä heinäkuuta 2000, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti yksityisyyden suojaa koskevien safe harbor -periaatteiden antaman suojan riittävyydestä ja niihin liittyvistä Yhdysvaltojen kauppaministeriön julkaisemista useimmin esitetyistä kysymyksistä, EYVL L 215. Euroopan unionin tuomioistuin totesi päätöksen pätemättömäksi asiassa C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto].

675 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

676 *Ibid.*, 84 kohta.

677 *Ibid.*, 88–89 kohta.

perusvapauksien ja -oikeuksien suojan taso edellytti, että lainsäädännössä, jolla puututaan perusoikeuskirjan 7 ja 8 artiklassa taattuihin perusoikeuksiin, on säädettävä selvistä ja täsmällisistä toimenpiteen laajuutta ja soveltamista koskevista säännöistä ja asetettava henkilötietojen suojaa koskevat vähimmäissuojatoimet, poikkeukset ja rajoitukset[678]. Koska komission päätöksessä ei todettu, että Yhdysvallat tosiasiallisesti takaa sisäisen lainsäädäntönsä tai kansainvälisten sitoumustensa johdosta suojan tällaisen tason, tuomioistuin totesi, että se ei täyttänyt tietosuojadirektiivin asiaankuuluvan siirtosäännöksen vaatimuksia ja oli siksi pätemätön[679].

Yhdysvaltojen suojan taso ei siis ”pääosiltaan vastannut” EU:n takaamia perusoikeuksia ja -vapauksia[680]. Euroopan unionin tuomioistuin totesi, että EU:n perusoikeuskirjan useita artikloja rikottiin. Ensinnäkin loukattiin 7 artiklan keskeistä sisältöä, koska Yhdysvaltojen lainsäädännön nojalla ”viranomaiset pääsevät yleisesti sähköisen viestinnän sisältöön”. Myös 47 artiklan keskeistä sisältöä rikottiin, koska lainsäädännössä ei anneta yksityisille mitään mahdollisuutta käyttää oikeussuojakeinoja, jotta he saisivat tutustua henkilötietoihinsa tai voisivat saada tällaiset tiedot oikaistuiksi tai poistetuiksi. Lisäksi, koska safe harbor -järjestelyllä rikottiin edellä mainittuja artikloja, henkilötietoja ei enää käsitelty lainmukaisesti, mikä rikkoi 8 artiklaa.

Kun Euroopan unionin tuomioistuin oli todennut safe harbor -järjestelyn pätemättömäksi, komissio ja Yhdysvallat sopivat uudesta kehyksestä, EU:n ja Yhdysvaltojen välisestä Privacy Shield -järjestelystä. Komissio antoi 12. heinäkuuta 2016 päätöksen, jossa todettiin, että Yhdysvallat takaa riittävän suojan tason henkilötiedoille, jotka siirretään unionista Yhdysvalloissa sijaitseviin organisaatioihin Privacy Shield -järjestelyn[681] nojalla.

678 *Ibid.*, 91–92 kohta.

679 *Ibid.*, 96–97 kohta.

680 *Ibid.*, 73–74 ja 96 kohta.

681 Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY nojalla EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tarjoaman tietosuojan tason riittävyydestä, EUVL L 207. Tietosuojatyöryhmä suhtautui myönteisesti parannuksiin, joita Privacy Shield -mekanismi toi safe harbor -päätökseen verrattuna, ja kiitti komissiota ja Yhdysvaltojen viranomaisia siitä, että Privacy Shield -asiakirjojen lopullisessa versiossa oli otettu huomioon EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tietosuojan riittävyyttä koskevan päätöksen luonnoksesta annetussa tietosuojatyöryhmän lausunnossa WP238 esitetyt huolenaiheet. Se korosti kuitenkin, että järjestelyyn jäi edelleen useita huolta aiheuttavia seikkoja. Lisätietoa on englanniksi tietosuojatyöryhmän lausunnossa ”*Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*”, annettu 13.4.2016, 16/EN WP 238.

Safe harbor -järjestelyn tapaan EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn tavoitteena on suojata henkilötietoja, joita siirretään EU:sta Yhdysvaltoihin kaupallisissa tarkoituksissa[682]. Yhdysvaltalaisyritykset voivat vapaaehtoisesti antaa oman varmennuksen Privacy Shield -luetteloon kuulumisesta ja sitoutua täyttämään järjestelyn tietosuojavaatimukset. Toimivaltaiset Yhdysvaltojen viranomaiset seuraavat ja todentavat, noudattavatko varmennetut yritykset näitä vaatimuksia.

Privacy Shield -järjestelyssä määrätään erityisesti

- EU:sta henkilötietoja vastaanottavien yhtiöiden tietosuojavelvollisuuksista
- yksilöiden suojasta ja oikeussuojakeinoista, erityisesti sellaisen oikeusasiamiesjärjestelmän perustamisesta, joka on riippumaton Yhdysvaltojen tiedustelupalveluista ja joka käsittelee valituksia yksityishenkilöiltä, jotka katsovat, että Yhdysvaltojen viranomaiset ovat käyttäneet heidän henkilötietojaan lainvastaisesti kansallisen turvallisuuden alalla
- vuotuisesta yhteisestä uudelleentarkastelusta, jossa arvioidaan järjestelyn toteuttamista[683]; ensimmäinen tarkastelu tehtiin syyskuussa 2017[684].

Yhdysvaltojen hallinto on antanut Privacy Shield -päätöksen tueksi kirjallisia sitoumuksia ja varmistuksia. Niissä määrätään rajoituksista ja suojatoimista, jotka koskevat Yhdysvaltojen hallinnon pääsyä henkilötietoihin lainvalvontaa ja kansallista turvallisuutta koskevia tarkoituksia varten.

7.3.2 Asianmukaisia suojatoimia edellyttävät siirrot

Sekä **EU:n oikeudessa** että **Euroopan neuvoston oikeudessa** tunnustetaan, että tietoja vievän rekisterinpitäjän ja kolmannessa maassa tai kansainvälisessä järjestössä sijaitsevan vastaanottajan välisillä asianmukaisilla suojatoimilla voidaan varmistaa vastaanottajan riittävän tietosuojan taso.

682 Lisätietoa on englanniksi tiedotteessa EU-U.S. Privacy Shield factsheet.

683 Lisätietoa on englanniksi Euroopan komission järjestelyä käsittelevällä verkkosivulla EU-U.S. Privacy Shield.

684 Euroopan komissio, komission kertomus Euroopan parlamentille ja neuvostolle EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn toiminnan ensimmäisestä vuosittaisesta tarkastelusta, COM(2017) 611 final, 18.10.2017. Ks. myös tietosuojatyöryhmä (englanniksi), *EU – U.S. Privacy Shield – First annual Joint Review*, annettu 28.11.2017, 17/EN WP 255.

EU:n oikeudessa henkilötietojen siirtäminen kolmanteen maahan tai kansainväliseen järjestöön sallitaan, jos rekisterinpitäjä tai henkilötietojen käsittelijä on toteuttanut asianmukaiset suojatoimet ja jos rekisteröityjen saatavilla on täytäntöönpanokelpoisia oikeuksia ja tehokkaita oikeussuojakeinoja[685]. EU:n tietosuojalainsäädännössä annetaan yksinomainen luettelo hyväksyttävistä asianmukaisista suojatoimista. Asianmukaisia suojatoimia voivat olla seuraavat:

- viranomaisten tai julkisten elinten välinen oikeudellisesti sitova ja täytäntöönpanokelpoinen väline
- yritystä koskevat sitovat säännöt
- tietosuojaa koskevat vakiolausekkeet, jotka tietosuojaviranomainen vahvistaa tai jotka komissio hyväksyy
- käytännesäännöt
- sertifiointimekanismit[686].

Asianmukaisia suojatoimia voivat olla myös EU:ssa sijaitsevan rekisterinpitäjän tai henkilötietojen käsittelijän ja kolmannessa maassa sijaitsevan vastaanottajan väliset yksilölliset sopimuslausekkeet. Toimivaltaisen valvontaviranomaisen on kuitenkin annettava lupa kyseisille sopimuslausekkeille ennen kuin niitä voidaan käyttää työkaluna henkilötietojen siirtämisessä. Myös viranomaiset voivat käyttää hallinnollisiin järjestelyihinsä sisältyviä tietosuojasäännöksiä, jos valvontaviranomainen on antanut niille luvan.[687]

Euroopan neuvoston oikeudessa sallitaan tietojen siirtäminen valtioon tai kansainväliselle järjestölle, joka ei ole uudistetun yleissopimuksen 108 sopimuspuoli, jos asianmukainen suojan taso varmistetaan. Se voi perustua

- valtion tai kansainvälisen järjestön lakiin tai
- oikeudellisesti sitovaan asiakirjaan kuuluvaan tapauskohtaiseen tai vakioituun suojatoimeen[688].

685 Yleinen tietosuoja-asetus, 46 artikla.

686 Yleinen tietosuoja-asetus, 46 artiklan 1 kohdan c ja d alakohta, 2 artiklan a, b, e ja f alakohta ja 47 artikla.

687 *Ibid.*, 46 artiklan 3 kohta.

688 Uudistettu yleissopimus 108, 14 artiklan 3 kohdan b alakohta.

Sopimuslausekkeita edellyttävät siirrot

Sekä **Euroopan neuvoston oikeudessa** että **EU:n oikeudessa** tunnustetaan, että tietoja vievän rekisterinpitäjän ja kolmannessa maassa sijaitsevan vastaanottajan välisillä sopimuslausekkeilla voidaan turvata vastaanottajan riittävä tietosuojan taso[689].

EU:ssa Euroopan komissio on laatinut tietosuojatyöryhmän avulla mallisopimuslausekkeet, jotka on komission päätöksellä virallisesti hyväksytty näytöksi tietosuojan riittävästä tasosta[690]. Koska komission päätökset ovat kaikilta osiltaan velvoittavia jäsenvaltioissa, tietojen siirron valvonnasta vastaavien kansallisten viranomaisten on tunnustettava nämä vakiosopimuslausekkeet omissa menettelyissään[691]. Näin ollen, jos tietoja vievä rekisterinpitäjä ja kolmannessa maassa sijaitseva vastaanottaja sopivat näistä lausekkeista ja allekirjoittavat ne, valvontaviranomaisen kuuluu pitää sitä riittävänä näyttönä asianmukaisista suojatoimista. Asiassa *Schrems* Euroopan unionin tuomioistuin kuitenkin katsoi, että Euroopan komissiolla ei ole toimivaltaa rajoittaa kansallisten valvontaviranomaisten valtuuksia valvoa henkilötietojen siirtämistä kolmanteen maahan, josta komissio on antanut tietosuojan riittävyyttä koskevan päätöksen[692]. Kansallisia valvontaviranomaisia ei näin ollen estetä käyttämästä valtuuksiaan, muun muassa oikeutta lykätä henkilötietojen siirtämistä tai kieltää se, kun siirrossa rikotaan EU:n tai kansallista tietosuojalainsäädäntöä, esimerkiksi silloin, kun tietojen tuoja ei noudata vakiosopimuslausekkeita[693].

EU:n oikeudelliseen kehykseen kuuluvat vakiosopimuslausekkeet eivät estä rekisterinpitäjiä laatimasta muita tapauskohtaisia ja yksilöllisiä sopimuslausekkeita, kunhan valvontaviranomainen hyväksyy ne[694]. Niillä on kuitenkin varmistettava sama suojan taso kuin vakiosopimuslausekkeilla. Tapauskohtaisia lausekkeita hyväksyessään valvontaviranomaisten on sovellettava yhdenmukaisuusmekanismia, jotta voidaan

689 Yleinen tietosuoja-asetus, 46 artiklan 3 kohta; uudistettu yleissopimus 108, 14 artiklan 3 kohdan b alakohta.

690 *Ibid.*, 46 artiklan 2 kohdan b alakohta ja 46 artiklan 5 kohta.

691 *Ibid.*, 46 artiklan 2 kohdan c alakohta; sopimus Euroopan unionin toiminnasta, 288 artikla.

692 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015, 96–98 kohta ja 102–105 kohta.

693 Komissio muutti päätöstään mallisopimuslausekkeista ottaakseen huomioon Euroopan unionin tuomioistuimen kannan asiassa *Schrems*. Komission täytäntöönpanopäätös (EU) 2016/2297, annettu 16 päivänä joulukuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista, henkilötietojen siirtoa kolmansiin maihin ja tällaisten tietojen siirtoa kyseisiin maihin sijoittautuneille henkilötietojen käsittelijöille koskevista mallisopimuslausekkeista annettujen päätösten 2001/497/EY ja 2010/87/EU muuttamisesta, EUVL 2016, L344.

694 Yleinen tietosuoja-asetus, 46 artiklan 3 kohdan a alakohta.

varmistaa sääntelyn yhdenmukainen toimintamalli kaikkialla unionissa[695]. Se tarkoittaa, että toimivaltaisen valvontaviranomaisen on annettava päätösehdotuksensa tiedoksi tietosuojaneuvostolle. Tietosuojaneuvosto antaa asiasta lausunnon, ja valvontaviranomaisen on otettava lausunto huomioon mahdollisimman kattavasti sen päätöstä koskevissa menettelyissä. Jos se ei aio noudattaa tietosuojaneuvoston lausuntoa, käynnistetään tietosuojaneuvoston kiistanratkaisumenettely, ja neuvosto antaa sitovan päätöksen[696].

Vakiosopimuslausekkeiden tärkeimmät ominaisuudet ovat seuraavat:

- kolmatta osapuolta suojaava lauseke, jonka nojalla rekisteröidyt voivat käyttää sopimukseen kuuluvia oikeuksia, vaikka he eivät olisi sopimuksen osapuolia

- tietojen vastaanottajan tai tuojan suostumus kuulua tietoja vievän rekisterinpitäjän kansallisen valvontaviranomaisen ja/tai tuomioistuinten määräysvaltaan kiistatilanteessa.

Tietoja vievä rekisterinpitäjä voi nyt valita kahdesta vakiolausekkeiden kokonaisuudesta, jotka ovat käytettävissä rekisterinpitäjien välisiä siirtoja varten[697]. Rekisterinpitäjän ja henkilötietojen käsittelijän välisiä vaihtoja varten on vain yksi vakiosopimuslausekkeiden kokonaisuus[698]. Näitä vakiosopimuslausekkeita käsitellään kuitenkin parhaillaan oikeudessa.

Esimerkki: Kun Euroopan unionin tuomioistuin oli todennut safe harbor -päätöksen pätemättömäksi[699], henkilötietojen siirrot Yhdysvaltoihin eivät voineet enää perustua kyseiseen tietosuojan riittävyyttä koskevaan päätökseen. Kun

695 *Ibid.*, 63 artiklan ja 64 artiklan 1 kohdan e alakohta.

696 *Ibid.*, 64 ja 65 artikla.

697 Kokonaisuus I sisältyy direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen kolmansiin maihin siirtoa varten 15 päivänä kesäkuuta 2001 tehdyn Euroopan komission päätöksen 2001/497/EY (EYVL 2001, L 181) liitteeseen (2001); kokonaisuus II sisältyy päätöksen 2001/497/EY muuttamisesta vaihtoehtoisten mallisopimuslausekkeiden ottamiseksi käyttöön henkilötietojen kolmansiin maihin siirtoa varten 27 päivänä joulukuuta 2004 tehdyn päätöksen 2004/915/EY (EUVL 2004, L 385) liitteeseen (2004).

698 Euroopan komissio (2010), komission päätös 2010/87, annettu 5 päivänä helmikuuta 2010, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisista mallisopimuslausekkeista henkilötietojen siirtoa varten kolmansiin maihin sijoittautuneille henkilötietojen käsittelijöille, EUVL 2010, L 39. Käsikirjan laatimisen aikaan Irlannin High Court. käsitteli vakiosopimuslausekkeiden käyttöä henkilötietojen Yhdysvaltoihin siirtämisen perustana.

699 EUT, C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015.

neuvottelut Yhdysvaltojen viranomaisten kanssa olivat käynnissä ja ennen uuden tietosuojan riittävyyttä koskevan päätöksen antamista (se annettiin lopulta 12. heinäkuuta 2016)[700], siirtoja voi tehdä ainoastaan muiden oikeusperustojen, kuten vakiosopimuslausekkeiden tai yritystä koskevien sitovien sääntöjen, perusteella. Useat yritykset, muun muassa Facebook Ireland (jota vastaan oli nostettu kanne, joka johti safe harbor -päätöksen toteamiseen pätemättömäksi) siirtyivät käyttämään vakiosopimuslausekkeita voidakseen jatkaa EU:n ja Yhdysvaltojen välisiä tiedonsiirtoja.

Maximillian Schrems teki Irlannin valvontaviranomaiselle valituksen, jossa se pyysi keskeyttämään tietojen siirtämisen Yhdysvaltoihin vakiosopimuslausekkeiden perusteella. Pääasiallisesti hän väitti, että kun hänen henkilötietojaan siirretään Facebookin irlantilaisesta tytäryhtiöstä Facebook Inc:lle ja Yhdysvalloissa sijaitseville palvelimille, niiden suojasta ei ole takuuta. Facebook Inc:tä sitovat Yhdysvaltain lait, joiden nojalla se voidaan velvoittaa luovuttamaan henkilötietoja Yhdysvaltojen lainvalvontaviranomaisille, eikä eurooppalaisten yksityishenkilöiden käytettävissä ole oikeussuojakeinoja tämän käytännön riitauttamiseksi[701]. Näiden syiden vuoksi Euroopan unionin tuomioistuin katsoi, että safe harbor -päätös oli pätemätön, ja vaikka tuomioistuimen tuomio rajoittui kyseisen päätöksen tutkimiseen, kantaja katsoi esiin nostettujen kysymysten olevan yhtä asiaankuuluvia myös silloin, kun siirto perustuu sopimuslausekkeisiin. Asiakirjan kirjoittamisen aikaan Irlannin High Court tutki asiaa. Kantaja aikoo ilmeisesti saattaa asian Euroopan unionin tuomioistuimen käsiteltäväksi, ja hänen tavoitteenaan on riitauttaa Euroopan komission mallisopimuslausekkeita koskevan päätöksen pätevyys. Kuten 5 luvussa kuvataan, ainoastaan Euroopan unionin tuomioistuimella on toimivalta todeta EU:n säädös pätemättömäksi.

Yritystä koskevia sitovia sääntöjä edellyttävät siirrot

EU:n oikeuden nojalla henkilötietoja voidaan siirtää yritystä koskevien sitovien sääntöjen perusteella yritysryhmässä tai yhteistä taloudellista toimintaa harjoittavien

700 Komission täytäntöönpanopäätös (EU) 2016/1250, annettu 12 päivänä heinäkuuta 2016, Euroopan parlamentin ja neuvoston direktiivin 95/46/EY mukaisesti EU:n ja Yhdysvaltojen välisen Privacy Shield -järjestelyn antaman suojan riittävyydestä.

701 Lisätietoa on tarkistetussa kantelussa, jonka Maximillian Schrems teki Irlannin tietosuojavaltuutetulle Facebook Ireland Ltd:stä 1. joulukuuta 2015.

yritysten välillä tehtävissä kansainvälisissä siirroissa[702]. Ennen kuin yritystä koskevia sitovia sääntöjä voidaan käyttää työkaluna henkilötietojen siirrossa, toimivaltaisen valvontaviranomaisen on hyväksyttävä ne yritystä koskevien sitovien sääntöjen mukaisesti hyödyntämällä yhdenmukaisuusmekanismia.

Yritystä koskevien sitovien sääntöjen hyväksyminen edellyttää, että ne ovat oikeudellisesti sitovia, että ne kattavat kaikki keskeiset tietosuojan periaatteet ja että niitä sovelletaan kaikkiin yritysryhmän jäseniin – ja että ne kaikki panevat säännöt täytäntöön. Niissä on nimenomaisesti annettava rekisteröidyille täytäntöönpanokelpoisia oikeuksia, niiden on sisällettävä kaikki keskeiset tietosuojan periaatteet ja noudatettava tiettyjä muodollisia vaatimuksia, kuten yrityksen rakenteen yksilöinti, siirtojen kuvaaminen ja tietosuojan periaatteiden soveltamisen yksilöinti. Tämä sisältää näiden tietojen antamisen rekisteröidyille. Yritystä koskevissa sitovissa säännöissä on yksilöitävä muun muassa rekisteröityjen oikeudet ja vastuu kaikista sääntöjen rikkomisista.[703] Yritystä koskevia sitovia sääntöjä hyväksyttäessä käynnistetään yhdenmukaisuusmekanismi valvontaviranomaisten yhteistyön varmistamiseksi (tätä kuvataan 5 luvussa).

Yhdenmukaisuusmekanismissa johtava valvontaviranomainen tarkastaa ehdotetut yritystä koskevat sitovat säännöt, hyväksyy päätösehdotuksen ja toimittaa sen tietosuojaneuvostolle. Tietosuojaneuvosto antaa asiasta lausunnon, ja johtava valvontaviranomainen voi hyväksyä virallisesti yritystä koskevat sitovat säännöt ottaen tietosuojaneuvoston lausunnon mahdollisimman kattavasti huomioon. Tämä lausunto ei ole oikeudellisesti sitova, mutta jos valvontaviranomainen ei aio noudattaa sitä, käynnistetään kiistanratkaisumenettely ja tietosuojaneuvoston on kokoonnuttava antamaan oikeudellisesti sitova päätös jäsentensä kahden kolmasosan enemmistöllä.[704]

Euroopan neuvoston oikeudessa oikeudellisesti sitovaan asiakirjaan kuuluvat tapauskohtaiset tai vakiosuojatoimet[705] sisältävät myös yritystä koskevat sitovat säännöt.

702 Yleinen tietosuoja-asetus, 47 artikla.

703 Yksityiskohtaisempi kuvaus on yleisen tietosuoja-asetuksen 47 artiklassa.

704 *Ibid.*, 57 artiklan 1 kohdan s alakohta, 58 artiklan 1 kohdan j alakohta, 64 artiklan 1 kohdan f alakohta, 65 artiklan 1 ja 2 kohta.

705 Uudistettu yleissopimus 108, 14 artiklan 3 kohdan b alakohta.

7.3.3 Erityistilanteita koskevat poikkeukset

EU:n oikeudessa henkilötietojen siirrot kolmanteen maahan voidaan oikeuttaa, vaikka asianmukaista päätöstä tai suojatoimia, kuten vakiosopimuslausekkeita tai yritystä koskevia sitovia sääntöjä ei ole, jossakin seuraavista tilanteista:

- rekisteröity antaa nimenomaisen suostumuksensa tiedonsiirtoon
- rekisteröity aloittaa – tai valmistautuu aloittamaan – sopimussuhteen, jossa tietojen siirto ulkomaille on välttämätöntä
- siirto on tarpeen rekisterinpitäjän ja kolmannen osapuolen välisen sopimuksen täytäntöönpanemiseksi rekisteröidyn etujen mukaisesti
- siirto on tärkeä yleisen edun kannalta
- siirto on tarpeen oikeudellisen vaateen laatimiseksi, esittämiseksi tai puolustamiseksi
- siirto on tarpeen rekisteröidyn elintärkeiden etujen suojelemiseksi
- tiedot siirretään yleisistä rekistereistä (tämä on esimerkki suuren yleisön ensisijaisista eduista, jotta voidaan saada yleisiin rekistereihin tallennettua tietoa)[706].

Jos mikään näistä tilanteista ei sovellu ja jos siirtojen perusteena ei voi olla tietosuojan riittävyyttä koskeva päätös tai asianmukaiset suojatoimet, siirto voidaan tehdä ainoastaan, jos se ei ole toistuva ja jos se koskee ainoastaan rajallista määrää rekisteröityjä ja on tarpeen rekisterinpitäjän sellaisten pakottavien ja oikeutettujen etujen toteuttamiseksi, joita rekisteröidyn edut tai perusoikeudet ja -vapaudet eivät syrjäytä[707]. Tällaisessa tapauksessa rekisterinpitäjän on arvioitava kaikki tiedonsiirtoon liittyvät seikat ja toteutettava suojatoimet. Rekisterinpitäjän on myös ilmoitettava valvontaviranomaiselle ja rekisteröidylle sekä siirrosta että pakottavista ja oikeutetuista eduista.

Se, että poikkeukset ovat lainmukaisten siirtojen viimeinen keino[708] (jota on käytettävä vain, jos tietosuojan riittävyyttä koskevaa päätöstä ja muita suojatoimia

706 Yleinen tietosuoja-asetus, 49 artikla.

707 *Ibid.*

708 *Ibid.*, 49 artiklan 1 kohta.

ei ole käytössä), korostaa niiden poikkeuksellista luonnetta, jota painotetaan vielä enemmän yleisen tietosuoja-asetuksen johdanto-osassa[709]. Näin ollen poikkeukset hyväksytään mahdollisuutena ”tehdä tiedonsiirtoja tietyissä tilanteissa” suostumuksen perusteella ja kun ”siirto tapahtuu satunnaisesti ja on tarpeellinen”[710] sopimukselle tai oikeudelliselle vaateelle.

Lisäksi tietosuojatyöryhmän ohjeiden mukaan erityistilanteita koskevien poikkeusten käytön on oltava poikkeuksellista, sen on perustuttava yksittäistapauksiin eikä niitä voida käyttää toistuvia tai suurimittaisia siirtoja varten[711]. Euroopan tietosuojavaltuutettu korosti myös asetuksen (EY) N:o 45/2001 mukaisten siirtojen oikeusperustana käytettävien poikkeusten poikkeuksellista luonnetta ja huomautti, että tätä ratkaisua pitäisi käyttää rajoitetuissa tapauksissa ja satunnaisiin siirtoihin[712].

Esimerkki: Global Distribution System (GDS) -palveluyritys, jonka päätoimipaikka on Yhdysvalloissa, toimittaa verkkovarausjärjestelmiä useille lentoyhtiöille, hotelleille ja risteilyaluksille ympäri maailmaa. Se käsittelee kymmenien miljoonien henkilöiden tietoja EU:ssa. GDS-yritys käyttää tietojen alkuperäisessä siirtämisessä Yhdysvalloissa sijaitseville palvelimilleen poikkeuksia siirtojen lainmukaisena perustana, koska ne ovat tarpeen sopimuksen tekemiseksi. Se ei näin ollen esitä mitään muita suojatoimia Euroopasta peräisin oleville henkilötiedoille, jotka siirretään Yhdysvaltoihin ja jaetaan sitten uudelleen hotelleihin ympäri maailmaa (eli myöhemmillekään siirroille ei ole suojatoimia). GDS-yritys ei noudata yleisen tietosuoja-asetuksen vaatimuksia lainmukaisista kansainvälisistä tietosiirroista, koska se käyttää poikkeuksia suurimittaisten siirtojen lainmukaisena perustana.

Ellei tietosuojan riittävyyttä koskevaa päätöstä ole annettu, EU tai sen jäsenvaltio voivat tärkeää yleistä etua koskevista syistä rajoittaa tiettyjen henkilötietoryhmien siirtoa kolmanteen maahan riippumatta kyseisten siirtojen täyttämistä ehdoista. Nämä rajoitukset on katsottava poikkeuksellisiksi, ja jäsenvaltioiden on ilmoitettava asianomaisista säännöksistä komissiolle.[713]

709 Ks. yleinen tietosuoja-asetus, 49 artiklan 1 kohdan a, b ja e alakohta ja johdanto-osan 113 kappale.

710 *Ibid.*, 49 artiklan 1 kohta.

711 Tietosuojatyöryhmä (2005), *valmisteluasiakirja 24. lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25.11.2005.

712 Euroopan tietosuojavaltuutettu, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, kannanotto, Bryssel, 14.7.2014, s. 15.

713 Ks. yleinen tietosuoja-asetus, 49 artiklan 5 kohta.

Euroopan neuvoston oikeudessa sallitaan tietojen siirtäminen alueille, joilla ei ole asianmukaista tietosuojaa, kun

- rekisteröity on antanut suostumuksen
- rekisteröidyn edut edellyttävät siirtoa
- siihen on tärkeitä oikeutettuja etuja, erityisesti huomattavia yleisiä etuja, joista on säädetty lailla
- se on demokraattisessa yhteiskunnassa välttämätön ja oikeasuhteinen toimenpide[714].

7.3.4 Siirrot kansainvälisten sopimusten perusteella

Jäsenvaltiot voivat tehdä kolmansien maiden kanssa kansainvälisiä sopimuksia, joissa määrätään henkilötietojen siirrosta tiettyihin tarkoituksiin. Sopimuksiin täytyy sisältyä asianmukaiset suojatoimet, joilla varmistetaan kyseessä olevien henkilöiden henkilötietojen suoja. Yleinen tietosuoja-asetus ei vaikuta näihin kansainvälisiin sopimuksiin.[715]

Jäsenvaltiot voivat myös tehdä kolmansien maiden tai kansainvälisten järjestöjen kanssa kansainvälisiä sopimuksia, joissa taataan yksityishenkilöiden perusoikeuksien ja -vapauksien asianmukainen suojataso, mikäli sopimukset eivät vaikuta yleisen tietosuoja-asetuksen soveltamiseen.

Samanlaisesta säännöstä määrätään uudistetun yleissopimuksen 108 12 artiklan 3 kohdan a alakohdassa.

Henkilötietojen siirtoa sisältäviä kansainvälisiä sopimuksia ovat esimerkiksi sopimukset matkustajarekistereistä.

Matkustajarekisterit

Lentoliikenteen harjoittajat keräävät varausprosessin yhteydessä matkustajarekisteritietoja (engl. Passenger Name Records, PNR), joihin kuuluvat nimet, osoitteet,

714 Uudistettu yleissopimus 108, 14 artiklan 4 kohta.

715 Yleinen tietosuoja-asetus, johdanto-osan 102 kappale.

luottokorttitiedot ja matkustajien istuinpaikat. Lentoliikenteen harjoittajat keräävät näitä tietoja myös omia kaupallisia tarkoituksiaan varten. EU on tehnyt sopimuksia tiettyjen kolmansien maiden (Australian, Kanadan ja Yhdysvaltojen) kanssa matkustajarekisteritietojen siirtämisestä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten. Unioni antoi myös vuonna 2016 direktiivin (EU) 2016/681 – joka tunnetaan EU:n PNR-direktiivinä[716]. Tämä direktiivi tarjoaa EU:n jäsenvaltioille oikeudellisen kehyksen matkustajarekisteritietojen siirtämiseksi muiden kolmansien maiden toimivaltaisille viranomaisille samoin terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten. Matkustajarekisteritietojen siirrot kolmansien maiden viranomaisille tehdään tapauskohtaisesti, ja niissä on arvioitava yksittäin, onko siirto tarpeen direktiivissä yksilöityä tarkoitusta varten, sekä taattava perusoikeuksien kunnioittaminen.

EU:n ja kolmansien maiden välillä matkustajarekisteritiedoista tehtyjen sopimusten yhteensopivuus EU:n perusoikeuskirjassa vahvistettujen yksityisyyden suojaa ja tietosuojaa koskevien perusoikeuksien kanssa on riitautettu. Kun EU allekirjoitti Kanadan kanssa käytyjen neuvottelujen jälkeen sopimuksen matkustajarekisteritietojen siirtämisestä ja käsittelystä vuonna 2014, Euroopan parlamentti päätti viedä asian Euroopan unionin tuomioistuimen käsiteltäväksi, jotta se arvioisi, onko sopimus laillinen EU:n oikeuden, erityisesti perusoikeuskirjan 7 ja 8 artiklan, kanssa.

Esimerkki: Lausunnossaan EU:n ja Kanadan PNR-tietoja koskevan sopimuksen lainmukaisuudesta[717] Euroopan unionin tuomioistuin totesi, että nykyisessä muodossaan suunniteltu sopimus oli yhteensopimaton perusoikeuskirjassa tunnustettujen perusoikeuksien kanssa eikä sitä siksi voitu tehdä. Koska siihen kuului henkilötietojen käsittelyä, se merkitsi puuttumista perusoikeuskirjan 8 artiklalla suojattuun henkilötietojen suojaa koskevaan oikeuteen. Samalla sillä rajoitetaan myös 7 artiklassa vahvistettua yksityis- ja perhe-elämän kunnioittamista koskevaa oikeutta, koska kokonaisuudessaan matkustajarekisteritiedot voivat yhdessä tarkasteltuina paljastaa koko matkareitin, matkustustottumuksia, eri henkilöiden välisiä suhteita sekä tietoja matkustajien taloudellisesta tilanteesta, heidän ravintotottumuksistaan tai heidän terveydentilastaan, ja vaikuttaa siten kielteisesti heidän yksityiselämäänsä.

716 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681, annettu 27 päivänä huhtikuuta 2016, matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten, EUVL 2016, L 119.

717 EUT, *unionin tuomioistuimen lausunto 1/15 (suuri jaosto)*, 26.7.2017.

Suunnitellussa sopimuksessa perusoikeuksiin puuttumista perusteltiin yleisen edun mukaisella tavoitteella eli yleisellä turvallisuudella sekä terrorismin ja vakavan kansainvälisen rikollisuuden torjumisella. Unionin tuomioistuin kuitenkin muistutti, että puuttumisen oikeutus edellyttää, että se rajoitetaan tavoitteen saavuttamisen kannalta täysin välttämättömään. Säännösten analysoinnin perusteella tuomioistuin katsoi, että suunniteltu sopimus ei täyttänyt ”täysin välttämättömän” kriteeriä. Johtopäätöksen aikaansaamiseksi tuomioistuin otti huomioon muun muassa seuraavat tekijät:

- Suunniteltuun sopimukseen sisältyi arkaluonteisten tietojen siirtämistä. Suunnitellun sopimuksen mukaisesti kerättäviin matkustajarekisteritietoihin voisi kuulua arkaluonteisia tietoja, kuten tietoja, joista ilmenee matkustajan rotu tai etninen alkuperä, uskonnollinen vakaumus tai terveydentila. Tietojen siirto Kanadan viranomaisille ja niiden suorittama käsittely voisivat vaarantaa syrjimättömyysperiaatteen ja edellyttäisivät siksi täsmällistä ja vahvaa oikeuttamisperustetta, joka olisi lähtöisin muista perusteista kuin yleisen turvallisuuden suojaamisesta ja vakavan rikollisuuden torjumisesta. Suunnitellussa sopimuksessa tällaista oikeuttamisperustetta ei ollut.[718]

- Lisäksi katsottiin, että kaikkien lentomatkustajien PNR-tietojen jatkuva säilytys viiden vuoden ajan heidän lähdettyään Kanadasta ylittää täysin välttämättömän rajat. Unionin tuomioistuin katsoi, että Kanadan viranomaiset voisivat säilyttää niiden matkustajien tiedot, jotka objektiivisten seikkojen perusteella voivat aiheuttaa uhan yleiselle turvallisuudelle, senkin jälkeen, kun kyseiset henkilöt ovat lähteneet Kanadasta. Sitä vastoin *kaikkien* matkustajien henkilötietojen säilyttäminen, kun heidän aiheuttamastaan riskistä yleiselle turvallisuudelle ei ole edes välillistä näyttöä, ei ole perusteltua.[719]

Uudistetun yleissopimuksen 108 neuvoa-antava komitea on antanut lausunnon PNR-sopimusten vaikutuksesta tietosuojaan Euroopan neuvoston oikeudessa[720].

718 *Ibid.*, 165 kohta.

719 *Ibid.*, 204–207 kohta.

720 Euroopan neuvosto, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19.8.2016.

Rahaliikenteen sanomanvälitystiedot

Belgiaan sijoittautunut Society for Worldwide Interbank Financial Telecommunication (SWIFT), joka hoitaa suurimman osan eurooppalaisten pankkien maailmanlaajuisista rahansiirroista, pitää yhtä tietojenkäsittelykeskusta Yhdysvalloissa, ja Yhdysvaltain valtiovarainministeriö pyysi sitä luovuttamaan tietoja terrorismin tutkintaa varten terrorismin rahoituksen jäljittämisohjelmassaan[721].

EU:n näkökulmasta näiden pohjimmiltaan eurooppalaisten tietojen luovuttamiselle ei ollut oikeudellista perustetta. Ne olivat saatavilla Yhdysvalloissa vain siksi, että yksi SWIFTin tietojenkäsittelykeskuksista sijaitsi Yhdysvalloissa.

EU ja Yhdysvallat tekivät vuonna 2010 erityisen sopimuksen, niin kutsutun SWIFT-sopimuksen, jolla luotiin tarvittava oikeudellinen peruste ja taattiin riittävä tietosuoja[722].

Tämän sopimuksen mukaan SWIFTin säilyttämiä rahataloudellisia tietoja luovutetaan myös jatkossa Yhdysvaltain valtiovarainministeriölle terrorismin tai terrorismin rahoituksen ennaltaehkäisyä, tutkintaa, paljastamista tai syytteeseenpanoa varten. Yhdysvaltain valtiovarainministeriö voi pyytää SWIFTiltä tietoja, kunhan pyyntö täyttää seuraavat vaatimukset:

- siinä yksilöidään mahdollisimman selvästi rahataloudelliset tiedot
- siinä perustellaan selkeästi tietojen tarpeellisuus
- se on rajattu mahdollisimman tarkasti pyydettävien tietojen määrän minimoimiseksi

721 Ks. tässä yhteydessä tietosuojatyöryhmä (2011), *lausunto 14/2011 rahanpesun ja terrorismin rahoituksen estämiseen liittyvistä tietosuojakysymyksistä*, WP 186, Bryssel, 13.6.2011; tietosuojatyöryhmä (2006), *lausunto 10/2006 henkilötietojen käsittelystä SWIFT-verkossa (Society for Worldwide Interbank Financial Telecommunication)*, WP 128, Bryssel, 22.11.2006; Belgian yksityiselämän suojaa käsittelevä komissio (*Commission de la protection de la vie privée*) (2008), *"Control and recommendation procedure initiated with respect to the company SWIFT scrl"*, päätös, 9.12.2008.

722 Neuvoston päätös 2010/412/EU, annettu 13 päivänä heinäkuuta 2010, terrorismin rahoituksen jäljittämisohjelmaa varten tapahtuvaa rahaliikenteen sanomanvälitystietojen käsittelyä ja siirtämistä Euroopan unionista Yhdysvaltoihin koskevan Euroopan unionin ja Amerikan yhdysvaltojen välisen sopimuksen tekemisestä, EUVL 2010, L 195, s. 3 ja 4. Sopimusteksti on tämän päätöksen liitteenä, EUVL 2010, L 195, s. 5–14.

- siinä ei pyydetä mitään yhtenäiseen euromaksualueeseen (SEPA) liittyviä tietoja.[723]

Europolin on saatava kopio Yhdysvaltain valtiovarainministeriön esittämästä pyynnöstä ja tarkistettava, onko SWIFT-sopimuksen periaatteita noudatettu[724]. Jos on, SWIFTin on toimitettava rahataloudelliset tiedot suoraan Yhdysvaltain valtiovarainministeriölle. Ministeriön on säilytettävä rahataloudellisia tietoja suojatussa fyysisessä ympäristössä, jossa niihin on pääsy vain terrorismia tai sen rahoitusta tutkivilla analyytikoilla. Rahataloudellisia tietoja ei myöskään saa liittää mihinkään muuhun tietokantaan. Yleisesti ottaen SWIFTin toimittamat tiedot on poistettava viimeistään viiden vuoden kuluttua niiden vastaanottamisesta. Yksittäisiä tutkinta- tai syytetoimia koskevia rahataloudellisia tietoja voidaan säilyttää vain niin kauan kuin niitä tarvitaan kyseisiä toimia varten.

Yhdysvaltain valtiovarainministeriö voi siirtää SWIFTiltä saamiaan tietoja Yhdysvalloissa tai sen ulkopuolella toimiville lainvalvonnasta, yleisestä turvallisuudesta tai terrorismin torjunnasta vastaaville viranomaisille yksinomaan terrorismin tai sen rahoituksen tutkintaa, paljastamista, ennaltaehkäisyä tai syytteeseenpanoa varten. Jos edelleen siirrettävät rahataloudelliset tiedot koskevat jonkin EU:n jäsenvaltion kansalaista tai asukasta, tietoja voidaan jakaa kolmannen maan viranomaisille ainoastaan kyseisen jäsenvaltion viranomaisen etukäteen antamalla suostumuksella. Edellä esitetystä voidaan poiketa, jos tietojen jakaminen on välttämätöntä yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhan vuoksi.

Riippumattomat valvojat, mukaan lukien Euroopan komission nimittämä henkilö, seuraavat SWIFT-sopimuksen periaatteiden noudattamista. Heillä on mahdollisuus tarkastella reaaliajassa ja takautuvasti kaikkia annetuista tiedoista tehtyjä hakuja, pyytää lisätietoja, joilla osoitetaan näiden hakujen yhteys terrorismiin, sekä valtuudet estää mikä tahansa haku tai kaikki haut, jotka vaikuttavat rikkovan sopimuksessa esitettyjä suojatoimia.

Rekisteröidyillä on oikeus saada toimivaltaiselta EU:n valvontaviranomaiselta vahvistus siitä, onko heidän henkilötietojen suojaa koskevia oikeuksiaan kunnioitettu. Rekisteröidyillä on myös oikeus saada Yhdysvaltain valtiovarainministeriön SWIFT-sopimuksen nojalla keräämät ja säilyttämät henkilötietonsa oikaistuiksi, poistetuiksi tai suojatuiksi. Rekisteröityjen tiedonsaantioikeuteen voidaan kuitenkin

723 *Ibid.*, 4 artiklan 2 kohta.

724 Europolin yhteisen valvontaviranomaisen tarkastuksissa on käsitelty Europolin toimintaa tällä alalla.

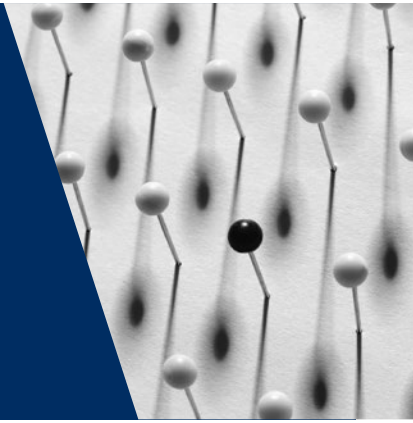
soveltaa tiettyjä oikeudellisia rajoituksia. Jos henkilötietojen antaminen evätään, rekisteröidylle on annettava kirjallinen selvitys epäämisestä ja kerrottava Yhdysvalloissa käytettävissä olevista hallinnollisista ja oikeudellisista oikeussuojakeinoista.

SWIFT-sopimus on voimassa viisi vuotta, ja sen ensimmäinen voimassaolojakso kesti elokuuhun 2015 asti. Sen voimassaoloa jatketaan ilman eri toimenpiteitä aina yhdellä vuodella kerrallaan, jollei jompikumpi osapuoli ilmoita toiselle osapuolelle ainakin kuusi kuukautta etukäteen aikomuksestaan olla jatkamatta sopimusta. Automaattista jatkamista on sovellettu elokuussa 2015, 2016 ja 2017, joten SWIFT-sopimuksen voimassaolo on varmistettu ainakin elokuuhun 2018 asti.[725]

725 *Ibid.*; 23 artiklan 2 kohta.

8

Tietosuoja poliisi- ja rikosasioissa



EU	Käsiteltävät asiat	EN
Poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi	**Yleisesti**	Uudistettu yleissopimus 108
	Poliisiasiat	Poliisiasioita koskeva suositus Käytännön opas henkilötietojen käytöstä poliisialalla
	Valvonta	EIT, *B.B. v. Ranska*, nro 5335/06, 2009 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 2008 EIT, *Allan v. Yhdistynyt kuningaskunta*, nro 48539/99, 2002 EIT, *Malone v. Yhdistynyt kuningaskunta*, nro 8691/79, 1984 EIT, *Klass ym. v. Saksa*, nro 5029/71, 1978 EIT, *Szabó ja Vissy v. Unkari*, nro 37138/14, 2016 EIT, *Vetter v. Ranska*, nro 59842/00, 2005
	Verkkorikollisuus	Tietoverkkorikollisuutta koskeva yleissopimus

EU	Käsiteltävät asiat	EN
Muut erityiset oikeudelliset välineet		
Prüm-päätös	**Erityiset henkilötiedot: sormenjäljet, dna, huliganismi, lentomatkustajien tiedot, televiestintätiedot jne.**	Uudistettu yleissopimus 108, 6 artikla Poliisiasioita koskeva suositus, käytännön opas henkilötietojen käytöstä poliisialalla
Ruotsin aloite (neuvoston puitepäätös 2006/960/YOS)	**Euroopan unionin jäsenvaltioiden lainvalvonta-viranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta**	EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 2008
Direktiivi (EU) 2016/681 matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland* ja *Kärntner Landesregierung ym.* [suuri jaosto], 2014 EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige ja Home Department vastaan Tom Watson ym.* [suuri jaosto], 2016	**Henkilötietojen säilyttäminen**	EIT, *B.B. v. Ranska*, nro 5335/06, 2009
Europol-asetus Eurojust-päätös	**Erityisvirastot**	Poliisiasioita koskeva suositus
Schengen II -päätös VIS-asetus Eurodac-asetus TTJ-päätös	**Erityiset yhteiset tietojärjestelmät**	Poliisiasioita koskeva suositus EIT, *Dalea v. Ranska*, nro 964/07, 2010

Euroopan neuvosto ja EU ovat panneet täytäntöön erityisiä oikeudellisia instrumentteja, joilla saatetaan tasapainoon yksilöiden tietosuojaan liittyvät edut ja yhteiskunnan edut, jotka liittyvät tietojen keräämiseen rikosten torjumiseksi sekä kansallisen

ja yleisen turvallisuuden varmistamiseksi. Tässä kohdassa tehdään yleiskatsaus Euroopan neuvoston oikeuteen (8.1 kohta) ja EU:n oikeuteen (8.2 kohta), jotka liittyvät tietosuojaan poliisi- ja rikosasioissa.

8.1 Tietosuojaa ja kansallista turvallisuutta poliisi- ja rikosasioissa käsittelevä Euroopan neuvoston oikeus

Keskeiset kohdat

- Uudistettu yleissopimus 108 ja Euroopan neuvoston poliisiasioita koskeva suositus kattavat tietosuojan kaikilla poliisityön alueilla.
- Tietoverkkorikollisuutta koskeva yleissopimus (Budapestin yleissopimus) on velvoittava kansainvälinen oikeudellinen asiakirja, joka koskee sähköisiä verkkoja vastaan ja niiden kautta tehtyjä rikoksia. Se on merkityksellinen myös sellaisten muiden kuin tietoverkkorikosten tutkinnassa, joihin liittyy sähköistä näyttöä.

Yksi tärkeä ero Euroopan neuvoston oikeuden ja EU:n oikeuden välillä on se, että **Euroopan neuvoston oikeutta** sovelletaan EU:n oikeudesta poiketen myös kansallisen turvallisuuden alaan. Tämä tarkoittaa, että sopimuspuolten on noudatettava ihmisoikeussopimuksen 8 artiklaa myös kansalliseen turvallisuuteen liittyvissä toimissa. Useat Euroopan ihmisoikeustuomioistuimen tuomiot koskevat valtion toimia kansallista turvallisuuslainsäädäntöä ja -käytäntöä koskevilla arkaluonteisilla aloilla[726].

Euroopan tasolla uudistettu yleissopimus 108 kattaa kaikki henkilötietojen käsittelyn alueet poliisi- ja rikosasioissa, ja sen määräyksillä on tarkoitus säännellä henkilötietojen käsittelyä yleisesti. Näin ollen uudistettua yleissopimusta 108 sovelletaan tietosuojaan poliisi- ja rikosasioissa. Geneettisten tietojen, rikoksiin, rikosoikeudenkäynteihin ja tuomioihin sekä kaikkiin niihin liittyviin turvatoimenpiteisiin liittyvien henkilötietojen, henkilön yksiselitteisesti yksilöivien biometristen tietojen sekä kaikkien arkaluonteisten henkilötietojen käsittely on sallittua vain, kun käytössä on asianmukaiset suojatoimet sellaisten riskien torjumiseksi, joita kyseisten tietojen

726 Ks. esim., EIT, *Klass ym. v. Saksa*, nro 5029/71, 6.9.1978; EIT, *Rotaru v. Romania* [suuri jaosto], nro 28341/95, 4.5.2000 ja EIT, *Szabó ja Vissy v. Unkari*, nro 37138/14, 12.1.2016.

käsittely voi aiheuttaa rekisteröidyn eduille, oikeuksille ja perusvapauksille. Tämä koskee erityisesti syrjinnän riskiä[727].

Poliisi- ja oikeusviranomaisten oikeudelliset tehtävät edellyttävät usein henkilötietojen käsittelyä, jolla saattaa olla vakavia seurauksia asianosaisille. Euroopan neuvoston vuonna 1987 hyväksymässä poliisiasioita koskevassa suosituksessa annetaan Euroopan neuvoston jäsenvaltioille ohjeita siitä, miten niiden tulisi panna yleissopimuksen 108 periaatteet täytäntöön poliisiviranomaisten suorittaman henkilötietojen käsittelyn yhteydessä[728]. Suositusta on täydennetty yleissopimuksen 108 neuvoa-antavan komitean laatimalla käytännön oppaalla henkilötietojen käytöstä poliisialalla[729].

Esimerkki: Asiassa *D.L. v. Bulgaria*[730] sosiaalipalvelut sijoittivat kantajan suljettuun kasvatuslaitokseen tuomioistuimen määräyksen nojalla. Laitoksessa valvottiin kaikkea kirjallista yhteydenpitoa ja puhelinkeskusteluja yleisesti ja valikoimattomasti. Euroopan ihmisoikeustuomioistuin katsoi, että 8 artiklaa rikottiin, koska kyseinen toimenpide ei ollut välttämätön demokraattisessa yhteiskunnassa. Tuomioistuin totesi, että on pyrittävä kaiken mahdollisin tavoin siihen, että laitokseen sijoitetuilla alaikäisillä olisi riittävät yhteydet ulkomaailmaan, koska se on olennainen osa heidän oikeuttaan ihmisarvoiseen kohteluun ja ehdottoman keskeistä heidän yhteiskuntakelpoisuudelleen. Tämä koski sekä vierailuja että kirjallista yhteydenpitoa tai puhelinkeskusteluja. Valvonnassa ei myöskään eroteltu viestintää perheenjäsenten tai lasten oikeuksia edustavien kansalaisjärjestöjen tai asianajajien kanssa. Päätös salakuunnella viestintää ei myöskään perustunut kunkin tietyn tapauksen riskien yksilölliseen analyysiin.

Esimerkki: Asiassa *Dragojević v. Kroatia*[731] kantajaa epäiltiin osallistumisesta huumekauppaan. Hänet todettiin syylliseksi, kun tutkintatuomari oli antanut luvan käyttää salaisia seurantatoimenpiteitä kantajan puhelujen salakuunteluun. Euroopan ihmisoikeustuomioistuin katsoi, että tämän kantelun

727 Uudistettu yleissopimus 108, 6 artikla.

728 Euroopan neuvosto, ministerineuvosto (1987), suositus Rec(87)15, poliisitoimen tietosuojaa koskeva suositus, 17.9.1987.

729 Euroopan neuvosto (2018), yleissopimuksen 108 neuvoa-antava komitea, Practical Guide on the use of personal data in the police sector, T-PD(2018)1.

730 EIT, *D.L. v. Bulgaria*, nro 7472/14, 19.5.2016.

731 EIT, *Dragojević v. Kroatia*, nro 68955/11, 15.1.2015.

kohteena ollut toimenpide merkitsi puuttumista yksityis- ja perhe-elämään ja kirjeenvaihtoon kohdistuvaa kunnioitusta koskevaan oikeuteen. Tutkintatuomarin antama lupa perustui ainoastaan syyttäjäviranomaisen lausuntoon, jonka mukaan tutkintaa ei voida tehdä muilla keinoin. Tuomioistuin pani myös merkille, että rikostuomioistuimet olivat rajoittaneet arviointiaan seurantatoimenpiteiden käytöstä ja että hallitus ei antanut käyttöön saatavilla olevia oikeussuojakeinoja. Näin ollen 8 artiklaa oli rikottu.

8.1.1 Poliisiasioita koskeva suositus

Euroopan ihmisoikeustuomioistuin on toistuvasti todennut, että poliisiviranomaiset ja kansalliset turvallisuusviranomaiset puuttuvat ihmisoikeussopimuksen 8 artiklan 1 kohdassa vahvistettuun oikeuteen, kun ne tallentavat ja säilyttävät henkilötietoja. Monessa ihmisoikeustuomioistuimen tuomiossa käsitellään tällaisen puuttumisen oikeutusta.[732]

Esimerkki: Asiassa *B.B. v. Ranska*[733] kantaja oli tuomittu vankeuteen alle 15-vuotiaisiin alaikäisiin kohdistuneista seksuaalirikoksista, joita hän oli tehnyt luottamusasemassa olevana henkilönä. Hän pääsi vankilasta vuonna 2000. Vuotta myöhemmin hän pyysi poistamaan maininnan vankeusrangaistuksesta rikosrekisteristään, mutta pyyntö evättiin. Vuonna 2004 Ranskan lainsäädännössä säädettiin seksuaalirikollisten kansallisen oikeudellisen tietokannan perustamisesta, ja kantajalle ilmoitettiin, että hänen tietonsa kirjattiin siihen. Euroopan ihmisoikeustuomioistuin päätti, että tuomitun seksuaalirikollisen tietojen kirjaaminen kansalliseen oikeudelliseen tietokantaan kuului ihmisoikeussopimuksen 8 artiklan soveltamisalaan. Kilpailevat yksilön ja yleiset edut oli kuitenkin pystytty saattamaan tasapainoon toteuttamalla riittävät tietosuojan suojatoimet, kuten rekisteröidyn oikeus pyytää tietojen poistamista, tietojen rajallinen säilytysaika ja tietoihin pääsyn rajaaminen. Tuomioistuin totesi, ettei ihmisoikeussopimuksen 8 artiklaa ollut rikottu.

732 Ks. esim., EIT, *Leander v. Ruotsi*, nro 9248/81, 26.3.1987; EIT, *M.M. v. Yhdistynyt kuningaskunta*, nro 24029/07, 13.11.2012; EIT, *M.K. v. Ranska*, nro 19522/09, 18.4.2013 tai EIT, *Aycaguer v. Ranska*, nro 8806/12, 22.6.2017.

733 EIT, *B.B. v. Ranska*, nro 5335/06, 17.12.2009.

Esimerkki: Asioissa *S. ja Marper v. Yhdistynyt kuningaskunta*[734] molemmat kantajat oli asetettu syytteeseen rikoksista, mutta heitä ei ollut tuomittu. Poliisi oli kuitenkin tallentanut ja säilyttänyt heidän sormenjälkensä, dna-tunnisteensa ja solunäytteensä. Säädöksen nojalla henkilön, jota epäiltiin rikoksesta, biometrisiä tietoja voitiin säilyttää rajattomasti, vaikka epäilty olisi myöhemmin julistettu syyttömäksi tai syytteistä olisi luovuttu. Euroopan ihmisoikeustuomioistuin katsoi, että yleinen ja valikoimaton henkilötietojen säilyttäminen ilman mitään aikarajaa siten, että syyttömiksi todetuilla henkilöillä oli vain rajoitettu mahdollisuus pyytää henkilötietojensa poistamista, muodosti suhteettoman puuttumisen kantajien oikeuteen nauttia yksityiselämän kunnioitusta. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Sähköisen viestinnän yhteydessä ratkaisevaa on viranomaisten puuttuminen yksityisyyden suojaa ja tietosuojaa koskeviin oikeuksiin. Viestinnän seuranta- tai kuuntelukeinot, kuten kuuntelu- tai salakuuntelulaitteet sallitaan vain, jos niistä on säädetty laissa ja jos ne ovat välttämättömiä demokraattisessa yhteiskunnassa seuraavien kannalta:

- valtion turvallisuuden suojelu
- yleinen turvallisuus
- valtion taloudelliset edut
- rikosten estäminen tai
- rekisteröidyn tai muiden henkilöiden oikeuksien ja vapauksien suojelu.

Useissa muissakin Euroopan ihmisoikeustuomioistuimen tuomioissa käsitellään mahdollisuutta puuttua yksityisyyden suojaa koskevaan oikeuteen seurannan kautta.

734 EIT, *S. ja Marper v. Yhdistynyt kuningaskunta* [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008, 119 ja 125 kohta.

Esimerkki: Asiassa *Allan v. Yhdistynyt kuningaskunta*[735] viranomaiset olivat salaa tallentaneet vangin yksityisiä keskusteluja hänen ystävänsä kanssa vankilan vierailualueella ja toisen syytetyn kanssa vankilan sellissä. Ihmisoikeustuomioistuin katsoi, että äänen ja kuvan tallennuslaitteiden käyttö kantajan sellissä, vankilan vierailualueella ja toisen vangin päällä rikkoi kantajan oikeutta nauttia yksityiselämän kunnioitusta. Koska millään lakiperusteisella järjestelmällä ei tuolloin säännelty poliisin mahdollisuutta käyttää salaisia tallennuslaitteita, kyseinen oikeuteen puuttuminen ei ollut lainmukaista. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Roman Zakharov v. Venäjä*[736] kantaja aloitti oikeusmenettelyn kolmea mobiiliverkko-operaattoria vastaan. Hän väitti, että hänen oikeuttaan puhelinviestinnän yksityisyyteen oli loukattu, koska operaattorit olivat asentaneet laitteita, joilla liittovaltion turvallisuuspalvelu pystyi salakuuntelemaan hänen puheluitaan ilman oikeuden etukäteen antamaa lupaa. Euroopan ihmisoikeustuomioistuin katsoi, että viestinnän salakuuntelua koskevilla kansallisilla säännöksillä ei annettu asianmukaisia ja tehokkaita takeita mielivaltaisuutta ja hyväksikäytön riskiä vastaan. Kansallisessa lainsäädännössä ei etenkään vaadittu tallennettujen tietojen poistamista sen jälkeen, kun säilyttämisen tavoite oli saavutettu. Lisäksi tuomioistuimen harjoittama valvonta oli rajallista, vaikka tuomioistuimen lupaa edellytettiin.

Esimerkki: Asiassa *Szabó ja Vissy v. Unkari*[737] kantajat väittivät, että Unkarin lainsäädäntö rikkoi Euroopan ihmisoikeussopimuksen 8 artiklaa, koska se ei ollut riittävän yksityiskohtainen tai täsmällinen. Lisäksi he väittivät, että lainsäädäntö ei tarjonnut riittäviä takeita hyväksikäytöltä ja mielivaltaisuudelta. Euroopan ihmisoikeustuomioistuin totesi, että Unkarin lainsäädännössä seurannalta ei edellytetty tuomioistuimen lupaa. Tuomioistuin pani kuitenkin merkille, että vaikka seurantaan tarvittiin oikeusministeriön lupa, tämä valvonta oli ilmeisen poliittista eikä sillä pystytty varmistamaan vaadittua arviointia ”ehdottoman välttämättömästä”. Kansallisessa lainsäädännössä ei myöskään säädetty tuomioistuinvalvonnasta, koska kohteille ei lähetettäisi ilmoitusta. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

735 EIT, *Allan v. Yhdistynyt kuningaskunta*, nro 48539/99, 5.11.2002.

736 EIT, *Roman Zakharov v. Venäjä* [suuri jaosto], nro 47143/06, 4.12.2015.

737 EIT, *Szabó ja Vissy v. Unkari*, nro 37138/14, 12.1.2016.

Koska poliisiviranomaisten suorittamalla henkilötietojen käsittelyllä voi olla merkittäviä seurauksia asianosaisille, ovat yksityiskohtaiset tietosuojasäännöt tietokantojen pitämiselle tällä alalla erityisen tarpeellisia. Euroopan neuvoston poliisiasioita koskevassa suosituksessa pyrittiin käsittelemään tätä näkökohtaa antamalla ohjeita siitä, miten tietoja tulisi kerätä poliisityötä varten; miten tiedostoja tulisi säilyttää tällä alalla; kenelle tulisi antaa pääsy näihin tiedostoihin, mukaan lukien edellytykset tietojen luovuttamiselle muiden maiden poliisiviranomaisille; miten rekisteröityjen tulisi voida käyttää tietosuojaoikeuksiaan; ja miten riippumattomien viranomaisten suorittama valvonta tulisi panna täytäntöön. Myös velvollisuutta turvata riittävä tietoturva käsiteltiin.

Suosituksessa ei sallita poliisiviranomaisten kerätä rajoittamattomasti kaikenlaisia tietoja. Poliisiviranomaisten oikeus kerätä henkilötietoja on rajoitettu siihen, mikä on tarpeellista todellisen vaaran ehkäisemiseksi tai erityiseen rikokseen liittyviä syytetoimia varten. Kaiken muun tietojen keruun on perustuttava erityiseen kansalliseen lainsäädäntöön. Arkaluonteisia henkilötietoja tulisi käsitellä vain siinä määrin kuin se on ehdottoman välttämätöntä tietyn tutkinnan yhteydessä.

Jos henkilötietoja kerätään rekisteröidyn tietämättä, rekisteröidylle tulisi kertoa tiedonkeruusta heti, kun asian paljastaminen ei enää haittaa tutkintaa. Myös teknisellä tarkkailulla tai muuten automatisoidusti tapahtuvan tietojen keräämisen tulisi perustua erityisiin säännöksiin.

Esimerkki: Asiassa *Versini-Campinchi ja Crasnianski v. Ranska*[738] kantaja oli asianajaja, joka puhui puhelimessa asiakkaan kanssa, kun tämän puhelinlinjaa salakuunneltiin tutkintatuomarin pyynnöstä. Puhtaaksikirjoitetusta keskustelusta kävi ilmi, että hän oli paljastanut asianajosalaisuuden piiriin kuuluvia tietoja. Syyttäjä lähetti nämä tiedot asianajajaliittoon, joka määräsi kantajalle rangaistuksen. Euroopan ihmisoikeustuomioistuin tunnusti, että asiassa puututtiin sekä henkilön, jonka puhelinta salakuunneltiin, että kantajan, jonka viestintää oli salakuunneltu ja myöhemmin kirjoitettu puhtaaksi, yksityis- ja perhe-elämään ja kirjeenvaihtoon kohdistuvaa kunnioitusta koskevaan oikeuteen. Puuttuminen oli tehty lain mukaan ja sen laillisena tavoitteena oli epäjärjestyksen estäminen. Kantaja oli pyytänyt tarkistamaan puhtaaksikirjoitettujen puhelimen kuuntelutietojen toimittamisen lainmukaisuuden häntä koskeneissa kurinpitomenettelyissä. Vaikka kanteella ei ollut pystytty mitätöimään puhtaaksikirjoitettua puhelinkeskustelua, Euroopan

738 EIT, *Versini-Campinchi ja Crasnianski v. Ranska*, nro 49176/11, 16.6.2016.

ihmisoikeustuomioistuin katsoi, että tehokkaalla valvonnalla oli pystytty rajoittamaan kantelun kohteena ollut puuttuminen demokraattisessa yhteiskunnassa välttämättömään. Tuomioistuin katsoi, että väite, jonka mukaan mahdollisuus rikosoikeudenkäyntiin asianajajaa vastaan puhtaaksikirjoitetun keskustelun perusteella voisi heikentää asianajajan ja hänen asiakkaansa välisen viestinnän vapautta ja siten asiakkaan oikeutta puolustukseen, ei ollut uskottava, kun itse asianajajan tekemä tietojen luovuttaminen saattoi olla häneltä lainvastaista käytöstä. Tuomioistuin totesi siksi, että 8 artiklaa ei ollut rikottu.

Euroopan neuvoston poliisiasioita koskevassa suosituksessa todetaan, että henkilötietoja säilytettäessä on erotettava seuraavat tietoryhmät selkeästi toisistaan: hallinnolliset tiedot ja poliisitiedot; erilaisten rekisteröityjen, kuten epäiltyjen, tuomittujen, uhrien ja todistajien henkilötiedot; sekä tosiseikat ja epäilyt tai olettamukset.

Poliisitietojen käyttötarkoituksen tulisi olla tarkkaan rajattu. Tämä asia vaikuttaa poliisitietojen luovuttamiseen kolmansille osapuolille: henkilötietojen siirtämistä tai luovuttamista poliisialalla tulisi säännellä sen pohjalta, liittyykö tietojen jakamiseen oikeutettua etua. Henkilötietojen siirtäminen tai luovuttaminen poliisialan ulkopuolelle tulisi sallia vain, kun siihen on selkeä laillinen velvollisuus tai lupa.

Esimerkki: Asiassa *Karabeyoğlu v. Turkki*[739] kantaja oli tuomari, jonka puhelinlinjoja seurattiin rikostutkinnassa laittomasta järjestöstä, johon hänen epäiltiin kuuluvan tai jota hänen ajateltiin auttavan ja tukevan. Syyttämättäjättämispäätöksen jälkeen rikostutkinnasta vastaava yleinen syyttäjä tuhosi kyseiset tallenteet. Niistä oli kuitenkin jäänyt jäljennös esitutkintaviranomaisille, jotka käyttivät sitten asianomaista aineistoa kantajaa koskevassa kurinpitotutkimuksessa. Euroopan ihmisoikeustuomioistuin katsoi, että asiaankuuluvaa lainsäädäntöä oli rikottu, koska tietoja oli käytetty muuhun tarkoitukseen kuin mihin ne oli kerätty, eikä niitä ollut tuhottu lakisääteisessä määräajassa. Puuttuminen kantajan yksityis- ja perhe-elämän kunnioitusta koskevaan oikeuteen ei ollut lainmukaista kurinpitomenettelyjen osalta.

Tietoja tulisi voida siirtää tai luovuttaa rajojen yli vain muiden maiden poliisiviranomaisille ja erityisten säännösten, mahdollisesti kansainvälisten sopimusten,

739 EIT, *Karabeyoğlu v. Turkki*, nro 30083/10, 7.6.2016.

nojalla, ellei tietojen luovuttaminen ole välttämätöntä vakavan ja välittömän vaaran torjumiseksi.

Riippumattoman valvojan on varmistettava, että poliisi noudattaa tietojen käsittelyssä kansallista tietosuojalainsäädäntöä. Rekisteröidyillä on oltava kaikki uudistetussa yleissopimuksessa 108 taatut tiedonsaantioikeudet. Jos rekisteröityjen tiedonsaantioikeuksia on rajoitettu yleissopimuksen 108 9 artiklan nojalla tehokkaiden poliisitutkintojen turvaamiseksi ja rikosoikeudellisten seuraamusten täytäntöön panemiseksi, rekisteröidyille on annettava kansallisessa lainsäädännössä mahdollisuus valittaa kansalliselle tietosuojaviranomaiselle tai muulle riippumattomalle elimelle.

8.1.2 Tietoverkkorikollisuutta koskeva Budapestin yleissopimus

Rikollisen toiminnan välineenä ja kohteena ovat yhä useammin sähköiset tietojenkäsittelyjärjestelmät, ja siksi tämän haasteen käsittelemiseksi tarvitaan uusia rikosoikeudellisia säännöksiä. Euroopan neuvosto onkin laatinut kansainvälisen oikeudellisen instrumentin, tietoverkkorikollisuutta koskevan yleissopimuksen – eli niin kutsutun Budapestin yleissopimuksen[740] – jolla puututaan sähköisiä verkkoja vastaan ja niiden kautta tehtyihin rikoksiin. Yleissopimukseen voivat liittyä myös muut kuin Euroopan neuvoston jäsenmaat. Vuoden 2018 alussa 14 Euroopan neuvoston ulkopuolista maata[741] oli liittynyt yleissopimukseen ja seitsemän muuta Euroopan neuvoston ulkopuolista maata saanut kutsun liittyä siihen.

Tietoverkkorikollisuutta koskeva yleissopimus on edelleen vaikutusvaltaisin kansainvälinen sopimus, jossa käsitellään internetin tai muun tietoverkon kautta tehtäviä rikoksia. Siinä vaaditaan sopimuspuolia ajantasaistamaan ja yhdenmukaistamaan rikoslainsäädäntöään seuraavilla aloilla: tietomurrot ja muut turvallisuusrikkomukset, mukaan lukien tekijänoikeusrikokset, tietokoneavusteiset petokset, lapsipornografia ja muut laittomat tietoverkkotoiminnat. Yleissopimuksessa määrätään myös valtuuksista suorittaa tietoverkkoihin kohdistuvia etsintöjä ja telepakkokeinoja tietoverkkorikollisuuden torjumisen yhteydessä. Se myös mahdollistaa

740 Euroopan neuvosto, ministerikomitea (2001), tietoverkkorikollisuutta koskeva yleissopimus, CETS nro 185, Budapest, 23.11.2001. Yleissopimus tuli voimaan 1.7.2004.

741 Australia, Chile, Dominikaaninen tasavalta, Israel, Japani, Kanada, Kolumbia, Mauritius, Panama, Senegal, Sri Lanka, Tonga, Tunisia ja Yhdysvallat. Ks. (englanniksi) luettelo yleissopimuksen 185 allekirjoituksista ja ratifioinneista, tilanne heinäkuussa 2017.

tehokkaan kansainvälisen yhteistyön. Yleissopimuksen lisäpöytäkirjassa käsitellään tietojärjestelmien välityksellä tehtyjen luonteeltaan rasististen ja muukalaisvihamielisten tekojen kriminalisointia.

Vaikka yleissopimus ei ole varsinaisesti tarkoitettu tietosuojan edistämiseen, sillä tehdään rangaistavaksi toimintoja, jotka todennäköisesti rikkovat rekisteröityjen oikeutta henkilötietojensa suojaan. Siinä edellytetään lisäksi, että sopimuspuolet antavat säädöksiä, joiden nojalla niiden kansalliset viranomaiset voivat siepata liikenne- ja sisältötietoja[742]. Se myös velvoittaa sopimuspuolet varmistamaan yleissopimuksen täytäntöönpanon yhteydessä riittävän suojan ihmisoikeuksille ja vapauksille, mukaan lukien ihmisoikeussopimuksen nojalla taatut oikeudet, kuten tietosuojaoikeus[743]. Sopimuspuolten ei tarvitse liittyä yleissopimukseen 108 voidakseen liittyä tietoverkkorikollisuutta koskevaan Budapestin yleissopimukseen.

8.2 Tietosuojaa poliisi- ja rikosasioissa käsittelevä EU:n oikeus

Keskeiset kohdat

- EU:ssa tietosuojaa poliisi- ja rikosasioissa säännellään sekä jäsenvaltioiden poliisi- ja oikeusviranomaisten ja EU:n toimijoiden rajat ylittävän että kansallisen käsittelyn yhteydessä.
- Jäsenvaltioiden on saatettava ja poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi osaksi kansallista lainsäädäntöä.
- Tietosuojaa poliisi- ja lainvalvontaviranomaisten rajat ylittävässä yhteistyössä, erityisesti terrorismin ja rajat ylittävän rikollisuuden torjunnassa, säännellään erityisillä säädöksillä.
- Euroopan poliisivirastolla (Europol), Euroopan oikeudellisen yhteistyön yksiköllä (Eurojust) ja äskettäin perustetulla Euroopan syyttäjänvirastolla, jotka ovat rajat ylittävää lainvalvontaa tukevia ja edistäviä EU:n elimiä, on omat erityiset tietosuojasääntönsä.

742 Euroopan neuvosto, ministerikomitea (2001), tietoverkkorikollisuutta koskeva yleissopimus, CETS nro 185, Budapest, 23.11.2001, 20 ja 21 artikla.

743 *Ibid.*, 15 artiklan 1 kohta.

- Erityisiä tietosuojasääntöjä on laadittu myös toimivaltaisten poliisi- ja oikeusviranomaisten rajat ylittävään tiedonvaihtoon EU:ssa käytettäviä yhteisiä tietojärjestelmiä varten. Näistä huomionarvoisia ovat erityisesti Schengenin tietojärjestelmä (Schengen II), viisumitietojärjestelmä (VIS) ja Eurodac, keskitetty järjestelmä, johon on tallennettu sormenjälkitiedot kolmansien maiden kansalaisilta, jotka ovat hakeneet turvapaikkaa jossakin EU:n jäsenvaltiossa.
- EU:ssa päivitetään parhaillaan edellä mainittuja tietosuojasäännöksiä, jotta ne saadaan vastaamaan poliisi- ja rikosoikeusviranomaisia koskevaa tietosuojadirektiiviä.

8.2.1 Poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi

Luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta annetun direktiivin (EU) 2016/680 (poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi)[744] tavoitteena on suojata rikosoikeudellisia tarkoituksia varten kerättyjä ja käsiteltyjä henkilötietoja. Näitä tarkoituksia ovat muun muassa

- rikosten ennalta estäminen, tutkiminen, paljastaminen tai rikoksiin liittyvät syytetoimet tai rikosoikeudellisten seuraamusten täytäntöönpano, mukaan lukien yleiseen turvallisuuteen kohdistuvilta uhkilta suojelu ja tällaisten uhkien ehkäisy
- rikosoikeudellisen seuraamuksen täytäntöönpano
- tapaukset, joissa poliisi- tai muut lainvalvontaviranomaiset toimivat lain puolustamiseksi ja yleisen turvallisuuden ja yhteiskunnan perusoikeuksien turvaamiseksi uhilta, joissa voisi olla kyse rikoksesta, ja niiden ehkäisemiseksi.

Poliisi- ja rikosoikeusviranomaisia koskevalla tietosuojadirektiivillä suojellaan rikosoikeudenkäynneissä mukana olevia eri ryhmiin kuuluvia henkilöitä, kuten todistajia, tiedonantajia, uhreja, epäiltyjä ja avunantajia. Poliisi- ja oikeusviranomaisten

744 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/680, annettu 27 päivänä huhtikuuta 2016, luonnollisten henkilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten ennalta estämistä, tutkimista, paljastamista tai rikoksiin liittyviä syytetoimia tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta, EUVL L 119, 4.5.2016, s. 89 (poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi).

on noudatettava direktiivin säännöksiä aina, kun kyseisiä henkilötietoja käsitellään lainvalvontatarkoituksia varten sekä direktiivin henkilökohtaiseen että aineelliseen soveltamisalaan kuuluvilla aloilla[745].

Tietojen käyttö on tietyin edellytyksin kuitenkin sallittua myös eri tarkoitukseen. Tietojen käsittely muuhun lainvalvontatarkoitukseen kuin siihen, johon henkilötiedot kerättiin, on sallittua vain, jos käsittely on lainmukaista, tarpeellista ja oikeasuhteista unionin oikeuden tai jäsenvaltion lainsäädännön mukaisesti[746]. Muita tarkoituksia varten sovelletaan yleistä tietosuoja-asetusta. Toimivaltaisten viranomaisten erityisvelvollisuutena kanteluista johtuvien vastuiden selvittämisessä on huolehtia lokitiedoista ja tietojen jakamisen dokumentoinnista.

Poliisi- ja rikosoikeusalalla toimivia toimivaltaisia viranomaisia ovat viranomaiset tai muut elimet, joille on jäsenvaltion lainsäädännössä annettu tehtäväksi käyttää julkista valtaa tai valtuuksia[747], esimerkiksi yksityiset vankilat[748]. Direktiiviä sovelletaan tietojenkäsittelyyn kotimaassa sekä jäsenvaltioiden poliisi- ja oikeusviranomaisten väliseen rajat ylittävään käsittelyyn. Sitä sovelletaan myös toimivaltaisten viranomaisten kolmansiin maihin ja kansainvälisille järjestöille tekemiin kansainvälisiin siirtoihin.[749] Se ei koske kansallista turvallisuutta eikä unionin toimielinten, elinten ja laitosten suorittamaa henkilötietojen käsittelyä[750].

Direktiivi perustuu suurelta osin yleisen tietosuoja-asetuksen periaatteisiin ja määritelmiin, ja siinä otetaan huomioon poliisi- ja rikosoikeusalan erityisluonne. Valvontaa voivat suorittaa samat jäsenvaltioiden viranomaiset kuin yleisen tietosuoja-asetuksenkin mukaisesti. Tietosuojavastaavan nimittäminen ja tietosuojaa koskevan vaikutustenarvioinnin tekeminen on otettu direktiiviin poliisi- ja rikosoikeusviranomaisten uusina velvollisuuksina[751]. Vaikka nämä käsitteet perustuvat yleiseen

745 Poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivi, 2 artiklan 1 kohta.

746 *Ibid.*, 4 artiklan 2 kohta.

747 *Ibid.*, 3 artiklan 7 kohta.

748 Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille Euroopan unionin toiminnasta tehdyn sopimuksen 294 artiklan 6 kohdan mukaisesti neuvoston kannasta yksilöiden suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä rikosten torjumista, tutkimista, selvittämistä ja syytteeseenpanoa tai rikosoikeudellisten seuraamusten täytäntöönpanoa varten sekä näiden tietojen vapaasta liikkuvuudesta ja neuvoston puitepäätöksen 2008/977/YOS kumoamisesta annettavan Euroopan parlamentin ja neuvoston direktiivin hyväksymiseen, COM(2016) 213 final, Bryssel, 11.4.2016.

749 Poliisi- ja rikosoikeusviranomaisia koskeva tietosuojadirektiivi, V luku.

750 *Ibid.*, 2 artiklan 3 kohta.

751 *Ibid.*, tietosuojavastaava 32 artiklassa ja vaikutustenarviointi 27 artiklassa.

tietosuoja-asetukseen, direktiivissä käsitellään poliisi- ja rikosoikeusviranomaisten erityisluonnetta. Asetuksella säänneltyyn kaupallisessa tarkoituksessa tehtyyn tietojenkäsittelyyn verrattuna turvallisuuteen liittyvä käsittely voi vaatia hieman joustavuutta. Esimerkiksi yleistä tietosuoja-asetusta vastaavan suojan tason takaaminen rekisteröidyille tiedonsaantia tai henkilötietoihin pääsemistä tai niiden poistamista koskevien oikeuksien osalta voisi merkitä, että kaikki lainvalvontatarkoituksissa tehdyt seurantatoimet olisivat lainvalvonnan kannalta tehottomia. Direktiivi ei siksi sisällä läpinäkyvyyden periaatetta. Turvallisuuteen liittyvässä käsittelyssä on sovellettava joustavasti myös tietojen minimoinnin periaatetta, jonka mukaan henkilötiedot on rajoitettava käsittelyn tarkoitusten kannalta ehdottoman välttämättömään, ja käyttötarkoitussidonnaisuuden periaatetta, jonka mukaan tietoja on käsiteltävä tiettyjä yksiselitteisiä tarkoituksia varten. Toimivaltaisten viranomaisten tietyssä tapauksessa keräämät ja tallentamat tiedot voivat osoittautua erittäin hyödyllisiksi tulevien tapausten ratkaisemisessa.

Käsittelyyn liittyvät periaatteet

Poliisi- ja rikosoikeusviranomaisia koskevassa tietosuojadirektiivissä asetetaan tiettyjä keskeisiä suojatoimia henkilötietojen käytölle. Siinä yksilöidään myös kyseisten tietojen käsittelyä ohjaavat periaatteet. Jäsenvaltioiden on varmistettava, että

- henkilötietoja käsitellään lainmukaisesti ja asianmukaisesti
- henkilötiedot kerätään tiettyjä nimenomaisia ja laillisia tarkoituksia varten, eikä niitä käsitellä näiden tarkoitusten kanssa yhteensopimattomalla tavalla
- henkilötiedot ovat asianmukaisia ja olennaisia eivätkä ne ole liian laajoja niihin tarkoituksiin, joita varten niitä käsitellään
- henkilötiedot ovat täsmällisiä ja tarvittaessa päivitettyjä; on toteutettava kaikki kohtuulliset toimenpiteet sen varmistamiseksi, että käsittelyn tarkoituksiin nähden virheelliset tiedot poistetaan tai oikaistaan viipymättä
- henkilötiedot säilytetään muodossa, josta rekisteröity on tunnistettavissa ainoastaan niin kauan kuin on tarpeen henkilötietojen käsittelytarkoitusten toteuttamista varten
- henkilötietoja käsitellään tavalla, jolla varmistetaan henkilötietojen asianmukainen tietoturva muun muassa suojaamalla niitä luvattomalta ja laittomalta

käsittelyltä sekä vahingossa tapahtuvalta häviämiseltä, tuhoutumiselta tai vahingoittumiselta asianmukaisia teknisiä tai organisatorisia toimenpiteitä hyödyntäen[752].

Direktiivin mukaan käsittely on laillista ainoastaan siltä osin kuin se on tarpeen asiaankuuluvan tehtävän suorittamiseksi. Lisäksi toimivaltaisen viranomaisen pitäisi suorittaa se direktiivissä täsmennettyjen tavoitteiden saavuttamiseksi EU:n oikeuden tai jäsenvaltion lainsäädännön perusteella.[753] Tietoja ei saa säilyttää pidempään kuin on tarpeen ja ne on poistettava tai niiden säilyttämisen tarpeellisuus on tarkistettava säännöllisesti tietyissä määräajoissa. Vain toimivaltainen viranomainen voi käyttää niitä tarkoitukseen, jota varten tiedot kerättiin, välitettiin tai annettiin saataville.

Rekisteröidyn oikeudet

Direktiivissä säädetään myös rekisteröidyn oikeuksista. Niitä ovat seuraavat:

- Oikeus saada tietoa. Jäsenvaltioiden on velvoitettava rekisterinpitäjä antamaan rekisteröidyn saataville 1) rekisterinpitäjän henkilöllisyys ja yhteystiedot, 2) tietosuojavastaavan yhteystiedot, 3) henkilötietojen käsittelyn tarkoitukset, 4) tieto siitä, että rekisteröidyllä on oikeus tehdä valitus valvontaviranomaiselle, ja valvontaviranomaisen yhteystiedot ja 5) tieto oikeudesta saada pääsy häntä itseään koskeviin henkilötietoihin sekä oikeudesta oikaista henkilötiedot tai poistaa ne ja rajoittaa henkilötietojen käsittelyä[754]. Näiden yleisten tietovaatimusten lisäksi direktiivissä säädetään, että erityistapauksissa ja rekisteröidyn tietojen käyttämiseksi rekisterinpitäjien on annettava rekisteröidyille tietoa käsittelyn oikeusperusteesta ja henkilötietojen säilytysajasta. Jos henkilötietoja on määrä välittää muille vastaanottajille, myös kolmansissa maissa tai kansainvälisissä järjestöissä, rekisteröidyille on ilmoitettava kyseiset vastaanottajaryhmät. Rekisterinpitäjien on myös annettava mitä tahansa lisätietoja ottaen huomioon erityisolosuhteet, joissa tietoja käsitellään – esimerkiksi, kun henkilötietoja on kerätty peitetoimina suoritettavan tarkkailun aikana eli rekisteröidyn tietämättä. Näin rekisteröidylle taataan oikeudenmukainen käsittely.[755]

752 *Ibid.*, 4 artiklan 1 kohta.

753 *Ibid.*, 8 artikla.

754 *Ibid.*, 13 artiklan 1 kohta.

755 *Ibid.*, 13 artiklan 2 kohta.

- Oikeus saada pääsy henkilötietoihin. Jäsenvaltioiden on varmistettava, että rekisteröidyllä on oikeus saada tietää, käsitelläänkö hänen henkilötietojaan vai ei. Jos niitä käsitellään, rekisteröidyllä on oltava oikeus saada pääsy tiettyihin tietoihin, kuten tietoihin käsiteltävistä tietoryhmistä.[756] Tätä oikeutta voidaan kuitenkin rajoittaa – esimerkiksi, jotta vältetään tutkimusten tai rikoksiin liittyvien syytetoimien estäminen, tai yleisen turvallisuuden ja muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi[757].

- Oikeus henkilötietojen oikaisemiseen. Jäsenvaltioilla on velvollisuus varmistaa, että rekisteröity voi ilman aiheetonta viivytystä saada virheelliset henkilötiedot oikaistuiksi. Rekisteröidyllä on myös oikeus saada puutteelliset henkilötiedot täydennettyä.[758]

- Oikeus henkilötietojen poistamiseen sekä käsittelyn rajoittamiseen. Rekisterinpitäjän on joissakin tapauksissa poistettava henkilötiedot. Rekisteröidyllä on myös oikeus saada henkilötietonsa poistetuksi mutta vain, kun niitä käsitellään lainvastaisesti.[759] Tietyissä tilanteissa henkilötietojen käsittelyä voidaan rajoittaa tietojen poistamisen sijasta. Tämä voidaan tehdä tapauksissa, joissa 1) tietojen paikkansapitävyys on kiistetty mutta sitä ei voida todentaa, tai 2) henkilötietoja tarvitaan todistelua varten.[760]

Jos rekisterinpitäjä kieltäytyy oikaisemasta tai poistamasta henkilötietoja tai rajoittamasta tietojen käsittelyä, rekisteröidylle on ilmoitettava siitä kirjallisesti. Jäsenvaltiot voivat rajoittaa tätä tiedonsaantioikeutta muun muassa yleisen turvallisuuden tai muiden henkilöiden oikeuksien ja vapauksien suojelemiseksi samoista syistä kuin tietoihin pääsyä koskevaa oikeutta voidaan rajoittaa.[761]

Rekisteröidyllä on tavallisesti oikeus saada tietoa henkilötietojensa käsittelystä ja hänellä on oikeus saada pääsy tietoihinsa, saada tiedot oikaistuksi tai poistetuksi tai rajoittaa käsittelyä. Hän voi käyttää näitä oikeuksia suoraan rekisterinpitäjän kanssa. Varmuudeksi poliisi- ja rikosoikeusviranomaisia koskevassa tietosuojadirektiivissä sallitaan myös rekisteröityjen oikeuksien välillinen käyttö tietosuojan

756 *Ibid.*, 14 artikla.
757 *Ibid.*, 15 artikla.
758 *Ibid.*, 16 artiklan 1 kohta.
759 *Ibid.*, 16 artiklan 2 kohta.
760 *Ibid.*, 16 artiklan 3 kohta.
761 *Ibid.*, 16 artiklan 4 kohta.

valvontaviranomaisen välityksellä. Se tulee kyseeseen, kun rekisterinpitäjä rajoittaa rekisteröidyn oikeutta.[762] Direktiivin 17 artiklan mukaan jäsenvaltioiden on toteutettava toimenpiteitä, joilla varmistetaan, että rekisteröityjen oikeuksia voidaan käyttää myös niiden valvontaviranomaisen välityksellä. Siksi rekisterinpitäjän on ilmoitettava rekisteröidylle välillisen käytön mahdollisuudesta.

Rekisterinpitäjän ja henkilötietojen käsittelijän velvollisuudet

Poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin yhteydessä rekisterinpitäjät ovat toimivaltaisia viranomaisia tai muita elimiä, joille on annettu tehtäväksi hoitaa julkishallinnon tehtäviä tai käyttää julkista valtaa, ja ne määrittävät henkilötietojen käsittelyn tarkoitukset ja keinot. Direktiivissä säädetään rekisterinpitäjien useista velvollisuuksista, jotta voidaan varmistaa lainvalvontatarkoituksiin käsiteltävien henkilötietojen suojan korkea taso.

Toimivaltaisten viranomaisten on säilytettävä lokitietoja automaattisessa käsittelyjärjestelmässä suorittamistaan käsittelytoimista. Lokitietoja on säilytettävä ainakin tietojen keräämisestä, muuttamisesta, kyselystä, luovuttamisesta siirrot mukaan lukien, yhdistämisestä ja poistamisesta.[763] Direktiivissä säädetään, että kyselyjä ja luovutuksia koskevien lokitietojen avulla on pystyttävä toteamaan kyseisten toimien perusteet, toteutuspäivä ja -aika sekä mahdollisuuksien mukaan henkilötietoja hakeneen tai niitä luovuttaneen henkilön tiedot ja näiden henkilötietojen vastaanottajien henkilöllisyys. Lokitietoja on käytettävä ainoastaan käsittelyn lainmukaisuuden tarkistamiseen, omaehtoiseen valvontaan, henkilötietojen eheyden ja turvallisuuden varmistamiseen sekä rikosoikeudellisiin menettelyihin[764]. Rekisterinpitäjän ja henkilötietojen käsittelijän on pyynnöstä asetettava lokitiedot valvontaviranomaisen saataville.

Rekisterinpitäjien yleisenä velvollisuutena on toteuttaa erityisesti tarvittavat tekniset ja organisatoriset toimenpiteet sen varmistamiseksi ja osoittamiseksi, että käsittely tapahtuu direktiivin mukaisesti[765]. Näitä toimenpiteitä suunnitellessaan rekisterinpitäjien on otettava huomioon käsittelyn luonne, laajuus ja asiayhteys sekä etenkin yksilöiden oikeuksiin ja vapauksiin mahdollisesti kohdistuvat riskit. Rekisterinpitäjien olisi otettava käyttöön sisäisiä toimintamalleja ja toteutettava

762 *Ibid.*, 17 artikla.

763 *Ibid.*, 25 artiklan 1 kohta.

764 *Ibid.*, 25 artiklan 2 kohta.

765 *Ibid.*, 19 artikla.

toimenpiteitä, joilla helpotetaan tietosuojaperiaatteiden, erityisesti sisäänrakennetun ja oletusarvoisen tietosuojan periaatteen noudattamista[766]. Jos käsittely todennäköisesti aiheuttaa henkilön oikeuksien ja vapauksien kannalta korkean riskin – esimerkiksi uusien teknologioiden käytön vuoksi – rekisterinpitäjien on toteutettava ennen käsittelyä tietosuojaa koskeva vaikutustenarviointi[767]. Direktiivissä myös luetellaan toimenpiteitä, jotka rekisterinpitäjien on toteutettava käsittelyn turvallisuuden varmistamiseksi. Näiden toimenpiteiden tarkoituksena on muun muassa evätä asiattomilta pääsy rekisterinpitäjien käsittelemiin henkilötietoihin, varmistaa, että valtuutetut henkilöt pääsevät ainoastaan valtuutuksensa piiriin kuuluviin henkilötietoihin sekä varmistaa, että käsittelyjärjestelmä toimii ja että järjestelmän toimintahäiriö ei voi vahingoittaa tallennettuja henkilötietoja.[768] Jos henkilötietojen tietoturvaloukkaus tapahtuu, rekisterinpitäjien on ilmoitettava siitä valvontaviranomaiselle kolmen vuorokauden kuluessa ja kuvattava tietoturvaloukkauksen luonne, sen todennäköiset seuraukset, asianomaisten henkilötietotyyppien ryhmät sekä asianomaisten rekisteröityjen arvioitu lukumäärä. Henkilötietojen tietoturvaloukkauksesta on ilmoitettava myös rekisteröidylle ”ilman aiheetonta viivytystä”, jos tietoturvaloukkaus todennäköisesti aiheuttaa korkean riskin hänen oikeuksilleen ja vapauksilleen.[769]

Direktiiviin sisältyy tilivelvollisuuden periaate, jonka mukaan rekisterinpitäjien on toteutettava toimenpiteitä varmistaakseen periaatteen noudattamisen. Rekisterinpitäjien on ylläpidettävä selostetta kaikista niiden vastuulla olevien käsittelytoimien eri luokista. Direktiivin 24 artiklassa esitetään kyseisen selosteen sisältö yksityiskohtaisesti. Selosteet on pyydettäessä annettava valvontaviranomaisen saataville, jotta tämä voi valvoa rekisterinpitäjän käsittelytoimia. Toinen tärkeä osoitusvelvollisuutta edistävä toimenpide on tietosuojavastaavan nimittäminen. Rekisterinpitäjien on nimitettävä tietosuojavastaava, vaikka direktiivin mukaan jäsenvaltiot voivat vapauttaa tuomioistuimet ja muut riippumattomat oikeusviranomaiset tästä velvoitteesta.[770] Tietosuojavastaavan tehtävät muistuttavat yleisen tietosuoja-asetuksen mukaisia tehtäviä. Tietosuojavastaava valvoo direktiivin noudattamista ja antaa tietoja käsitteleville työntekijöille tietoja ja neuvoja, jotka koskevat heidän tietosuojasäännösten mukaisia velvollisuuksiaan. Tietosuojavastaava antaa myös

766 *Ibid.*, 20 artikla.

767 *Ibid.*, 27 artikla.

768 *Ibid.*, 29 artikla.

769 *Ibid.*, 30 ja 31 artikla.

770 *Ibid.*, 32 artikla.

neuvoja tietosuojaa koskevasta vaikutustenarvioinnista ja toimii valvontaviranomaisen yhteyspisteenä.

Siirrot kolmansiin maihin tai kansainvälisille järjestöille

Yleisen tietosuoja-asetuksen tapaan direktiivissä säädetään edellytyksistä henkilötietojen siirrolle kolmansiin maihin tai kansainvälisille järjestöille. Henkilötietojen vapaa siirtäminen EU:n oikeudenkäyttöalueen ulkopuolelle voisi vaarantaa EU:n oikeudessa taatut suojatoimet ja vahvan suojan. Itse edellytykset ovat kuitenkin melko erilaiset kuin yleisessä tietosuoja-asetuksessa. Henkilötietoja voidaan siirtää kolmansiin maihin tai kansainvälisille järjestöille, jos[771]

- siirto on tarpeen direktiivin tavoitteita varten
- henkilötiedot siirretään kolmanteen maahan tai kansainväliselle järjestölle rekisterinpitäjälle, joka on direktiivin mukaan toimivaltainen – vaikka tähän sääntöön on poikkeus yksittäis- ja erityistapauksissa[772]
- rajat ylittävän yhteistyön aikana saatujen henkilötietojen siirtäminen kolmansiin maihin tai kansainvälisille järjestöille edellyttää sen jäsenvaltion lupaa, josta tiedot ovat peräisin, vaikka tästä vaatimuksesta voidaan vapauttaa kiireellisissä tapauksissa
- komissio on hyväksynyt tietosuojan riittävyyttä koskevan päätöksen, asianmukaisista suojatoimista on säädetty tai sovelletaan erityistilanteita koskevia poikkeuksia
- henkilötietojen siirtäminen edelleen muuhun kolmanteen maahan tai muulle kansainväliselle järjestölle edellyttää, että alkuperäisen siirron toteuttanut toimivaltainen viranomainen antaa luvan edelleen siirtämiselle otettuaan asianmukaisesti huomioon muun muassa rikoksen vakavuuden ja henkilötietojen suojan tason maassa, johon tai jolle tiedot siirretään edelleen[773].

Direktiivin mukaan henkilötietoja voidaan siirtää, jos yksi kolmesta edellytyksestä täyttyy. Ensimmäinen edellytys on, että Euroopan komissio on antanut tietosuojan

771 *Ibid.*, 35 artikla.

772 *Ibid.*, 39 artikla.

773 *Ibid.*, 35 artiklan 1 kohta.

riittävyyttä koskevan päätöksen direktiivin mukaisesti. Päätös voi koskea kolmannen maan koko aluetta tai kolmannen maan tiettyjä sektoreita tai kansainvälistä järjestöä. Tämä voidaan kuitenkin tehdä vain, jos varmistetaan riittävä suojan taso ja direktiivissä määritetyt edellytykset täyttyvät[774]. Tällaisissa tapauksissa henkilötietojen siirrolle ei tarvita jäsenvaltion lupaa[775]. Komission on seurattava kehitystä, joka saattaa vaikuttaa tietosuojan riittävyyttä koskevien päätösten toimivuuteen. Päätökseen täytyy myös sisältyä säännöllisen tarkistuksen mekanismi. Komissio voi myös kumota päätöksen, muuttaa sitä tai keskeyttää sen soveltamisen, jos saatavilla olevista tiedoista ilmenee, että kolmannella maalla tai kansainvälisellä järjestöllä ei ole enää edellytyksiä tarjota riittävää tietosuojan tasoa. Siinä tapauksessa komission on aloitettava kolmannen maan tai kansainvälisen järjestön kanssa neuvottelut tilanteen korjaamiseksi.

Jos päätöstä tietosuojan riittävyydestä ei ole, siirrot voivat perustua asianmukaisiin suojatoimiin. Niistä voidaan määrätä oikeudellisesti sitovassa välineessä tai rekisterinpitäjä voi arvioida itse henkilötietojen siirtoon liittyvät seikat ja todeta, että asianmukaiset suojatoimet on toteutettu. Itsearvioinnissa olisi otettava huomioon Europolin tai Eurojustin ja kolmannen maan tai kansainvälisen järjestön välillä mahdollisesti tehdyt yhteistyösopimukset, salassapitovelvollisuuden olemassaolo ja tietty käsittelytarkoitus sekä varmistus siitä, että henkilötietoja ei käytetä kuolemanrangaistuksen tai minkään julman ja epäinhimillisen kohtelun toteuttamiseen.[776] Viimeksi mainitussa tapauksessa rekisterinpitäjän on ilmoitettava toimivaltaiselle valvontaviranomaiselle tähän ryhmään kuuluvien siirtojen sarjat[777].

Vaikka päätöstä tietosuojan riittävyydestä ei ole annettu eikä asianmukaisista suojatoimista ole säädetty, siirrot voidaan kuitenkin sallia direktiivissä tarkoitetuissa erityistilanteissa. Näitä tilanteita ovat muun muassa rekisteröidyn tai toisen henkilön elintärkeiden etujen suojaaminen ja jäsenvaltion tai kolmannen maan yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan ehkäiseminen.[778]

Yksittäis- ja eritystapauksissa toimivaltaiset viranomaiset voivat siirtää tietoja kolmansiin maihin sijoittautuneille vastaanottajille, jotka eivät ole toimivaltaisia viranomaisia, jos edellä kuvatuista kolmesta edellytyksestä yhden täyttämisen lisäksi

774 *Ibid.*, 36 artikla.

775 *Ibid.*, 36 artiklan 1 kohta.

776 *Ibid.*, johdanto-osan 71 kappale.

777 *Ibid.*, 37 artiklan 1 kohta.

778 *Ibid.*, 38 artiklan 1 kohta.

täytetään myös direktiivin 39 artiklassa esitetyt lisäedellytykset. Siirron on etenkin oltava ehdottoman välttämätön, jotta siirron toteuttava toimivaltainen viranomainen, joka vastaa myös sen määrittämisestä, että yksilöiden perusoikeudet ja -vapaudet eivät syrjäytä siirron oikeuttavaa yleistä etua, voi suorittaa tehtävänsä. Nämä siirrot on dokumentoitava, ja siirron toteuttavan toimivaltaisen viranomaisen on ilmoitettava niistä toimivaltaiselle valvontaviranomaiselle[779].

Direktiivissä vaaditaan kolmansien maiden ja kansainvälisten järjestöjen osalta lisäksi kehittämään kansainvälisiä yhteistyökeinoja, jotta voidaan edistää lainsäädännön tosiasiallista täytäntöönpanoa ja auttaa siten tietosuojan valvontaviranomaisia tekemään yhteistyötä muiden maiden valvontaviranomaisten kanssa[780].

Riippumaton valvonta ja rekisteröityjen oikeussuojakeinot

Kunkin jäsenvaltion on varmistettava, että vähintään yksi riippumaton kansallinen valvontaviranomainen vastaa direktiivin nojalla annettujen säännösten soveltamisen valvonnasta ja sitä koskevasta neuvonnasta[781]. Direktiiviä varten perustettava valvontaviranomainen voi olla sama kuin yleisen tietosuoja-asetuksen mukaan perustettu valvontaviranomainen, mutta jäsenvaltiot voivat halutessaan nimittää eri viranomaisen, mikäli se täyttää riippumattomuuskriteerit. Valvontaviranomaisten on myös käsiteltävä vaatimukset, joita kuka tahansa henkilö esittää oikeuksiensa ja vapauksiensa suojelusta toimivaltaisten viranomaisten suorittamassa henkilötietojen käsittelyssä.

Jos rekisteröidyn oikeuksien käyttö evätään pakottavista syistä, rekisteröidyllä on oltava oikeus hakea muutosta toimivaltaisesta valvontaviranomaisesta ja/tai tuomioistuimesta. Jos henkilölle aiheutuu vahinkoa direktiivin täytäntöön panevan kansallisen lainsäädännön rikkomisesta, hänellä on oikeus saada korvaus rekisterinpitäjältä tai muulta jäsenvaltion lainsäädännön mukaisesti toimivaltaiselta viranomaiselta[782]. Yleisesti ottaen rekisteröidyillä on oltava oikeus oikeussuojakeinoihin aina, kun rikotaan heidän oikeuksiaan, jotka on taattu direktiivin täytäntöön panevalla kansallisella lainsäädännöllä[783].

779 *Ibid.*, 37 artiklan 3 kohta.

780 *Ibid.*, 40 artikla.

781 *Ibid.*, 41 artikla.

782 *Ibid.*, 56 artikla.

783 *Ibid.*, 54 artikla.

8.3 Tietosuojaa koskevat muut erityiset oikeudelliset välineet lainvalvonta-asioissa

Poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin lisäksi jäsenvaltioiden hallussa olevien tietojen vaihtoa erityisillä aloilla säännellään useilla oikeudellisilla välineillä. Niitä ovat muun muassa neuvoston puitepäätös 2009/315/YOS jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä, neuvoston päätös 2000/642/YOS jäsenvaltioiden rahanpesun selvittelykeskusten välistä yhteistyötä koskevista järjestelyistä, joita noudatetaan tietojenvaihdossa, ja neuvoston 18 päivänä joulukuuta 2006 tehty puitepäätös 2006/960/YOS Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta.[784]

Merkittävää on, että toimivaltaisten viranomaisten väliseen rajatylittävään yhteistyöhön[785] kuuluu jatkuvasti enemmän tietojen vaihtoa maahanmuutosta. Tämän alan ei katsota kuuluvan poliisi- ja rikosoikeusasioihin, mutta se on monesti tärkeä poliisi- ja oikeusviranomaisten työssä. Sama pätee tietoihin EU:n tuoduista tai EU:sta viedyistä tavaroista. Sisärajatarkastusten poistaminen Schengen-alueen myötä on lisännyt petosriskiä. Jäsenvaltioiden on siksi pitänyt tehostaa yhteistyötä, erityisesti parantamalla rajatylittävää tiedonvaihtoa, jotta kansallisen ja EU:n tullilainsäädännön rikkomiset voidaan paljastaa ja jotta niistä voidaan asettaa syytteeseen entistä helpommin. Viime vuosina vakava ja järjestäytynyt rikollisuus ja terrorismi ovat lisäksi lisääntyneet maailmassa. Siihen voi liittyä matkustamista maasta toiseen ja se on osoittanut, että useissa tapauksissa poliisi- ja lainvalvontaviranomaisten rajat ylittävää yhteistyötä on lisättävä[786].

784 Euroopan unionin neuvosto (2009), neuvoston puitepäätös 2009/315/YOS, tehty 26 päivänä helmikuuta 2009, jäsenvaltioiden välisen rikosrekisteritietojen vaihdon järjestämisestä ja sisällöstä, EUVL 2009, L 93; Euroopan unionin neuvosto (2000), neuvoston päätös 2000/642/YOS, tehty 17 päivänä lokakuuta 2000, jäsenvaltioiden rahanpesun selvittelykeskusten välistä yhteistyötä koskevista järjestelyistä, joita noudatetaan tietojenvaihdossa, EYVL 2000, L 271; neuvoston puitepäätös 2006/960/YOS, tehty 18 päivänä joulukuuta 2006 , Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta, EUVL L 386.

785 Euroopan komissio (2012), *komission tiedonanto Euroopan parlamentille ja neuvostolle – Lainvalvontayhteistyön vahvistaminen EU:ssa: eurooppalainen tiedonvaihtomalli (EIXM)*, COM(2012) 735 final, Bryssel, 7.12.2012.

786 Ks. Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden ehkäisemistä, paljastamista, tutkimista ja syytteeseenpanoa varten, COM(2011) 32 final, Bryssel, 2.2.2011, s. 1.

Prüm-päätös

Merkittävä esimerkki virallisesta kansallisten tietojen vaihdon muodossa tapahtuvasta rajatylittävästä yhteistyöstä on neuvoston päätös 2008/615/YOS, sekä sen täytäntöönpanosäännökset päätöksessä 2008/615/YOS, rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi (Prüm-päätös), jolla Prümin sopimus sisällytettiin EU-oikeuteen vuonna 2008.[787] Prümin sopimus oli kansainvälistä poliisiyhteistyötä koskenut sopimus, jonka Alankomaat, Belgia, Espanja, Itävalta, Luxemburg, Ranska ja Saksa allekirjoittivat vuonna 2005[788].

Prüm-päätöksen tavoitteena on auttaa sen allekirjoittaneita jäsenvaltioita parantamaan tietojen jakamista rikollisuuden estämiseksi ja torjumiseksi kolmella alalla: terrorismissa, rajanylittävässä rikollisuudessa ja laittomassa muuttoliikkeessä. Siksi päätöksessä annetaan seuraavia aloja koskevia sääntöjä:

- Dna-tunnisteiden, sormenjälkitietojen ja tiettyjen kansallisten ajoneuvorekisteritietojen automatisoitu saatavuus
- tietojen toimittaminen sellaisten suurtapahtumien yhteydessä, joilla on rajat ylittäviä ulottuvuuksia
- terrorismirikosten estämiseen tarkoitettujen tietojen toimittaminen
- muut toimenpiteet, joilla tehostetaan rajat ylittävää poliisiyhteistyötä.

Prüm-päätöksen nojalla saataville annettaviin tietokantoihin sovelletaan kokonaisuudessaan kansallista lainsäädäntöä, mutta tietojenvaihtoon sovelletaan lisäksi tätä päätöstä, jonka yhteensopivuus poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin kanssa on arvioitava. Kyseisten tiedonsiirtojen valvonnasta vastaavia toimivaltaisia elimiä ovat kansalliset tietosuojan valvontaviranomaiset.

787 Euroopan unionin neuvosto (2008), neuvoston päätös 2008/615/YOS, tehty 23 päivänä kesäkuuta 2008, rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin ja rajatylittävän rikollisuuden torjumiseksi, EUVL 2008, L 210.

788 Belgian kuningaskunnan, Saksan liittotasavallan, Espanjan kuningaskunnan, Ranskan tasavallan, Luxemburgin suurherttuakunnan, Alankomaiden kuningaskunnan ja Itävallan tasavallan välillä rajatylittävän yhteistyön tehostamisesta erityisesti terrorismin, rajatylittävän rikollisuuden ja laittoman muuttoliikkeen torjumiseksi tehty sopimus.

Puitepäätös 2006/960/YOS – Ruotsin aloite

Puitepäätös 2006/960/YOS (Ruotsin aloite)[789] on toinen esimerkki lainvalvontaviranomaisten kansallisten tietojen vaihtamista koskevasta rajat ylittävästä yhteistyöstä. Ruotsin aloitteessa keskitytään erityisesti tiedustelutietojen ja tietojen vaihtoon, ja sen 8 artiklassa esitetään erityiset tietosuojasäännöt.

Tämän säädöksen mukaan tietojen ja tiedustelutietojen käyttöön on sovellettava vastaanottavan jäsenvaltion kansallisia tietosuojasäännöksiä niiden samojen sääntöjen mukaisesti, joita sovellettaisiin, jos ne olisi kerätty kyseisessä jäsenvaltiossa. Päätöksen 8 artiklassa mennään pidemmällä toteamalla, että toimittaessaan tietoja ja tiedustelutietoja toimivaltainen lainvalvontaviranomainen voi kansallisen lainsäädäntönsä mukaisesti asettaa tiedot vastaanottavalle toimivaltaiselle lainvalvontaviranomaiselle niiden käyttöä koskevia ehtoja. Näitä ehtoja voidaan soveltaa myös rikostutkinnan tai rikostiedusteluoperaation, jonka puitteissa tietojen ja tiedustelutietojen vaihto on tapahtunut, tuloksista raportointiin. Kun kuitenkin kansallisessa lainsäädännössä säädetään poikkeuksista käyttöä koskeviin rajoituksiin (esim. tuomioistuinten tai lainsäädäntöelinten osalta), tietoja ja tiedustelutietoja saa käyttää ainoastaan, kun tiedot toimittanutta jäsenvaltiota on ennalta kuultu.

Toimitettuja tietoja ja tiedustelutietoja voidaan käyttää

- niihin tarkoituksiin, joihin ne on toimitettu, tai
- yleiseen turvallisuuteen kohdistuvan välittömän ja vakavan uhkan estämiseksi.

Käsittely muihin tarkoituksiin voidaan sallia, mutta vain tiedot toimittaneen jäsenvaltion etukäteen antamalla luvalla.

Ruotsin aloitteessa todetaan lisäksi, että käsiteltäviä henkilötietoja on suojeltava kansainvälisten säädösten, kuten

- yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä tehdyn Euroopan neuvoston yleissopimuksen mukaisesti[790]

789 Euroopan unionin neuvosto (2006), neuvoston puitepäätös 2006/960/YOS, tehty 18 päivänä joulukuuta 2006, Euroopan unionin jäsenvaltioiden lainvalvontaviranomaisten välisen tietojen ja tiedustelutietojen vaihdon yksinkertaistamisesta, EUVL L 386/89, 29.12.2006.

790 Euroopan neuvosto (1981), yleissopimus yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, ETS nro 108.

- yleissopimukseen liitetyn valvontaviranomaisista ja tietojen siirroista eri maiden välillä 8 päivänä marraskuuta 2001 tehdyn lisäpöytäkirjan mukaisesti[791]

- Euroopan neuvoston henkilötietojen käyttöä poliisialalla sääntelevän suosituksen nro R(87) 15[792] mukaisesti.

EU:n PNR-direktiivi

Matkustajarekisteritiedot (PNR) ovat lentomatkustajia koskevia tietoja, joita liikenteenharjoittajat keräävät ja tallentavat varaus- ja lähtöselvitysjärjestelmiinsä omia kaupallisia tarkoituksiaan varten. Niihin kuuluu erityyppisiä tietoja, kuten matkustuspäivät, matkareitti, lipputiedot, yhteystiedot, tiedot matkatoimistosta, jonka kautta lento on varattu, maksutapa, paikkanumero ja matkatavaratiedot.[793] Matkustajarekisteritietojen käsittely voi auttaa lainvalvontaviranomaisia tunnistamaan tunnetut tai mahdolliset epäillyt ja tekemään arviointeja matkustusmallien ja muiden rikollisiin toimiin tavallisesti liittyvien indikaattorien perusteella. Matkustajarekisteritietoja analysoimalla voidaan myös jäljittää takautuvasti sellaisten henkilöiden matkareittejä, joiden epäillään osallistuneen rikollisiin toimiin. Sen avulla lainvalvontaviranomaiset voivat havaita rikollisverkostoja.[794] EU on tehnyt kolmansien maiden kanssa joitakin sopimuksia matkustajarekisteritietojen vaihtamisesta, kuten 7 kohdassa selitetään. Se on lisäksi ottanut käyttöön matkustajarekisteritietojen käsittelyn EU:ssa matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten annetun direktiivin 2016/681/EU (EU:n PNR-direktiivi)[795] nojalla. Direktiivissä säädetään lentoliikenteen harjoittajien velvollisuudesta toimittaa matkustajarekisteritiedot toimivaltaisille viranomaisille ja perustaa tiukat tietosuojaa koskevat suojatoimet kyseisten tietojen käsittelyä ja keräämistä varten. EU:n

791 Euroopan neuvosto (2001), valvontaviranomaisia ja maan rajan yli tapahtuvaa tietojen siirtoa koskeva lisäpöytäkirja yleissopimukseen yksilöiden suojelusta henkilötietojen automaattisessa tietojenkäsittelyssä, ETS nro 108.

792 Euroopan neuvosto (1987), ministerikomitean suositus nro. R (87) 15 jäsenvaltioille henkilötietojen käytön sääntelystä poliisialalla (hyväksytty ministerikomiteassa 17.9.1987 varaministerin 410. kokouksessa).

793 Euroopan komissio (2011), ehdotus Euroopan parlamentin ja neuvoston direktiiviksi matkustajarekisteritietojen käytöstä terrorismirikosten ja vakavan rikollisuuden ehkäisemistä, paljastamista, tutkimista ja syytteeseenpanoa varten, COM(2011) 32 final, Bryssel, 2.2.2011, s. 1.

794 Euroopan komissio (2015), tietokooste "Fact Sheet Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives", Bryssel, 11.1.2015.

795 Euroopan parlamentin ja neuvoston direktiivi (EU) 2016/681, annettu 27 päivänä huhtikuuta 2016, matkustajarekisteritietojen (PNR) käytöstä terrorismirikosten ja vakavan rikollisuuden ennalta estämistä, paljastamista ja tutkintaa sekä tällaisiin rikoksiin liittyviä syytetoimia varten, EUVL 2016, L 119, s. 132.

PNR-direktiiviä sovelletaan kansainvälisiin lentoihin EU:hun ja EU:sta mutta myös EU:n sisäisiin lentoihin, jos jäsenvaltio niin päättää.[796]

PNR-tiedot saavat sisältää vain EU:n PNR-direktiivissä sallitut tiedot. Ne on säilytettävä yhdessä tietoyksikössä, turvallisessa paikassa kussakin jäsenvaltiossa. PNR-tiedoista on erotettava tunnistamisen mahdollistavat tiedonosat kuusi kuukautta sen jälkeen, kun ne on saatu lentoliikenteen harjoittajalta, ja niitä saa säilyttää enintään viiden vuoden ajan[797]. PNR-tietoja vaihdetaan jäsenvaltioiden välillä, jäsenvaltioiden ja Europolin välillä ja vain tapauskohtaisesti kolmansien maiden kanssa.

PNR-tietojen siirtämisen ja käsittelyn ja rekisteröidyille taattujen oikeuksien on oltava poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin mukaisia, ja niissä on varmistettava perusoikeuskirjassa, uudistetussa yleissopimuksessa 108 ja Euroopan ihmisoikeussopimuksessa edellytetty yksityisyyden ja henkilötietojen suojan korkea taso.

Poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin mukaan toimivaltaiset riippumattomat kansalliset valvontaviranomaiset ovat vastuussa myös jäsenvaltioiden EU:n PNR-direktiivin nojalla antamien säännösten soveltamisen seurannasta ja sitä koskevasta neuvonnasta.

Televiestintätietojen säilyttäminen

Tietojen säilyttämistä koskeva direktiivi[798] – joka todettiin pätemättömäksi 8. huhtikuuta 2014 asiassa *Digital Rights Ireland* – velvoitti viestintäpalvelujen tarjoajat pitämään metatiedot saatavilla vakavan rikollisuuden torjuntaa koskevaa erityistarkoitusta varten vähintään kuusi mutta enintään 24 kuukautta riippumatta siitä, tarvitsiko palveluntarjoaja kyseisiä tietoja vielä laskutusta tai palvelujen teknistä tarjoamista varten.

796 PNR-direktiivi, L 119, s. 132, 1 artiklan 1 kohta ja 2 artiklan 1 kohta.

797 *Ibid.*, 12 artiklan 1 ja 2 kohta.

798 Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL 2006, L 105.

Televiestintätietojen säilyttäminen tarkoittaa selvästi puuttumista asianosaisten henkilöiden yksityisyyden suojaan[799]. Tämän puuttumisen oikeutus on riitautettu useissa oikeudenkäynneissä EU:n jäsenvaltioissa[800].

Esimerkki: Asioissa *Digital Rights Ireland* ja *Kärntner Landesregierung ym.*[801] Digital Rights -ryhmä esitti Irlannin High Courtissa ja Michael Seitlinger Itävallan perustuslakituomioistuimessa kanteet, joissa kyseenalaistettiin niiden kansallisten toimenpiteiden lainmukaisuus, joiden nojalla sähköisiä televiestintätietoja voidaan säilyttää. Digital Rights pyysi Irlannin tuomioistuinta toteamaan direktiivin 2006/24/EY ja terroristirikoksiin liittyvät kansallisen rikosoikeuden osat pätemättömiksi. Samoin Michael Seitlinger ja yli 11 000 muuta kantajaa kyseenalaistivat Itävallan televiestintälain, jolla direktiivi 2006/24/EY saatetaan osaksi kansallista lainsäädäntöä, ja vaativat kumoamaan sen.

Unionin tuomioistuin käsitteli nämä ennakkoratkaisupyynnöt ja totesi tietojen säilyttämistä koskevan direktiivin pätemättömäksi. Tuomioistuimen mukaan tietojen, joita direktiivin mukaan voidaan säilyttää, kokonaisuudesta saa hyvin tarkkaa tietoa ihmisistä. Tuomioistuin tutki myös, miten vakavaa puuttuminen yksityis- ja perhe-elämän kunnioitusta ja henkilötietojen suojaa koskeviin perusoikeuksiin oli. Se totesi, että säilyttäminen täyttää yleisen edun mukaisen tavoitteen – eli vakavan turvallisuuden torjumisen ja niin ollen yleisen turvallisuuden. Tuomioistuin kuitenkin totesi, että EU:n lainsäätäjä oli loukannut suhteellisuusperiaatetta antamalla direktiivin. Vaikka direktiivi voi olla asianmukainen vaaditun tavoitteen saavuttamiseksi, se ”sisältää laajaperäisen ja erityisen vakavan puuttumisen näihin [yksityiselämän kunnioitusta ja henkilötietojen suojaa koskeviin] perusoikeuksiin unionin oikeusjärjestyksessä ilman, että tällaista puuttumista olisi tarkasti rajoitettu säännöksillä, joilla voidaan taata, että se todella rajoitetaan täysin välttämättömään”.

799 Euroopan tietosuojavaltuutettu (2011), *lausunto, annettu 31 päivänä toukokuuta 2011, komission arviointikertomuksesta neuvostolle ja Euroopan parlamentille – tietojen säilyttämistä koskeva direktiivi (direktiivi 2006/24/EY)*, 31.5.2011.

800 Saksa, liittovaltion perustuslakituomioistuin (*Bundesverfassungsgericht*), 1 BvR 256/08, 2.3.2010; Romania, liittovaltion perustuslakituomioistuin (*Curtea Constituțională a României*), nro 1258, 8.10.2009; Tšekki, perustuslakituomioistuin (*Ústavní soud České republiky*), 94/2011 säädöskokoelma, 22.3.2011.

801 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014, 65 kohta.

Jos tietojen säilyttämisestä ei ole erityistä lainsäädäntöä, tietojen säilyttäminen sallitaan poikkeuksena direktiivin 2002/58/EY (sähköisen viestinnän tietosuojadirektiivi)[802] mukaiseen luottamuksellisuuteen ennalta ehkäisevänä toimenpiteenä, mutta sen tarkoituksena on oltava ainoastaan vakavan rikollisuuden torjuminen. Tällainen säilyttäminen on rajoitettava siihen, mikä on ehdottoman välttämätöntä säilytettävien tietoluokkien, asianomaisten viestintäkeinojen, kyseessä olevien henkilöiden ja säilytyksen valitun keston osalta. Kansalliset viranomaiset voivat saada säilytettävät tiedot käyttöönsä tiukoin ehdoin, muun muassa riippumattoman viranomaisen etukäteisen tarkastuksen jälkeen. Tietoja on säilytettävä EU:ssa.

Esimerkki: Asioissa *Digital Rights Ireland* ja *Kärntner Landesregierung ym.*[803] annettujen tuomioiden jälkeen unionin tuomioistuimen käsiteltäväksi saatettiin kaksi muuta asiaa, jotka koskivat Ruotsissa ja Yhdistyneessä kuningaskunnassa sähköisten viestintäpalvelujen tarjoajille määrättyä yleistä velvollisuutta säilyttää televiestintätietoja pätemättömäksi todetun tietojen säilyttämistä koskevan direktiivin mukaisesti. Asioissa *Tele2 Sverige* ja *Home Department vastaan Tom Watson ym.*[804] unionin tuomioistuin totesi, että kansallinen lainsäädäntö, jossa säädetään tietojen yleisestä ja valikoimattomasta säilyttämisestä vaatimatta minkäänlaista yhteyttä säilytettäviksi säädettyjen tietojen ja yleistä turvallisuutta koskevan uhan välillä ja yksilöimättä mitään ehtoja – esim. säilytysaikaa, maantieteellistä aluetta, vakavaan rikollisuuteen todennäköisesti sekaantuneiden henkilöiden ryhmää – ylittää ehdottoman välttämättömän rajat, eikä sitä voida katsoa oikeutetuksi demokraattisessa yhteiskunnassa, kuten edellytetään direktiivissä 2002/58/EY luettuna EU:n perusoikeuskirjan valossa.

Tulevaisuudennäkymät

Euroopan komissio julkaisi tammikuussa 2017 ehdotuksen asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä. Sen

802 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla, (sähköisen viestinnän tietosuojadirektiivi), EYVL 2002, L 201.

803 EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014.

804 EUT, yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB vastaan Post- och telestyrelsen ja Secretary of State for the Home Department vastaan Tom Watson ym.* [suuri jaosto], 21.12.2016.

tarkoituksena on kumota ja korvata sähköisen viestinnän tietosuojadirektiivi.[805] Ehdotuksessa ei ole erityisiä säännöksiä tietojen säilyttämisestä. Siinä kuitenkin säädetään, että jäsenvaltiot voivat rajoittaa lailla tiettyjä velvollisuuksia ja oikeuksia silloin kun tällainen rajoittaminen on välttämätön ja oikeasuhteinen toimenpide demokraattisessa yhteiskunnassa erityisten yleisten etujen, kuten kansallisen turvallisuuden, puolustuksen tai yleisen turvallisuuden takaamiseksi sekä rikosten ennalta estämisen, tutkimisen, paljastamisen tai rikoksiin liittyvien syytetoimien tai rikosoikeudellisten seuraamusten täytäntöönpanon takaamiseksi[806]. Näin ollen jäsenvaltiot voisivat pitää voimassa tai luoda kansallisia tietojen säilyttämistä koskevia säännöstöjä, jotka mahdollistavat kohdennetut tietojen säilyttämistä koskevat toimenpiteet, sikäli kuin tällaiset säännöstöt ovat unionin oikeuden mukaisia ottaen huomioon unionin tuomioistuimen oikeuskäytäntö sähköisen viestinnän tietosuojadirektiivin ja Euroopan unionin perusoikeuskirjan tulkinnasta[807]. Käsikirjaa laadittaessa asetuksen hyväksyminen oli käsiteltävänä.

EU:n ja Yhdysvaltojen välinen puitesopimus lainvalvontatarkoituksia varten vaihdettavien henkilötietojen suojaamiseksi

EU:n ja Yhdysvaltojen välinen puitesopimus rikosten ennalta estämiseen, tutkimiseen, paljastamiseen ja rikoksia koskeviin syytetoimiin liittyvien henkilötietojen käsittelystä tuli voimaan 1. helmikuuta 2017[808]. EU:n ja Yhdysvaltojen välisen puitesopimuksen tarkoituksena on varmistaa henkilötietojen korkeatasoinen suoja EU:n kansalaisille sekä lisätä EU:n ja Yhdysvaltojen lainvalvontaviranomaisten yhteistyötä. Sillä täydennetään voimassa olevia EU:n ja Yhdysvaltojen sekä jäsenvaltioiden ja Yhdysvaltojen välillä voimassa olevia lainvalvontaviranomaisten välisiä sopimuksia ja autetaan ottamaan käyttöön selvät ja yhdenmukaistetut tietosuojasäännöt tämän alan tulevia sopimuksia varten. Tämän osalta sopimuksen tarkoituksena on perustaa kestävä oikeudellinen kehys helpottaman tietojen vaihtoa.

Sopimus ei itsessään ole sopiva oikeusperusta henkilötietojen vaihdolle, mutta kyseessä olevat henkilöt saavat siitä asianmukaiset tietosuojaa koskevat

805 Euroopan komissio (2017), *ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus)*, COM(2017) 10 final, Bryssel, 10.1.2017.

806 *Ibid.*, johdanto-osan 26 kappale.

807 Ks. sähköisen viestinnän tietosuoja-asetuksesta annetun ehdotuksen COM(2017) 10 final perustelujen 1.3 kohta.

808 Ks. EU:n neuvosto (2016), "*Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement'*", lehdistötiedote 305/16, 2.6.2016.

suojatoimet. Se koskee kaikkia henkilötietoja, joita tarvitaan rikosten, mukaan lukien terrorismi, ennalta estämistä, tutkimista, paljastamista ja rikoksiin liittyviä syytetoimia varten[809].

Sopimuksessa määrätään useista suojatoimista, joilla varmistetaan, että henkilötietoja käytetään ainoastaan sopimuksessa yksilöityihin tarkoituksiin. Siinä taataan EU:n kansalaisille erityisesti seuraava suoja:

- tietojen käytön rajoitukset: henkilötietoja saa käyttää vain rikosten ennalta estämiseen, tutkimiseen, paljastamiseen ja rikoksia koskeviin syytetoimiin
- suoja mielivaltaiselta ja perusteettomalta syrjinnältä
- tietojen siirtäminen edelleen: kaikki tietojen siirtäminen edelleen muuhun maahan kuin Yhdysvaltoihin tai EU:n jäsenvaltioon tai kansainväliselle järjestölle edellyttää tiedot alun perin lähettäneen maan toimivaltaisen viranomaisen etukäteen antamaa suostumusta
- tietojen laatu: henkilötietoja on säilytettävä täsmällisinä, merkityksellisinä, ajantasaisina ja täydellisinä
- käsittelyn turvallisuus, myös ilmoitus henkilötietojen tietoturvaloukkauksista
- arkaluonteisten tietojen käsittely on sallittua ainoastaan, jos sovelletaan lainmukaisesti riittäviä suojatoimia
- säilyttämisajat: henkilötietoja ei saa säilyttää pidempään kuin on tarpeen ja asianmukaista
- tietoihin pääsyä ja tietojen oikaisua koskevat oikeudet: jokaisella on oikeus saada pääsy henkilötietoihinsa tietyin ehdoin ja pyytää virheellisten tietojen korjaamista

809 Amerikan yhdysvaltojen ja Euroopan unionin sopimus rikosten ennalta estämiseen, tutkimiseen, paljastamiseen ja rikoksia koskeviin syytetoimiin liittyvien henkilötietojen suojasta, tehty 18.5.2016 (alkuperäinen versio englanninkielinen), 8557/16, 3 artiklan 1 kohta. Ks. myös komission 26.5.2010 päivätty ilmoitus (englanniksi) EU:n ja Yhdysvaltojen tietosuojasopimusta koskevista neuvotteluista, MEMO/10/216, ja Euroopan komission 26.5.2010 päivätty lehdistötiedote (2010) tiukoista tietosuojanormeista EU:n ja Yhdysvaltojen välisessä tietosuojasopimuksessa, IP/10/609.

- automaattiset päätökset edellyttävät asianmukaisia suojatoimia, muun muassa mahdollisuutta vaatia, että käsittelyyn osallistuu ihminen

- tehokas valvonta, muun muassa EU:n ja Yhdysvaltojen valvontaviranomaisten välinen yhteistyö

- oikeudellinen muutoksenhaku ja täytäntöönpanokelpoisuus: EU:n kansalaisilla on oikeus[810] oikeudelliseen muutoksenhakuun yhdysvaltalaisissa tuomioistuimissa, jos Yhdysvaltojen viranomaiset kieltävät tietoihin pääsyn tai tietojen oikaisun tai luovuttavat heidän henkilötietojaan lainvastaisesti.

Puitesopimuksen nojalla on myös perustettu järjestelmä, jossa ilmoitetaan henkilötietojen tietoturvaloukkauksista tarvittaessa asianomaisten henkilöiden jäsenvaltion toimivaltaisille viranomaisille. Sopimuksessa taatuilla oikeudellisilla suojatoimilla varmistetaan EU:n kansalaisten yhdenvertainen kohtelu Yhdysvalloissa, jos yksityisyyttä loukataan.[811]

8.3.1 Tietosuoja EU:n oikeusasioiden virastoissa ja lainvalvontavirastoissa

Europol

EU:n lainvalvontavirastolla, Europolilla, on päämaja Haagissa ja kansalliset yksiköt (ENU:t) kaikissa jäsenvaltioissa. Europol perustettiin vuonna 1998; sen nykyinen oikeudellinen asema EU:n toimielimenä perustuu asetukseen Euroopan unionin

810 Presidentti Obama allekirjoitti 24. helmikuuta 2016 Yhdysvaltojen oikeudellista muutoksenhakua koskevan lain US Judicial Redress Act.

811 Euroopan tietosuojavaltuutettu antoi lausunnon EU:n ja Yhdysvaltojen sopimuksesta ja suositteli muun muassa seuraavia muutoksia: 1) lisätään maininta tietojen siirtämisen erityistarkoituksista artiklaan, jossa käsitellään tietojen säilyttämistä vain niin kauan kuin on tarpeen ja asianmukaista, ja 2) selvennetään, että arkaluonteisten tietojen massasiirto ei ole sallittua. Ks. Euroopan tietosuojavaltuutettu, Opinion 1/2016, *Preliminary Opinion on the agreement between the United State of America and the European Union on the protection of personal information relating to the prevention, investigation, detection and prosecution of criminal offences*, 35 kohta (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun alustavasta lausunnosta, joka koskee Amerikan yhdysvaltojen ja Euroopan unionin välistä sopimusta henkilötietojen suojasta rikosten ehkäisemisen, tutkinnan, paljastamisen ja syytteeseenpanon yhteydessä).

lainvalvontayhteistyövirastosta (Europol-asetus)[812]. Europolin tehtävänä on auttaa vähintään kahteen jäsenvaltioon vaikuttavan järjestäytyneen rikollisuuden, terrorismin ja muiden Europol-asetuksen liitteessä I lueteltujen vakavan rikollisuuden muotojen ehkäisemisessä ja tutkinnassa. Se tekee tämän vaihtamalla tietoja ja toimimalla EU:n tietokeskuksena, josta saa tiedustelutietojen analyyseja ja uhka-arviointeja.

Saavuttaakseen tavoitteensa Europol on perustanut Europolin tietojärjestelmän, joka tarjoaa jäsenvaltioille tietokannan, jonka kautta ENU:t voivat vaihtaa rikoksiin liittyviä tiedostelu- ja muita tietoja. Europolin tietojärjestelmän kautta voidaan tarjota saataville tietoja, jotka liittyvät henkilöihin, joita epäillään tai jotka on tuomittu Europolin toimivaltaan kuuluvasta rikoksesta, tai henkilöihin, joiden osalta on tosiasioihin perustuvaa näyttöä siitä, että he aikovat tehdä Europolin toimivaltaan kuuluvia rikoksia. Europol ja ENU:t voivat tallentaa tietoja suoraan Europolin tietojärjestelmään ja hakea sieltä tietoja. Ainoastaan tiedot järjestelmään tallentaneella osapuolella on oikeus muuttaa, oikaista tai poistaa näitä tietoja. Myös EU:n elimet, kolmannet maat ja kansainväliset järjestöt voivat antaa tietoa Europolille.

Europol voi myös hankkia tietoja, joihin kuuluvat myös henkilötiedot, julkisesti saatavilla olevista lähteistä, kuten internetistä. Henkilötietojen siirrot EU:n elimille ovat sallittuja vain, jos ne ovat tarpeen Europolin tai vastaanottavan EU:n elimen tehtävän suorittamiseksi. Henkilötietojen siirrot kolmansiin maihin tai kansainvälisille järjestöille ovat sallittuja vain, jos Euroopan komissio tekee päätöksen, jonka mukaan kyseisen maan tai järjestön tietosuojan taso on riittävä, jäljempänä ’tietosuojan tason riittävyyttä koskeva päätös’, tai jos voimassa on kansainvälinen sopimus tai yhteistyösopimus. Europol voi vastaanottaa ja käsitellä yksityisiltä osapuolilta ja yksityishenkilöiltä peräisin olevia henkilötietoja vain tiukoin ehdoin eli jos kyseiset tiedot on siirtänyt kansallinen yksikkö kansallisen lainsäädäntönsä mukaisesti, yhteyspiste kolmannessa maassa tai kansainvälisessä järjestössä, jonka kanssa tehdään vakiintunutta yhteistyötä yhteistyösopimuksen perusteella, tai kolmannen maan viranomainen tai kansainvälinen järjestö, jota koskee tietosuojan tason riittävyyttä koskeva päätös tai jonka kanssa unioni on tehnyt kansainvälisen sopimuksen. Kaikki tietojenvaihdot tehdään suojatun tiedonvaihtoverkkosovelluksen (SIENA) kautta.

812 Euroopan parlamentin ja neuvoston asetus (EU) 2016/794, annettu 11 päivänä toukokuuta 2016, Euroopan unionin lainvalvontayhteistyövirastosta (Europol) sekä neuvoston päätösten 2009/371/YOS, 2009/934/YOS, 2009/935/YOS, 2009/936/YOS ja 2009/968/YOS korvaamisesta ja kumoamisesta, EUVL L 135, 24.5.2016, s. 53.

Uuden kehityksen vuoksi Europoliin on perustettu erikoistuneita keskuksia. Euroopan verkkorikostorjuntakeskus perustettiin Europoliin vuonna 2013.[813] Keskus toimii verkkorikollisuutta koskevan tiedon solmukohtana EU:ssa. Se auttaa reagoimaan nopeasti tietoverkoissa tapahtuviin rikoksiin, kehittää ja ottaa käyttöön digitaalisia tutkintakeinoja ja levittää verkkorikollisuuden tutkinnan alalla hyviksi todettuja toimintatapoja. Keskuksessa keskitytään seuraaviin verkkorikollisuuden muotoihin:

- järjestäytyneiden rikollisryhmien tekemät verkkorikokset, jotka tuottavat merkittävää rikoshyötyä, kuten verkkopetokset
- verkkorikokset, jotka aiheuttavat uhreille vakavaa haittaa, kuten verkossa tapahtuva lasten seksuaalinen hyväksikäyttö
- verkkorikokset, jotka kohdistuvat unionin elintärkeisiin infrastruktuureihin ja tietojärjestelmiin.

Euroopan terrorismintorjuntakeskus perustettiin tammikuussa 2016 antamaan jäsenvaltioille operatiivista tukea terroristirikoksiin liittyvissä tutkimuksissa. Se tekee reaaliaikaisten operatiivisten tietojen ristiintarkastuksia Europolilla jo olevien tietojen perusteella, selvittää nopeasti talouteen liittyvät johtolangat ja analysoi kaikki saataville olevat tutkimustiedot, jotta terroristiverkostoista voidaan laatia jäsennelty kuva.[814]

Ihmisten salakuljetusta tutkiva eurooppalainen keskus (EMSC) perustettiin helmikuussa 2016 neuvoston marraskuussa 2015 pidetyn kokouksen jälkeen tukemaan jäsenvaltioita muuttajien salakuljetukseen osallistuvien rikollisverkostojen paljastamisessa ja purkamisessa. Se toimii tietokeskuksena ja tukee EU:n alueellisten toimintayksikköjen toimistoja Cataniassa (Italia) ja Pireuksessa (Kreikka). Ne auttavat kansallisia viranomaisia useilla aloilla, muun muassa tiedustelutietojen jakamisessa, rikostutkinnoissa ja ihmisiä salakuljettavien rikollisverkostojen syytetoimissa.[815]

813 Ks. myös EDPS (2012), *Opinion of the Data Protection Supervisor on the Communication from the European Commission to the Council and the European Parliament on the establishment of a European Cybercrime Centre*, Bryssel, 29.6.2012 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunto Euroopan komission neuvostolle ja Euroopan parlamentille osoittamasta tiedonannosta ”Rikostentorjunta digitaaliaikana: Euroopan verkkorikostorjuntakeskuksen perustaminen”).

814 Ks. Europolin englanninkielinen verkkosivu terrorismintorjuntakeskuksesta.

815 Ks. Europolin englanninkielinen verkkosivusto EMSC:stä.

Europolin toimintaan sovelletaan tehostettua tietosuojaa. Se perustuu EU:n toimielinten tietosuoja-asetuksen[816] periaatteisiin ja on myös yhdenmukainen poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin, uudistetun yleissopimuksen 108 ja poliisiasioita koskevan suosituksen kanssa.

Rikoksen uhrien, todistajien tai muiden henkilöiden, jotka voivat antaa tietoja rikoksista, sekä alle 18-vuotiaiden henkilöiden henkilötietojen käsittely on sallittua, jos se on ehdottoman tarpeellista ja oikeasuhteista Europolin tavoitteiden puitteisiin kuuluvien rikosten ehkäisyä tai torjuntaa varten[817]. Henkilötietojen käsittely on kielletty, paitsi jos se on ehdottoman tarpeellista ja oikeasuhteista Europolin tavoitteiden puitteisiin kuuluvien rikosten ehkäisyä tai torjuntaa varten ja jos nämä tiedot täydentävät Europolin käsittelemiä muita henkilötietoja[818]. Molemmissa tapauksissa vain Europolilla saa olla pääsy asianomaisiin tietoihin[819].

Tietojen säilyttäminen on sallittu ainoastaan niin kauan, kuin se on tarpeellista ja oikeasuhteista, ja tarvetta jatkaa tietojen säilyttämistä on tarkasteltava kolmen vuoden välein tai muutoin tiedot poistetaan ilman eri toimenpiteitä[820].

Europol voi tietyin ehdoin siirtää suoraan henkilötietoja unionin elimelle tai kolmannen maan viranomaiselle tai kansainväliselle järjestölle[821]. Jos henkilötietojen tietoturvaloukkaus loukkaa rekisteröidyn oikeuksia ja vapauksia merkittävästi, siitä on ilmoitettava rekisteröidylle ilman aiheetonta viivytystä[822]. Jäsenvaltioissa nimitetään kansallinen valvontaviranomainen valvomaan henkilötietojen käsittelyä Europolissa[823].

Euroopan tietosuojavaltuutetun tehtävänä on valvoa perusoikeuksien ja -vapauksien suojelua Europolin suorittaman henkilötietojen käsittelyn yhteydessä ja varmistaa se sekä antaa ohjeita Europolille ja rekisteröidyille kaikista henkilötietojen käsittelyä koskevista seikoista. Tämän takia tietosuojavaltuutettu vastaanottaa ja tutkii

816 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001, L 8.

817 Europol-asetus, 30 artiklan 1 kohta.

818 *Ibid.*, 30 artiklan 2 kohta.

819 *Ibid.*, 30 artiklan 3 kohta.

820 *Ibid.*, 31 kohta.

821 *Ibid.*, 24 artikla unionin elimistä ja 25 artikla kolmansista maista ja kansainvälisistä järjestöistä.

822 *Ibid.*, 35 artikla.

823 Europol-asetus, 42 artikla.

kanteluita ja toimii tiiviissä yhteistyössä kansallisten valvontaviranomaisten kanssa.[824] Tietosuojavaltuutettu ja kansalliset valvontaviranomaiset kokoontuvat vähintään kahdesti vuodessa yhteistyöneuvostossa, jolla on neuvoa-antava tehtävä[825]. Jäsenvaltioiden on perustettava lailla valvontaviranomainen, jolla on toimivalta valvoa, että jäsenvaltion suorittama henkilötietojen siirto, haku ja mikä tahansa toimittaminen valtion tasolta Europolille on luvallista[826]. Jäsenvaltioiden on myös varmistettava, että kansallinen valvontaviranomainen voi toimia täysin riippumattomasti suorittaessaan Europol-asetuksen mukaisia tehtäviään ja täyttäessään sen mukaisia velvollisuuksiaan[827]. Europol pitää lokitietoja tai dokumentaatiota tietojenkäsittelytoimistaan, jotta voidaan tarkistaa tietojenkäsittelyn lainmukaisuus, toteuttaa omaehtoista valvontaa ja varmistaa tietojen eheys ja tietoturvallisuus. Näissä lokitiedoissa on tietoa henkilötietojen keräämiseen, muuttamiseen, tietoihin pääsyyn sekä niiden paljastamiseen, yhdistämiseen tai poistamiseen liittyvistä käsittelytoimista automaattisissa käsittelyjärjestelmissä[828].

Euroopan tietosuojavaltuutetun päätökseen voidaan hakea muutosta Euroopan unionin tuomioistuimessa[829]. Jokaisella yksilöllä, jolle on aiheutunut vahinkoa laittoman tietojenkäsittelytoimen vuoksi, on oikeus saada korvausta kärsimästään vahingosta joko Europolilta tai siltä jäsenvaltiolta, jossa vahinko on aiheutunut. Yksilön on nostettava kanne Europolia vastaan Euroopan unionin tuomioistuimessa tai jäsenvaltiota vastaan kyseisen jäsenvaltion toimivaltaisessa tuomioistuimessa.[830] Europolin toimintaa voi valvoa myös kansallisten parlamenttien ja Euroopan parlamentin erityinen yhteisparlamentaarinen valvontaryhmä[831]. Jokaisella yksilöllä on oikeus saada pääsy häntä itseään koskeviin henkilötietoihin, joita Europolilla voi olla hänestä, sekä oikeus saada kyseiset henkilötiedot tarkastetuiksi, oikaistuiksi tai poistetuiksi. Näihin voidaan soveltaa poikkeuksia ja rajoituksia.

824 *Ibid.*, 43 ja 44 artikla.

825 *Ibid.*, 45 artikla.

826 *Ibid.*, 42 artiklan 1 kohta.

827 *Ibid.*, 42 artiklan 1 kohta.

828 *Ibid.*, 40 artikla.

829 *Ibid.*, 48 artikla.

830 *Ibid.*, 50 artikla.

831 *Ibid.*, 51 artikla.

Eurojust

Vuonna 2002 perustettu Eurojust on Haagissa päämajaansa pitävä EU:n elin, joka edistää oikeudellista yhteistyötä vähintään kahteen jäsenvaltioon vaikuttavien vakavien rikosten tutkinta- ja syytetoimissa[832]. Eurojustilla on toimivalta

- edistää ja parantaa tutkinta- ja syytetoimien koordinointia jäsenvaltioiden toimivaltaisten kansallisten viranomaisten välillä

- helpottaa oikeudelliseen yhteistyöhön liittyvien pyyntöjen ja päätösten täytäntöönpanoa.

Eurojustin tehtävien toteuttaminen on kansallisten jäsenten vastuulla. Jokainen jäsenvaltio nimeää Eurojustiin yhden tuomarin tai syyttäjän, jonka asema määräytyy kansallisen lainsäädännön mukaan ja jolla on tarvittava toimivalta suorittaa oikeudellisen yhteistyön edistämiseksi ja parantamiseksi tarvittavat tehtävät. Lisäksi kansalliset jäsenet täyttävät yhdessä kollegiona erityisiä Eurojustin tehtäviä.

Eurojust voi käsitellä henkilötietoja siinä määrin kuin se on tarpeen sen tavoitteiden toteuttamiseksi. Tämä mahdollisuus kattaa kuitenkin vain tarkoin määritellyt tiedot henkilöistä, joita epäillään Eurojustin toimivaltaan kuuluvasta rikoksesta tai osallisuudesta tällaiseen rikokseen tai jotka on tuomittu tällaisesta rikoksesta. Eurojust voi myös käsitellä tiettyjä tietoja, jotka koskevat Eurojustin toimivaltaan kuuluvien rikosten todistajia tai uhreja[833]. Poikkeustapauksissa Eurojust voi käsitellä rajoitetun ajan myös muita rikoksen tekohetken olosuhteisiin liittyviä henkilötietoja, jos niillä on välitöntä merkitystä meneillään oleville tutkintatoimille. Eurojust voi toimivaltansa puitteissa tehdä yhteistyötä muiden EU:n toimielinten, elinten ja virastojen kanssa ja vaihtaa niiden kanssa henkilötietoja. Eurojust voi myös tehdä yhteistyötä ja vaihtaa henkilötietoja kolmansien maiden ja järjestöjen kanssa.

832 Euroopan unionin neuvosto (2002), neuvoston päätös 2002/187/YOS, tehty 28 päivänä helmikuuta 2002, Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi, EYVL 2002, L 63; Euroopan unionin neuvosto (2003), neuvoston päätös 2003/659/YOS, tehty 18 päivänä kesäkuuta 2003, Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi tehdyn päätöksen 2002/187/YOS muuttamisesta, EUVL 2003, L 44; Euroopan unionin neuvosto (2009), neuvoston päätös 2009/426/YOS, tehty 16 päivänä joulukuuta 2008, Eurojustin vahvistamisesta sekä Eurojust-yksikön perustamisesta vakavan rikollisuuden torjunnan tehostamiseksi tehdyn päätöksen 2002/187/YOS muuttamisesta, EUVL 2009, L 138 (Eurojust-päätökset).

833 Konsolidoitu versio neuvoston päätöksestä 2002/187/YOS sellaisena kuin se on muutettuna neuvoston päätöksellä 2003/659/YOS ja neuvoston päätöksellä 2009/426/YOS, 15 artiklan 2 kohta.

Tietosuojan osalta Eurojustin on taattava vähintään Euroopan neuvoston uudistetun yleissopimuksen 108 ja siihen myöhemmin tehtyjen muutosten periaatteita vastaava tietosuojan taso. Tietojen vaihdossa on noudatettava erityisiä sääntöjä ja rajoituksia, joista on sovittu joko yhteistyösopimuksessa tai käytännön järjestelyissä Eurojustia koskevien neuvoston päätösten ja Eurojustin tietosuojasääntöjen mukaisesti[834].

Eurojustiin on perustettu riippumaton yhteinen valvontaviranomainen, jonka tehtävänä on valvoa Eurojustin suorittamaa henkilötietojen käsittelyä. Yksityishenkilö voi valittaa yhteiselle valvontaviranomaiselle, jos hän ei tyydy Eurojustin vastaukseen tiedonsaantia tai henkilötietojen korjaamista, suojaamista tai poistamista koskeneeseen pyyntöön. Jos Eurojust käsittelee henkilötietoja lainvastaisesti, se on vastuussa sen jäsenvaltion lainsäädännön mukaisesti, jossa sen päätoimipaikka sijaitsee, eli Alankomaiden lainsäädännön mukaisesti kaikista rekisteröidylle aiheutuneista vahingoista.

Tulevaisuudennäkymät

Euroopan komissio antoi heinäkuussa 2013 ehdotuksen asetukseksi Eurojustin uudistamisesta. Ehdotukseen liittyi ehdotus Euroopan syyttäjänviraston (ks. jäljempänä) perustamisesta. Asetuksen tavoitteena on yhdenmukaistaa toimintoja ja rakennetta Lissabonin sopimuksen mukaisesti. Uudistuksen tavoitteena on myös tehdä selkeä ero Eurojustin kollegion suorittamien Eurojustin operatiivisten tehtävien ja sen hallinnollisten tehtävien välillä. Näin myös jäsenvaltiot pystyvät keskittymään aiempaa enemmän operatiivisiin tehtäviin. Kollegion avuksi hallinnollisten tehtävien suorittamisessa perustetaan uusi hallintoneuvosto.[835]

Euroopan syyttäjänvirasto

Jäsenvaltioilla on yksinomainen toimivalta petosten ja Euroopan unionin talousarviota vahingoittavien rikosten syytteeseenpanossa, vaikka niillä voi olla myös rajatylittäviä seurauksia. Kyseisten rikosten tekijöiden tutkiminen, syytteeseen asettaminen ja oikeuteen vieminen on entistäkin tärkeämpää, erityisesti jatkuvan

834 Säännökset henkilötietojen käsittelyä ja tietosuojaa Eurojustissa koskevasta työjärjestyksestä, EUVL 2005, C 68/01, 19.3.2005, s. 1.

835 Ks. Euroopan komission englanninkielinen verkkosivu Eurojustista.

talouskriisin vuoksi.[836] Euroopan komissio on ehdottanut asetusta Euroopan syyttäjänviraston perustamisesta[837]. Sen tarkoituksena on torjua EU:n taloudellisia etuja vahingoittavia rikoksia. Euroopan syyttäjänvirasto perustetaan tiiviimmän yhteistyön menettelyssä, jossa vähintään yhdeksän jäsenvaltiota voi aloittaa tiiviimmän yhteistyön EU:n rakenteiden alalla ilman, että muut EU:n valtiot ovat osallisina[838]. Belgia, Bulgaria, Espanja, Kreikka, Kroatia, Kypros, Latvia, Liettua, Luxemburg, Portugali, Ranska, Romania, Saksa, Slovakia, Slovenia, Suomi, Tšekki ja Viro ovat liittyneet tiiviimpään yhteistyöhön. Italia ja Itävalta ovat ilmaisseet aikomuksensa liittyä[839].

Euroopan syyttäjänvirastolla on toimivalta tutkia unionin taloudellisia etuja vahingoittavia rikoksia ja nostaa syytteitä niiden perusteella. Sen tavoitteena on koordinoida tehokkaasti tutkinta- ja syytetoimia eri kansallisissa oikeusjärjestyksissä ja parantaa resurssien käyttöä sekä tietojenvaihtoa Euroopan tasolla.[840]

Euroopan syyttäjänviraston päällikkönä toimii Euroopan syyttäjä. Kussakin jäsenvaltiossa toimii vähintään yksi valtuutettu Euroopan syyttäjä, joka vastaa tutkinta- ja syytetoimista kyseisessä jäsenvaltiossa.

Ehdotuksessa säädetään vahvoista suojatoimista, joilla taataan syyttäjänviraston tutkimuksiin osallistuvien henkilöiden oikeudet kansallisen lainsäädännön, EU:n oikeuden ja EU:n perusoikeuskirjan mukaisesti. Eniten perusoikeuksiin vaikuttavien tutkintatoimien toteuttamiseen on saatava etukäteen kansallisen tuomioistuimen lupa[841]. Syyttäjänviraston tutkimuksiin sovelletaan kansallisten tuomioistuinten laillisuusvalvontaa[842].

---

836 Ks. Euroopan komissio (2013), ehdotus neuvoston asetukseksi Euroopan syyttäjänviraston perustamisesta, COM(2013) 534 final, Bryssel, 17.7.2013, s. 1 ja komission englanninkielinen verkkosivu syyttäjänvirastosta.

837 Euroopan komissio (2013), ehdotus neuvoston asetukseksi Euroopan syyttäjänviraston perustamisesta, COM(2013) 534 final, Bryssel, 17.7.2013.

838 Euroopan unionin toiminnasta tehty sopimus, 86 artiklan 1 kohta ja 329 artiklan 1 kohta.

839 Ks. Euroopan unionin neuvosto (2017), "*20 jäsenmaata sopuun yksityiskohdista Euroopan syyttäjänviraston (EPPO) perustamiseksi*", lehdistötiedote, 8.6.2017.

840 Euroopan komissio (2013), ehdotus neuvoston asetukseksi Euroopan syyttäjänviraston perustamisesta, COM(2013) 534 final, Bryssel, 17.7.2013, s. 1 ja s. 51–51. Ks. myös Euroopan komission englanninkielinen verkkosivusto Euroopan syyttäjänvirastosta.

841 Euroopan komissio (2013), ehdotus neuvoston asetukseksi Euroopan syyttäjänviraston perustamisesta, COM(2013) 534 final, Bryssel, 17.7.2013, 26 artiklan 4 kohta.

842 *Ibid.*, 36 artikla.

EU:n toimielinten tietosuoja-asetusta[843] sovelletaan syyttäjänviraston suorittamaan hallinnollisten henkilötietojen käsittelyyn. Operatiivisiin asioihin liittyvien henkilötietojen käsittelyä varten Euroopan syyttäjänvirastolla on Europolin tapaan erillinen tietosuojajärjestelmä, joka on samankaltainen kuin Europolin ja Eurojustin toimissa käytettävä, koska syyttäjänviraston toimien harjoittamiseen kuuluu henkilötietojen käsittelyä lainvalvonta- ja syyttäjäviranomaisten kanssa jäsenvaltioiden tasolla. Euroopan syyttäjänviraston tietosuojasäännöt ovat siksi lähes samanlaiset kuin poliisi- ja rikosoikeusviranomaisia koskevan tietosuojadirektiivin säännöt. Euroopan syyttäjänviraston perustamisesta annetun ehdotuksen mukaan henkilötietojen käsittelyssä on noudatettava lainmukaisuuden ja oikeudenmukaisuuden periaatteita, käyttötarkoitussidonnaisuutta, tietojen minimointia, täsmällisyyttä, eheyttä ja luottamuksellisuutta. Syyttäjänviraston on mahdollisuuksien mukaan erotettava selkeästi toisistaan erityyppisten rekisteröityjen henkilötiedot, kuten rikoksesta tuomittujen henkilöiden, pelkästään epäiltyjen henkilöiden, uhrien ja todistajien henkilötiedot. Sen on myös pyrittävä tarkistamaan käsiteltävien henkilötietojen laatu ja erottamaan mahdollisuuksien mukaan tosiseikkoihin perustuvat henkilötiedot henkilökohtaisiin arviointeihin perustuvista henkilötiedoista.

Ehdotuksessa on säännöksiä rekisteröityjen oikeuksista, erityisesti tiedonsaantioikeudesta, oikeudesta saada pääsy omiin henkilötietoihin, oikeudesta saada tiedot oikaistuiksi tai poistetuiksi tai rajoittaa käsittelyä. Siinä säädetään, että kyseisiä oikeuksia voi myös käyttää välillisesti, Euroopan tietosuojavaltuutetun kautta. Siinä esitetään myös käsittelyn turvallisuuden ja vastuuvelvollisuuden periaatteet ja edellytetään, että syyttäjänvirasto toteuttaa asianmukaisia teknisiä ja organisatorisia toimenpiteitä, joilla varmistetaan asianmukainen suojan taso käsittelyn aiheuttamilta riskeiltä, sekä pitää kirjaa kaikista käsittelytoimista ja tekee tietosuojaa koskevan vaikutustenarvioinnin ennen käsittelyä, kun käsittely (esimerkiksi, jos siinä käytetään uusia teknologioita) aiheuttaa todennäköisesti henkilön oikeuksien kannalta suuren riskin. Ehdotuksessa säädetään myös, että kollegio nimittää tietosuojavastaavan, jonka on osallistuttava asianmukaisesti kaikkiin henkilötietojen käsittelyyn liittyviin asioihin ja varmistettava, että Euroopan syyttäjänvirasto noudattaa sovellettavaa tietosuojalainsäädäntöä.

843 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001, L 8.

8.3.2 Tietosuoja EU-tason yhteisissä tietojärjestelmissä

Sen lisäksi, että jäsenvaltiot voivat vaihtaa keskenään tietoja ja että EU:hun on perustettu rajatylittävää rikollisuutta torjumaan erityisiä viranomaisia, kuten Europol, Eurojust ja Euroopan syyttäjänvirasto, EU:ssa on otettu käyttöön erilaisia yhteisiä tietojärjestelmiä, joiden kautta toimivaltaiset kansalliset ja EU:n viranomaiset voivat tehdä entistä sujuvammin yhteistyötä ja vaihtaa tietoja rajaturvallisuuden, maahanmuutto- ja turvapaikka-asioiden ja tullin aloilla erityisiä tarkoituksia varten. Koska Schengenin alue perustettiin ensin EU:n oikeudesta itsenäisesti toimivalla kansainvälisellä sopimuksella, Schengenin tietojärjestelmä (SIS) kehittyi monenvälisistä sopimuksista, ja se tuotiin myöhemmin EU:n oikeuden piiriin. Viisumitietojärjestelmä (VIS), Eurodac, Eurosur ja tullitietojärjestelmä (TTJ) perustettiin EU:n oikeuteen kuuluvina välineinä.

Näiden järjestelmien valvonta on jaettu kansallisten valvontaviranomaisten ja Euroopan tietosuojavaltuutetun kesken. Suojan korkean tason varmistamiseksi nämä viranomaiset tekevät yhteistyötä valvonnan koordinointiryhmissä, joissa käsitellään seuraavia laaja-alaisia tietojärjestelmiä: 1) Eurodac, 2) viisumitietojärjestelmä, 3) Schengenin tietojärjestelmä, 4) tullitietojärjestelmä ja 5) sisämarkkinoiden tietojärjestelmä[844]. Valvonnan koordinointiryhmät kokoontuvat tavallisesti kahdesti vuodessa valitun puheenjohtajan johdolla ja antavat ohjeita, keskustelevat rajat ylittävistä asioista ja hyväksyvät yhteisiä tutkintakehyksiä.

Vuonna 2012 perustettu laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaava Euroopan unionin virasto (tietotekniikkavirasto)[845] vastaa toisen sukupolven Schengenin tietojärjestelmän (SIS II), viisumitietojärjestelmän (VIS) ja Eurodac-järjestelmän operatiivisesta hallinnoinnista. Tietotekniikkaviraston päätehtävänä on varmistaa tietojärjestelmien tehokas, turvallinen ja jatkuva toiminta Se vastaa myös tarvittavien toimenpiteiden toteuttamisesta järjestelmien ja tietojen turvaamiseksi.

844 Ks. Euroopan tietosuojavaltuutetun (englanninkielinen) verkkosivusto valvonnan koordinoinnista.

845 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1077/2011, annettu 25 päivänä lokakuuta 2011, vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston perustamisesta, EUVL 2011, L 286.

Schengenin tietojärjestelmä

Vuonna 1985 Euroopan yhteisöihin kuuluneet Benelux-maat, Saksa ja Ranska tekivät sopimuksen tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla (Schengenin sopimus). Sopimuksella oli tarkoitus luoda Schengenin alue, jolla henkilöt voisivat liikkua vapaasti ilman rajatarkastuksia.[846] Rajojen avaamisesta yleiselle turvallisuudelle aiheutuvan uhan vastapainoksi rajatarkastuksia Schengenin alueen ulkorajoilla vahvistettiin ja kansallisten poliisi- ja oikeusviranomaisten välistä yhteistyötä tiivistettiin.

Uusien valtioiden liityttyä Schengenin sopimukseen koko järjestelmä sisällytettiin lopulta EU:n oikeudelliseen kehykseen Amsterdamin sopimuksella[847] Päätös pantiin täytäntöön vuonna 1999. Schengenin tietojärjestelmän uusin versio, niin kutsuttu SIS II, otettiin käyttöön 9. huhtikuuta 2013. Se palvelee nykyään kaikkien EU:n jäsenvaltioiden[848] lisäksi Islantia, Liechtensteinia, Norjaa ja Sveitsiä[849]. Myös Europol ja Eurojust voivat käyttää SIS II -järjestelmää.

SIS II sisältää keskusjärjestelmän (C-SIS), kansallisen järjestelmän (N-SIS) jokaisessa jäsenvaltiossa, sekä keskusjärjestelmän ja kansallisten järjestelmien välisen viestintäinfrastruktuurin. C-SIS sisältää tiettyjä jäsenvaltioiden henkilöistä ja esineistä tallentamia tietoja. C-SIS-järjestelmää käyttävät kansalliset rajavalvonta-, poliisi-, tulli-, viisumi- ja oikeusviranomaiset eri puolilla Schengen-aluetta. Jokainen jäsenvaltio käyttää C-SIS:stä kansallista kopiota, jota kutsutaan kansalliseksi Schengenin tietojärjestelmäksi (N-SIS), ja päivittää sitä säännöllisesti siten, että samalla myös C-SIS päivittyy. SIS-järjestelmä antaa erilaisia kuulutuksia, jos

- henkilöllä ei ole oikeutta tulla Schengen-alueelle tai oleskella siellä; tai

846 Benelux-talousliiton valtioiden, Saksan liittotasavallan ja Ranskan tasavallan hallitusten välinen sopimus tarkastusten asteittaisesta lakkauttamisesta yhteisillä rajoilla, EYVL 2000, L 239.

847 Euroopan yhteisöt (1997), Amsterdamin sopimus Euroopan unionista tehdyn sopimuksen, Euroopan yhteisöjen perustamissopimusten ja niihin liittyvien tiettyjen asiakirjojen muuttamisesta, EYVL 1997, C 340.

848 Irlanti, Kroatia ja Kypros tekevät valmistelutoimia SIS II -järjestelmään liittymiseksi, mutta ne eivät vielä kuulu siihen. Schengenin tietojärjestelmästä on englanniksi tietoa Euroopan komission muuttoliike- ja sisäasioiden pääosaston verkkosivustolla.

849 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, annettu 20 päivänä joulukuuta 2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL 2006, L 381; Euroopan unionin neuvosto (2007), neuvoston päätös 2007/533/YOS, tehty 12 päivänä kesäkuuta 2007 , toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, (SIS II), EUVL 2007, L 205.

- oikeus- tai lainvalvontaviranomaiset etsivät kyseistä henkilöä tai esinettä (eli eurooppalainen pidätysmääräys, pyynnöt hienovaraisesta valvonnasta); tai

- henkilö on ilmoitettu kadonneeksi; tai

- tavarat, kuten setelit, autot, perävaunut, aseet tai henkilötodistukset on ilmoitettu varastetuiksi tai kadonneiksi.

Kun kuulutus on annettu, SIRENE-toimistojen kautta käynnistetään jatkotoimet. SIS II:ssa on uusina toimintoina muun muassa mahdollisuus tallentaa biometrisiä tietoja, kuten sormenjälkiä ja valokuvia; uusia kuulutusluokkia, kuten varastetut veneet, ilma-alukset, kontit tai maksuvälineet; entistä tarkempia kuulutuksia henkilöistä ja esineistä; kopioita eurooppalaisista pidätysmääräyksistä henkilöistä, joita etsitään kiinniottoa tai luovuttamista varten.

SIS II perustuu kahteen toisiaan täydentävään säädökseen: SIS II -päätökseen[850] ja SIS II -asetukseen[851]. EU:n lainsäätäjä käytti päätöksen ja asetuksen antamiseen eri oikeusperustoja. Päätös koskee SIS II -järjestelmän käyttöä rikosasioissa tehtävään poliisiyhteistyöhön ja oikeudelliseen yhteistyöhön (EU:n entinen kolmas pilari) kuuluvia tarkoituksia varten. Asetus koskee kuulutusmenettelyjä, jotka kuuluvat henkilöiden vapaaseen liikkumiseen liittyvien viisumi-, turvapaikka- ja maahanmuuttoasioita koskevien ja muiden toimintalinjojen soveltamisalaan (entinen ensimmäinen pilari). Kunkin pilarin kuulutusmenettelyjä on säänneltävä erillisillä säädöksillä, koska molemmat säädökset annettiin ennen Lissabonin sopimusta ja pilarirakenteen kumoamista.

Molemmissa säädöksissä on sääntöjä tietosuojasta. SIS II -päätöksessä kielletään arkaluonteisen tietojen käsittely[852]. Henkilötietojen käsittely kuuluu uudistetun yleissopimuksen 108 soveltamisalaan[853]. Henkilöillä on myös oikeus saada tieto SIS II -järjestelmään tallennetuista itseään koskevista henkilötiedoista[854].

850 Neuvoston päätös 2007/533/YOS, tehty 12 päivänä kesäkuuta 2007, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL L 205, 7.8.2007.

851 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1987/2006, annettu 20 päivänä joulukuuta 2006, toisen sukupolven Schengenin tietojärjestelmän (SIS II) perustamisesta, toiminnasta ja käytöstä, EUVL L 381, 28.12.2006.

852 SIS II -päätös, 56 artikla; SIS II -asetus, 40 artikla.

853 SIS II -päätös, 57 artikla.

854 SIS II -päätös, 58 artikla; SIS II -asetus, 41 artikla.

SIS II -asetuksella säännellään ehtoja ja menettelyjä, jotka koskevat kolmansien maiden kansalaisia koskevien kuulutusten tallentamista SIS II:een ja niiden käsittelyä siinä jäsenvaltioon saapumisen tai siellä oleskelun epäämiseksi. Siinä annetaan myös sääntöjä jäsenvaltioon saapumista tai siellä oleskelua koskevien lisätietojen ja täydentävien tietojen vaihtoa varten.[855] Asetuksessa on sääntöjä myös tietosuojasta. Yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa tarkoitettuja arkaluonteisia tietoja ei saa käsitellä[856]. SIS II -asetus sisältää myös tiettyjä rekisteröidyn oikeuksia, jotka ovat

- rekisteröidyn oikeus saada tieto itseään koskevista henkilötiedoista[857]
- oikeus saada asiavirheitä sisältävät tiedot oikaistuiksi[858]
- oikeus saada oikeudettomasti tallennetut tiedot poistettaviksi[859] ja
- oikeus saada ilmoitus rekisteröidystä tehdystä kuulutuksesta. Tiedot on toimitettava kirjallisesti ja niihin on liitettävä jäljennös kansallisesta päätöksestä, jonka perusteella kuulutus on tehty, tai sitä koskeva viite.[860]

Tiedonsaantioikeutta ei sovelleta, jos 1) henkilötietoja ei ole saatu rekisteröidyltä ja tietojen antaminen osoittautuu mahdottomaksi tai vaatii suhteettoman paljon työtä, 2) rekisteröity on jo saanut tiedon tai 3) kansallisessa lainsäädännössä sallitaan rajoittaminen muun muassa valtion kansallisen turvallisuuden takaamiseksi tai rikosten ennalta estämiseksi[861].

Sekä SIS II -päätöksen että SIS II -asetuksen mukaan henkilön oikeutta saada tieto SIS II:een tallennetuista tiedoista voidaan käyttää missä tahansa jäsenvaltiossa, ja sitä käsitellään kyseisen jäsenvaltion kansallisen lainsäädännön mukaan[862].

855 SIS II -asetus, 2 artikla.
856 *Ibid.*, 40 artikla.
857 *Ibid.*, 41 artiklan 1 kohta.
858 *Ibid.*, 41 artiklan 5 kohta.
859 *Ibid.*, 41 artiklan 5 kohta.
860 *Ibid.*, 42 artiklan 1 kohta.
861 *Ibid.*, 42 artiklan 2 kohta.
862 SIS II -asetus, 41 artiklan 1 kohta; SIS II -päätös, 58 artikla.

Esimerkki: Asiassa *Dalea v. Ranska*[863] kantajalta evättiin viisumi Ranskaan, koska Ranskan viranomaiset olivat ilmoittaneet Schengenin tietojärjestelmään, ettei häntä tulisi päästää maahan. Kantaja käytti tarkastusoikeuttaan sekä oikeutta saada tiedot korjatuiksi tai poistetuiksi ensin Ranskan tietosuojaviranomaiselta ja lopuksi korkeimmasta hallinto-oikeudesta, mutta pyyntö evättiin. Euroopan ihmisoikeustuomioistuin katsoi, että kantaja oli kirjattu Schengenin tietojärjestelmään lainmukaisesti ja että kirjaamisen laillisena tarkoituksena oli ollut kansallisen turvallisuuden suojaaminen. Koska kantaja ei ollut osoittanut kärsineensä vahinkoa sen johdosta, että häneltä oli evätty pääsy Schengen-alueelle, ja koska hänen suojaamiseksensa mielivaltaisilta päätöksiltä oli toteutettu riittävät toimenpiteet, puuttuminen oikeuteen nauttia yksityiselämän kunnioitusta oli ollut oikeasuhteista. Kantajan 8 artiklaan perustuvaa valitusta ei näin ollen otettu tutkittavaksi.

Toimivaltainen kansallinen valvontaviranomainen kussakin jäsenvaltiossa valvoo kansallista N-SIS-järjestelmää. Kansallisen valvontaviranomaisen on varmistettava, että N-SIS-järjestelmässä tapahtunut tietojenkäsittely tarkastetaan vähintään joka neljäs vuosi[864]. Kansalliset valvontaviranomaiset ja Euroopan tietosuojavaltuutettu tekevät yhteistyötä ja varmistavat SIS:n koordinoidun valvonnan, kun taas C-SIS:n valvonnasta vastaa Euroopan tietosuojavaltuutettu. Avoimuuden varmistamiseksi toimista lähetetään yhteinen toimintaselvitys Euroopan parlamentille, neuvostolle ja tietotekniikkavirastolle joka toinen vuosi. SIS-järjestelmän valvonnan koordinoinnin varmistamiseksi on perustettu SIS II -järjestelmän valvonnan koordinointiryhmä, joka kokoontuu kahdesti vuodessa. Ryhmä koostuu Euroopan tietosuojavaltuutetusta ja niiden jäsenvaltioiden valvontaviranomaisten edustajista, jotka ovat ottaneet SIS II -järjestelmän käyttöön, sekä Islannin, Liechtensteinin, Norjan ja Sveitsin edustajista, koska SIS-järjestelmä koskee myös niitä, sillä ne kuuluvat Schengenin alueeseen.[865] Irlanti, Kroatia ja Kypros eivät vielä kuulu SIS II -järjestelmään, ja siksi ne osallistuvat valvonnan koordinointiryhmään vain tarkkailijoina. Euroopan tietosuojavaltuutettu ja kansalliset valvontaviranomaiset tekevät valvonnan koordinointiryhmässä aktiivisesti yhteistyötä vaihtamalla tietoja, auttamalla toisiaan tarkastusten ja tutkimusten tekemisessä, laatimalla yhdenmukaistettuja ehdotuksia mahdollisten ongelmien yhteisiksi ratkaisuiksi ja lisäämällä tietoisuutta tietosuojaoikeuksista[866]. SIS II -järjestelmän valvonnan koordinointiryhmä antaa myös

863 EIT, *Dalea v. Ranska*, nro 964/07, 2.2.2010.

864 SIS II -asetus, 60 artiklan 2 kohta.

865 Ks. Euroopan tietosuojavaltuutetun (englanninkielinen) verkkosivusto Schengenin tietojärjestelmästä.

866 SIS II -asetus, 46 artikla; SIS II -päätös, 62 artikla.

ohjeita rekisteröityjen avuksi. Rekisteröidyille on esimerkiksi laadittu ohjeet avuksi tiedonsaantioikeuksien käyttämisessä.[867]

Tulevaisuudennäkymät

Euroopan komissio teki vuonna 2016 SIS-järjestelmän arvioinnin[868], jossa todettiin, että käytössä on kansallisia järjestelmiä, joiden avulla rekisteröidyt voivat tarkastaa itseään koskevat SIS II -järjestelmään tallennetut tiedot ja saada asiavirheitä sisältävät tiedot oikaistuiksi tai poistetuiksi tai saada niistä vahingonkorvausta. SIS II -järjestelmän tuloksellisuuden ja tehokkuuden parantamiseksi Euroopan komissio esitti kolme ehdotusta asetuksiksi:

- SIS-järjestelmän perustamisesta, toiminnasta ja käytöstä rajatarkastuksissa annettu asetus, jolla kumotaan SIS II -asetus

- SIS-järjestelmän perustamisesta, toiminnasta ja käytöstä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä annettu asetus, jolla kumotaan muun muassa SIS II -päätös, ja

- asetus SIS-järjestelmän käytöstä laittomasti oleskelevien kolmansien maiden kansalaisten palauttamiseksi.

Ehdotuksissa on tärkeää, että niiden nojalla voidaan käsitellä muita biometristen tietojen ryhmiä nykyiseen SIS II -järjestelmään jo kuuluvien valokuvien ja sormenjälkien lisäksi. Myös kasvojäljet, kämmenjäljet ja dna-tunnisteet tallennetaan SIS-tietokantaan. Lisäksi, kun SIS II -asetuksen ja SIS II -päätöksen nojalla henkilön tunnistamiseksi voitiin tehdä haku sormenjäljillä, ehdotuksissa tästä hausta tehdään pakollista, jos henkilön henkilöllisyyttä ei voida varmistaa muulla tavalla. Kasvokuvia, valokuvia ja kämmenjälkiä täytetään järjestelmän haussa ja ihmisten tunnistamisessa, kun siitä tulee teknisesti mahdollista. Uudet biometrisiä tunnisteita koskevat säännöt aiheuttavat erityisiä riskejä yksilöiden oikeuksille. Komission

867 Ks. SIS II -järjestelmän valvonnan koordinointiryhmän englanninkieliset ohjeet, *The Schengen Information System. A guide for exercising the right of access*, jotka ovat saatavilla Euroopan tietosuojavaltuutetun verkkosivustolla.

868 Euroopan komissio, komission kertomus Euroopan parlamentille ja neuvostolle toisen sukupolven Schengenin tietojärjestelmän (SIS II) arvioinnista asetuksen (EY) N:o 1987/2006 24 artiklan 5 kohdan, 43 artiklan 3 kohdan ja 50 artiklan 5 kohdan sekä päätöksen 2007/533/YOS 59 artiklan 3 kohdan ja 66 artiklan 5 kohdan mukaisesti, COM(2016) 880 final, Bryssel, 21.12.2016.

ehdotuksista antamassaan lausunnossa[869] Euroopan tietosuojavaltuutettu pani merkille, että biometriset tiedot ovat erittäin arkaluonteisia ja että niiden käyttöönoton tällaisessa laajamittaisessa tietokannassa pitäisi perustua näyttöön perustuvaan arviointiin siitä, onko niiden käyttö SIS-järjestelmässä tarpeellista. Toisin sanoen olisi osoitettava, että uusien tunnisteiden käsittely on tarpeen. Euroopan tietosuojavaltuutettu katsoi myös, että tarvitaan lisäselvennystä siitä, minkälaista tietoa dna-tunnisteeseen voidaan sisällyttää. Koska dna-tunniste voi sisältää arkaluonteista tietoa (selkeimpänä esimerkkinä terveysongelmia paljastavat tiedot), SIS-järjestelmään tallennettujen dna-tunnisteiden pitäisi sisältää vain vähimmäistiedot, jotka ovat ehdottoman välttämättömiä kadonneiden henkilöiden tunnistamiseksi ja joista jätetään yksiselitteisesti pois terveystiedot, rotu ja kaikki muut arkaluonteiset tiedot[870]. Ehdotuksissa otetaan kuitenkin käyttöön täydentäviä suojatoimia, joilla rajoitetaan tietojen kerääminen ja edelleenkäsittely vain siihen, mikä on ehdottoman välttämätöntä ja tarpeen operatiivisista syistä, ja pääsy näihin tietoihin rajoitetaan vain niihin henkilöihin, joilla on operatiivinen tarve käsitellä niitä[871]. Ehdotuksissa myös valtuutetaan eu-LISA laatimaan jäsenvaltioille säännöllisin väliajoin tietojen laatua koskevia kertomuksia, jotta kuulutuksia voidaan tarkistaa säännöllisesti tietojen laadun varmistamiseksi[872].

Viisumitietojärjestelmä

Viisumitietojärjestelmä (VIS), joka on niin ikään tietotekniikkaviraston hallinnoima, kehitettiin EU:n yhteisen viisumipolitiikan täytäntöönpanon tueksi[873]. VIS:n avulla Schengen-maat voivat vaihtaa viisumin hakijoiden tietoja sellaisen täysin keskitetyn

869 EDPS (2017), EDPS Opinion on the new legal basis of the Schengen Information System, lausunto 7/2017, 2.5.2017 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee Schengenin tietojärjestelmän uutta oikeusperustaa).

870 *Ibid.*, 22 kohta.

871 Euroopan komissio (2016), ehdotus Euroopan parlamentin ja neuvoston asetukseksi Schengenin tietojärjestelmän (SIS) perustamisesta, toiminnasta ja käytöstä poliisiyhteistyössä ja rikosasioissa tehtävässä oikeudellisessa yhteistyössä, asetuksen (EU) N:o 515/2014 muuttamisesta sekä asetuksen (EY) N:o 1986/2006, neuvoston päätöksen 2007/533/YOS ja komission päätöksen 2010/261/EU kumoamisesta, COM(2016) 883 final, Bryssel, 21.12.2016.

872 *Ibid.*, s. 15.

873 Euroopan unionin neuvosto (2004), neuvoston päätös, tehty 8 päivänä kesäkuuta 2004, viisumitietojärjestelmän (VIS) perustamisesta, EUVL 2004, L 213; Euroopan parlamentin ja neuvoston asetus (EY) N:o 767/2008, annettu 9 päivänä heinäkuuta 2008, viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta (VIS-asetus), EUVL 2008, L 218; Euroopan unionin neuvosto (2008), neuvoston päätös 2008/633/YOS, tehty 23 päivänä kesäkuuta 2008, jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi, EUVL 2008, L 218.

järjestelmän kautta, joka yhdistää Schengen-maiden EU:n ulkopuolella sijaitsevat konsulaatit ja lähetystöt kaikkien Schengen-maiden ulkorajojen ylityspaikkoihin. VIS käsittelee lyhytaikaista oleskelua tai kauttakulkua varten Schengen-alueelle haettavien viisumien tietoja. VIS:n avulla rajavalvontaviranomaiset voivat tarkistaa käyttäen biometrisiä tunnisteita, erityisesti sormenjälkiä, onko viisumin esittävä henkilö sen oikea haltija, ja tunnistaa henkilöt, joilla ei ole asiakirjoja tai joiden asiakirjat ovat väärennettyjä.

Viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta annetulla asetuksella (EY) N:o 767/2008 (VIS-asetus) säädetään edellytykset ja menettelyt, joita sovelletaan lyhytaikaista oleskelua koskeviin viisumihakemuksiin liittyvien henkilötietojen siirtämiseen. Se koskee myös hakemuksia koskevia päätöksiä, eli myös niitä, jotka koskevat viisumin mitätöimistä, peruuttamista tai pidentämistä.[874] VIS-asetus koskee pääasiassa hakijaa ja hänen viisumejaan koskevia tietoja, valokuvia, sormenjälkiä, linkkejä aiempiin hakemuksiin sekä hakijan mukana matkustavien henkilöiden hakemustiedostoja ja henkilöiden kutsumista koskevia tietoja[875]. Pääsy viisumitietojärjestelmään tietojen tallentamista, muuttamista tai poistamista varten on varattu ainoastaan viisumiviranomaisille, kun taas tietojen hakemista varten viisumitietojärjestelmään voivat päästä viisumiviranomaisten lisäksi viranomaiset, joilla on toimivalta tehdä tarkastuksia ulkorajojen ylityspaikoilla sekä maahanmuuttoon ja turvapaikkaan liittyviä tarkastuksia.

Toimivaltaiset kansalliset poliisiviranomaiset ja Europol voivat tietyin edellytyksin pyytää pääsyä VIS-järjestelmään tallennettuihin tietoihin terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi[876]. Koska VIS on tarkoitettu välineeksi, jolla tuetaan yhteisen viisumipolitiikan täytäntöönpanoa, 3.2 kohdassa selitettyä käyttötarkoitussidonnaisuuden periaatetta, joka edellyttää, että henkilötietoja käsitellään vain tiettyjä nimenomaisia ja laillisia tarkoituksia varten ja että niiden on oltava asianmukaisia, olennaisia eikä liian laajoja siihen tarkoitukseen, missä niitä käsitellään, rikottaisiin, jos VIS-järjestelmästä tehtäisiin lainvalvontaväline. Tämän vuoksi kansallisille lainvalvontaviranomaisille ja Europolille

874 VIS-asetus, 1 artikla.

875 Viisumitietojärjestelmästä (VIS) ja lyhytaikaista oleskelua varten myönnettäviä viisumeja koskevasta jäsenvaltioiden välisestä tietojenvaihdosta 9 päivänä heinäkuuta 2008 annetun asetuksen (EY) N:o 767/2008 (VIS-asetus) 5 artikla, EUVL 2008, L 218.

876 Euroopan unionin neuvosto (2008), neuvoston päätös 2008/633/YOS, annettu 23 päivänä kesäkuuta 2008, jäsenvaltioiden nimeämien viranomaisten ja Europolin pääsystä tekemään hakuja viisumitietojärjestelmästä (VIS) terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi, EUVL 2008, L 218.

ei myönnetä automaattista pääsyä VIS-tietokantaan. Pääsy voidaan myöntää vain tapauskohtaisesti, ja se edellyttää tiukkoja suojatoimia. Näiden viranomaisten pääsyä VIS-järjestelmään ja tietojen hakemista siitä koskevista edellytyksistä ja suojatoimista säädetään neuvoston päätöksessä 2008/644/YOS[877].

VIS-asetuksessa säädetään myös rekisteröityjen oikeuksista. Niitä ovat

- oikeus saada vastuulliselta jäsenvaltiolta ilmoitus jäsenvaltiossa henkilötietojen käsittelystä vastaavasta rekisterinpitäjästä ja sen yhteystiedoista, tarkoituksesta, johon heidän henkilötietojaan käytetään viisumitietojärjestelmässä, tietojen vastaanottajien ryhmistä ja tietojen säilyttämisajasta. Viisuminhakijoille on lisäksi ilmoitettava siitä, että tietojen tallentaminen VIS-järjestelmään on pakollista hakemuksen käsittelyä varten. Jäsenvaltioiden on myös ilmoitettava heille heidän oikeudestaan tutustua itseään koskeviin tietoihin ja pyytää tietojen oikaisemista tai poistamista ja lisäksi on ilmoitettava näiden oikeuksien käyttöä koskevista menettelyistä[878]

- oikeus saada tietoonsa viisumitietojärjestelmään tallennetut heitä itseään koskevat tiedot[879]

- oikeus saada virheelliset tiedot oikaistuiksi[880]

- oikeus saada lainvastaisesti tallennetut tiedot poistetuiksi[881].

VIS-järjestelmän valvonnan varmistamiseksi perustettiin VIS-järjestelmän valvonnan koordinointiryhmä. Siinä on edustajat Euroopan tietosuojavaltuutetusta ja kansallisista valvontaviranomaisista, ja se kokoontuu kahdesti vuodessa. Ryhmässä on edustajat 28:sta EU:n jäsenvaltiosta ja Islannista, Liechtensteinista, Norjasta ja Sveitsistä.

877 *Ibid.*

878 VIS-asetus, 37 artikla.

879 *Ibid.*, 38 artiklan 1 kohta.

880 *Ibid.*, 38 artiklan 2 kohta.

881 *Ibid.*, 38 artiklan 2 kohta.

Eurodac

Eurodacin nimi tulee eurooppalaista sormenjälkitutkimusta tarkoittavista sanoista European Dactyloscopy[882]. Kyseessä on keskitetty järjestelmä, joka sisältää niiden kolmansien maiden kansalaisten ja kansalaisuudettomien henkilöiden sormenjälkitiedot, jotka ovat hakeneet turvapaikkaa jossakin EU:n jäsenvaltiossa[883]. Järjestelmä on ollut toiminnassa tammikuusta 2003 lähtien, kun neuvoston asetus (EY) N:o 2725/2000 annettiin. Sen uudelleenlaadittua versiota alettiin soveltaa vuonna 2015. Sen pääasiallisena tarkoituksena on auttaa määrittämään jäsenvaltio, joka on vastuussa turvapaikkahakemuksen käsittelystä asetuksen (EY) N:o 604/2013 mukaisesti. Asetuksessa vahvistetaan perusteet ja menettelyt kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämistä varten (Dublin III -asetus).[884] Eurodacin sisältämiä henkilötietoja voidaan pääasiassa käyttää Dublin III -asetuksen soveltamisen helpottamiseksi.[885]

Jäsenvaltioiden lainvalvontaviranomaiset ja Europol voivat vertailla rikostutkimuksiin liittyviä sormenjälkiä Eurodacin sormenjälkitietoihin mutta vain terrorismirikosten ja muiden vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi. Koska Eurodac on tarkoitettu välineeksi, jolla tuetaan EU:n turvapaikkapolitiikan täytäntöönpanoa, eikä lainvalvontavälineeksi, lainvalvontaviranomaiset voivat päästä

882 Ks. Euroopan tietosuojavaltuutetun (englanninkielinen) verkkosivusto Eurodacista.

883 Neuvoston asetus (EY) N:o 2725/2000, annettu 11 päivänä joulukuuta 2000, Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten Dublinin yleissopimuksen tehokkaaksi soveltamiseksi, EYVL 2000, L 316; neuvoston asetus (EY) N:o 407/2002, annettu 28 päivänä helmikuuta 2002, tietyistä säännöistä Eurodac-järjestelmän perustamisesta sormenjälkien vertailemista varten Dublinin yleissopimuksen tehokkaaksi soveltamiseksi annetun asetuksen (EY) N:o 2725/2000 täytäntöönpanemiseksi, EYVL 2002, L 62 (Eurodac-asetukset), Euroopan parlamentin ja neuvoston asetus (EU) N:o 603/2013, annettu 26 päivänä kesäkuuta 2013, Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013 tehokkaaksi soveltamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä sekä vapauden, turvallisuuden ja oikeuden alueen laaja-alaisten tietojärjestelmien operatiivisesta hallinnoinnista vastaavan eurooppalaisen viraston perustamisesta annetun asetuksen (EU) N:o 1077/2011 muuttamisesta, EUVL 2013, L 180, s. 1 (uudelleenlaadittu Eurodac-asetus).

884 Euroopan parlamentin ja neuvoston asetus (EU) N:o 604/2013, annettu 26 päivänä kesäkuuta 2013, kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta, EUVL 2013, L 180 (Dublin III -asetus).

885 Uudelleenlaadittu Eurodac-asetus, EUVL 2013, L 180, s. 1, 1 artiklan 1 kohta.

tietokantaan vain erityistapauksissa, erityistilanteissa ja tiukoin edellytyksin.[886] Lainvalvontatarkoituksissa tehtyyn myöhempään tietojen käyttöön sovelletaan poliisi- ja rikosoikeusviranomaisia koskevaa tietosuojadirektiiviä, kun taas tietojen käyttö päätarkoitukseen eli Dublin III -asetuksen soveltamisen helpottamiseksi on suojattu yleisellä tietosuoja-asetuksella. Henkilötietoja, jotka jäsenvaltio tai Europol saa uudelleenlaaditun Eurodac-asetuksen nojalla, ei saa siirtää kolmansille maille, kansainvälisille järjestöille tai unioniin tai sen ulkopuolelle sijoittautuneille yksityisille yhteisöille[887].

Eurodac koostuu tietotekniikkaviraston hallinnoimasta keskusyksiköstä, joka on tarkoitettu sormenjälkien tallentamiseen ja vertailemiseen, sekä jäsenvaltioiden ja keskustietokannan välisestä sähköisestä tiedonsiirtojärjestelmästä. Jäsenvaltiot ottavat sormenjäljet ja siirtävät keskusyksikköön tiedot niistä kaikilta vähintään 14-vuotiailta EU:n ulkopuolisten maiden kansalaisilta ja kansalaisuudettomilta henkilöiltä, jotka hakevat turvapaikkaa niiden alueella tai jotka pidätetään maan ulkorajojen luvattoman ylittämisen takia. Jäsenvaltiot voivat myös ottaa sormenjälkiä EU:n ulkopuolisten maiden kansalaisilta ja kansalaisuudettomilta henkilöiltä, jotka on tavattu oleskelemasta luvattomasti niiden alueelta, ja siirtää tiedot keskusyksikköön.

Vaikka kaikki jäsenvaltiot voivat tehdä hakuja Eurodaciin ja pyytää vertailemaan sormenjälkitietoja, vain sormenjäljet ottaneella ja tiedot niistä keskusjärjestelmään siirtäneellä jäsenvaltiolla on oikeus muuttaa tietoja oikaisemalla tai täydentämällä niitä tai poistamalle ne[888]. Tietotekniikkavirasto pitää kirjaa kaikista tietojenkäsittelytoimista tietosuojan seuraamiseksi ja tietoturvallisuuden varmistamiseksi[889]. Kansallisten valvontaviranomaisten on autettava ja neuvottava rekisteröityjä näiden oikeuksien käytössä[890]. Sormenjälkitietojen keräämiseen ja siirtämiseen sovelletaan kansallisten tuomioistuinten laillisuusvalvontaa[891]. EU:n toimielinten tietosuoja-asetusta[892] ja Euroopan tietosuojavaltuutetun harjoittamaa valvontaa sovelletaan keskusjärjestelmän käsittelytoimiin. Tietotekniikkavirasto hallinnoi sitä Eurodacin

886 *Ibid.*, 1 artiklan 2 kohta.

887 *Ibid.*, 35 artikla.

888 *Ibid.*, 27 artikla.

889 *Ibid.*, 28 artikla.

890 *Ibid.*, 29 artikla.

891 *Ibid.*, 29 artikla.

892 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta, EYVL 2001, L 8.

osalta.[893] Jos henkilölle aiheutuu vahinkoa lainvastaisesta tietojenkäsittelystä tai siitä, ettei jokin teko ole Eurodac-asetuksen mukainen, henkilöllä on oikeus saada vahingosta vastuussa olevalta jäsenvaltiolta korvaus aiheutuneesta vahingosta[894]. On kuitenkin korostettava, että turvapaikanhakijat ovat erityisen haavoittuvassa asemassa oleva ryhmä, ja he ovat usein tehneet pitkän ja vaarallisen matkan. Heidän haavoittuvuutensa ja usein epävarma tilanteensa turvapaikkahakemuksen käsittelyn aikana voi käytännössä vaikeuttaa heidän oikeuksiensa, myös korvausoikeuden, käyttämistä.

Eurodacin käyttämiseksi lainvalvontatarkoituksiin jäsenvaltioiden on nimitettävä viranomaiset, joilla on oikeus pyytää pääsyä siihen, sekä viranomaiset, jotka tarkistavat, että vertailupyynnöt ovat lainmukaisia[895]. Kansallisten viranomaisten ja Europolin pääsyyn Eurodacin sormenjälkitietokantaan sovelletaan erittäin tiukkoja ehtoja. Pyynnön esittävän viranomaisen on esitettävä perusteltu sähköinen pyyntö vasta sen jälkeen, kun tietoja on vertailtu muiden käytettävissä olevien tietojärjestelmien, kuten kansallisten sormenjälkitietokantojen ja VIS-järjestelmän, tietojen kanssa. Vertailu katsotaan oikeasuhteiseksi, jos se on ylivoimaisen tärkeä yleisen turvallisuuden kannalta. Vertailun on oltava ehdottoman tarpeen, sen on liityttävä tiettyyn tapaukseen, ja on oltava perusteltuja syitä olettaa, että vertailu edistää merkittävästi jonkin kyseessä olevan rikoksen torjuntaa, havaitsemista tai tutkimista erityisesti silloin, kun on perusteltu epäily siitä, että terrorismirikoksesta tai muusta vakavasta rikoksesta epäilty henkilö, tällaiseen rikokseen syyllistynyt henkilö tai tällaisen rikoksen uhri kuuluu ryhmään, jolta otetaan sormenjäljet Eurodac-järjestelmässä. Vertailu on tehtävä vain sormenjälkitiedoilla. Europolin on myös saatava sormenjäljet ottaneen jäsenvaltion suostumus.

Turvapaikanhakijoihin liittyviä henkilötietoja säilytetään Eurodacissa kymmenen vuotta siitä päivästä lähtien, jolloin sormenjäljet on otettu, paitsi jos rekisteröity saa jonkin EU:n jäsenvaltion kansalaisuuden. Silloin tiedot on välittömästi poistettava. Ulkorajan luvattoman ylittämisen takia pidätettyjen ulkomaalaisten tietoja säilytetään 18 kuukautta. Nämä tiedot on poistettava välittömästi, jos rekisteröity saa oleskeluluvan, poistuu EU:n alueelta tai saa jäsenvaltion kansalaisuuden. Turvapaikan saaneiden henkilöiden tiedot pysyvät käytettävissä terrorismirikosten ja muiden

893 Uudelleenlaadittu Eurodac-asetus, EUVL 2013, L 180, s. 1, 31 artikla.

894 *Ibid.*, 37 artikla.

895 Roots, L. (2015), "The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies Tallinn University of Technology*, nide 5, nro 2, s. 108–129.

vakavien rikosten torjumiseksi, havaitsemiseksi ja tutkimiseksi tehtävää vertailua varten kolme vuotta.

Kaikkien EU:n jäsenvaltioiden lisäksi myös Islanti, Norja, Liechtenstein ja Sveitsi käyttävät Eurodacia kansainvälisten sopimusten pohjalta.

Eurodacin valvonnan varmistamiseksi on perustettu Eurodacin valvonnan koordinointiryhmä. Siinä on edustajat Euroopan tietosuojavaltuutetusta ja kansallisista valvontaviranomaisista, ja se kokoontuu kahdesti vuodessa. Ryhmässä on edustajat 28:sta EU:n jäsenvaltiosta sekä Islannista, Liechtensteinista, Norjasta ja Sveitsistä.[896]

Tulevaisuudennäkymät

Euroopan komissio antoi toukokuussa 2016 ehdotuksen Eurodac-asetuksen uudelleenlaadinnasta osana uudistusta, jonka tarkoituksena on parantaa Euroopan yhteisen turvapaikkajärjestelmän toimintaa[897]. Ehdotettu uudelleenlaadinta on tärkeä, koska se laajentaa huomattavasti alkuperäisen Eurodac-tietokannan soveltamisalaa. Eurodac perustettiin alun perin tukemaan Euroopan yhteisen turvapaikkajärjestelmän täytäntöönpanoa tarjoamalla sormenjälkitietoja, joiden avulla voidaan määrittää, mikä jäsenvaltio on vastuussa EU:ssa jätetyn turvapaikkahakemuksen tutkimisesta. Ehdotetulla uudelleenlaadinnalla laajennetaan tietokannan soveltamisalaa, jotta laittomien siirtolaisten palauttamista voidaan helpottaa.[898] Kansalliset viranomaiset pystyvät tekemään tietokannasta hakuja laittomasti EU:ssa oleskelevien tai laittomasti EU:hun saapuneiden kolmansien maiden kansalaisten tunnistamiseksi, jotta saadaan näyttöä, joka auttaa jäsenvaltioita näiden henkilöiden palauttamisessa. Lisäksi tällä hetkellä voimassa olevissa oikeudellisissa järjestelmissä vaaditaan vain sormenjälkitietojen keräämistä ja tallentamista, mutta ehdotuksen

896 Ks. Euroopan tietosuojavaltuutetun (englanninkielinen) verkkosivusto Eurodacista.

897 Euroopan komissio, ehdotus Euroopan parlamentin ja neuvoston asetukseksi Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten [kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013] tehokkaaksi soveltamiseksi, laittomasti oleskelevan kolmannen maan kansalaisen tai kansalaisuudettoman henkilön tunnistamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä (uudelleenlaadittu), COM(2016) 272 final, 4.5.2016.

898 Ks. ehdotuksen perustelut, s. 3.

mukaan aletaan kerätä henkilöiden kasvokuvia[899], jotka ovat toinen biometristen tunnisteiden muoto. Ehdotuksella myös alennettaisiin niiden lasten vähimmäisikää, joilta biometrisiä tietoja voidaan kerätä – kuuteen vuoteen[900] 14 vuodesta, joka on vuoden 2013 asetuksessa vähimmäisikä. Ehdotuksen soveltamisalan laajentaminen merkitsee puuttumista entistä useampien sellaisten yksilöiden yksityiselämän suojaa ja tietosuojaa koskeviin oikeuksiin, joiden tiedot voivat olla tietokannassa. Tämän puuttumisen vastapainoksi ehdotuksessa ja Euroopan parlamentin LIBE-valiokunnan siihen ehdottamissa tarkistuksissa[901] pyritään vahvistamaan tietosuojavaatimuksia. Käsikirjaa laadittaessa ehdotusta käsiteltiin parlamentissa ja neuvostossa.

Eurosur

Euroopan rajavalvontajärjestelmän (Eurosur)[902] tarkoituksena on tukea Schengen-alueen ulkorajojen valvontaa havaitsemalla, estämällä ja torjumalla laitonta maahanmuuttoa ja rajatylittävää rikollisuutta. Se tehostaa tiedonvaihtoa ja operatiivista yhteistyötä kansallisten koordinointikeskusten ja Frontexin, uuden yhdennetyn rajaturvallisuuden periaatteen kehittämisestä ja soveltamisesta vastaavan EU-viraston[903], välillä. Sen yleiset tavoitteet ovat

899 Euroopan komissio, ehdotus Euroopan parlamentin ja neuvoston asetukseksi Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten [kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013] tehokkaaksi soveltamiseksi, laittomasti oleskelevan kolmannen maan kansalaisen tai kansalaisuudettoman henkilön tunnistamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä (uudelleenlaadittu), COM(2016) 272 final, 4.5.2016, 2 artiklan 1 kohta.

900 *Ibid.*, 2 artiklan 2 kohta.

901 Euroopan parlamentti, *mietintö ehdotuksesta Euroopan parlamentin ja neuvoston asetukseksi Eurodac-järjestelmän perustamisesta sormenjälkien vertailua varten kolmannen maan kansalaisen tai kansalaisuudettoman henkilön johonkin jäsenvaltioon jättämän kansainvälistä suojelua koskevan hakemuksen käsittelystä vastuussa olevan jäsenvaltion määrittämisperusteiden ja -menettelyjen vahvistamisesta annetun asetuksen (EU) N:o 604/2013 tehokkaaksi soveltamiseksi, laittomasti oleskelevan kolmannen maan kansalaisen tai kansalaisuudettoman henkilön tunnistamiseksi sekä jäsenvaltioiden lainvalvontaviranomaisten ja Europolin esittämistä, Eurodac-tietoihin lainvalvontatarkoituksessa tehtäviä vertailuja koskevista pyynnöistä (uudelleenlaadittu)*, PE 597.620v03-00, 9.6.2017.

902 Euroopan parlamentin ja neuvoston asetus (EU) N:o 1052/2013, annettu 22 päivänä lokakuuta 2013, Euroopan rajavalvontajärjestelmän (Eurosur) perustamisesta, EUVL 2013, L 295.

903 Euroopan parlamentin ja neuvoston asetus (EU) 2016/1624, annettu 14 päivänä syyskuuta 2016, eurooppalaisesta raja- ja merivartiostosta ja Euroopan parlamentin ja neuvoston asetuksen (EU) 2016/399 muuttamisesta sekä Euroopan parlamentin ja neuvoston asetuksen (EY) N:o 863/2007, neuvoston asetuksen (EY) N:o 2007/2004 ja neuvoston päätöksen 2005/267/EY kumoamisesta, EUVL L 251.

- EU:hun laittomasti päässeiden maahanmuuttajien määrän vähentäminen
- laittomien maahanmuuttajien kuolemantapausten määrän vähentäminen pelastamalla ihmisiä merellä
- sisäisen turvallisuuden parantaminen koko EU:ssa ehkäisemällä rajatylittävää rikollisuutta[904].

Eurosur-järjestelmä otettiin käyttöön 2. joulukuuta 2013 kaikissa jäsenvaltioissa, joilla on ulkorajoja, ja muissa jäsenvaltioissa 1. joulukuuta 2014. Asetusta sovelletaan jäsenvaltioiden maaulkorajojen, meriulkorajojen ja ilmaulkorajojen valvontaan. Eurosur-järjestelmässä vaihdetaan ja käsitellään hyvin rajoitetusti henkilötietoja, koska jäsenvaltioilla ja Frontexilla on oikeus vaihtaa vain laivojen tunnistenumeroita. Eurosurissa vaihdetaan operatiivisia tietoja, kuten partioiden ja erityistapahtumien paikkoja, ja yleisesti ottaen vaihdettavat tiedot eivät voi sisältää henkilötietoja.[905] Jos henkilötietoja poikkeuksellisesti vaihdetaan Eurosur-järjestelmässä, asetuksessa säädetään, että tietosuojaa koskevaa EU:n yleistä säännöstöä sovelletaan täysimääräisesti[906].

Eurosurissa varmistetaan näin ollen tietosuoja toteamalla, että henkilötietojen vaihdoissa on noudatettava poliisi- ja rikosoikeusviranomaisia koskevassa tietosuojadirektiivissä ja yleisessä tietosuoja-asetuksessa esitettyjä vaatimuksia ja suojatoimia[907].

904 Ks. myös Euroopan komissio (2008), *komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Euroopan rajavalvontajärjestelmän (Eurosur) luomisesta*, COM(2008) 68 final, Bryssel, 13.2.2008; Euroopan komissio (2011), *Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur),* komission yksilöiden valmisteluasiakirja, SEC(2011) 1536 final, Bryssel, 12.12.2011, s. 18.

905 Euroopan komissio, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29.11.2013.

906 Asetus (EU) N:o 1052/2013, johdanto-osan 13 kappale ja 13 artikla.

907 *Ibid.*, johdanto-osan 13 kappale ja 13 artikla.

Tullitietojärjestelmä

Toinen tärkeä EU:n tasolla käyttöön otettu yhteinen tietojärjestelmä on tullitietojärjestelmä (TTJ).[908] Sisämarkkinoiden perustamisen yhteydessä poistettiin kaikki tavaroiden liikkumiseen EU:n alueella kohdistuneet tarkastukset ja muodollisuudet, mikä kasvatti petosten riskiä. Riskin vastapainoksi tehostettiin jäsenvaltioiden tullihallintojen välistä yhteistyötä. TTJ:n tavoitteena on auttaa jäsenvaltioita kansallisen ja EU:n tulli- ja maatalouslainsäädännön vakavien rikkomisten estämisessä, tutkinnassa ja syytteeseenpanossa. TTJ on perustettu kahdella säädöksellä, joilla on eri oikeusperustat: Neuvoston asetus (EY) N:o 515/97 koskee eri kansallisten hallintoviranomaisten yhteistyötä petosten torjumiseksi tulliliiton ja yhteisen maatalouspolitiikan yhteydessä, ja neuvoston päätöksen 2009/917/YOS tavoitteena on auttaa tullilainsäädännön vakavien rikkomisten estämisessä, tutkinnassa ja syytteeseenpanossa. Tämä tarkoittaa, että TTJ:ssä ei ole kyse pelkästään lainvalvonnasta.

TTJ:n sisältämiin tietoihin kuuluu henkilötietoja, jotka liittyvät tuotteisiin, kuljetusvälineisiin, yrityksiin, henkilöihin sekä pidätettyihin, takavarikoituihin tai menetetyksi tuomittuihin tavaroihin ja käteisvaroihin. Käsiteltävät tietoryhmät on määritelty selkeästi. Niitä ovat kyseessä olevan henkilön nimet, kansalaisuus, sukupuoli, syntymäpaikka ja -aika, peruste tietojen tallentamiselle järjestelmään ja kuljetusvälineen rekisterinumero.[909] Näitä tietoja voidaan käyttää ainoastaan tullisäännösten rikkomisesta epäiltyjen henkilöiden havainnointia, ilmoittamista tai erityistarkastuksia sekä strategista tai operatiivista analyysia varten.

TTJ:n tietoihin pääsevät vain kansalliset tulli-, vero-, maatalous-, kansanterveys- ja poliisiviranomaiset sekä Europol ja Eurojust.

Henkilötietojen käsittelyssä on noudatettava asetuksella (EY) N:o 515/97 ja neuvoston päätöksellä 2009/917/YOS vahvistettuja sekä yleisen tietosuoja-asetuksen, EU:n toimielinten tietosuoja-asetuksen, uudistetun yleissopimuksen 108 ja poliisiasioita koskevan suosituksen säännöksiä ja määräyksiä. Euroopan tietosuojavaltuutettu

908 Euroopan unionin neuvosto (1995), neuvoston säädös, annettu 26 päivänä heinäkuuta 1995 tietotekniikan käyttöä tullialalla koskevan yleissopimuksen tekemisestä, EYVL 1995, C 316, sellaisena kuin se on muutettuna jäsenvaltioiden hallintoviranomaisten keskinäisestä avunannosta sekä jäsenvaltioiden hallintoviranomaisten ja komission yhteistyöstä tulli- ja maatalousasioita koskevan lainsäädännön moitteettoman soveltamisen varmistamiseksi 13 päivänä maaliskuuta 1997 annetulla neuvoston asetuksella (EY) N:o 515/97, Euroopan unionin neuvosto (2009); neuvoston päätös 2009/917/YOS, tehty 30 päivänä marraskuuta 2009, tietotekniikan käytöstä tullialalla, EUVL 2009, L 323 (TTJ-päätös).

909 Ks. TTJ-päätös, 24, 25 ja 28 artikla.

valvoo, että TTJ:n tietojen käsittelyssä noudatetaan asetusta (EY) N:o 45/2001. Euroopan tietosuojavaltuutettu järjestää vähintään kerran vuodessa tapaamisen kaikkien niiden kansallisten tietosuojaviranomaisten kanssa, jotka ovat toimivaltaisia valvomaan TTJ:ään liittyviä asioita.

EU:n tietojärjestelmien välinen yhteentoimivuus

Muuttoliikkeen hallinta, EU:n ulkorajojen yhdennetty rajaturvallisuus ja terrorismin ja rajatylittävän rikollisuuden torjunta aiheuttavat suuria haasteita ja ovat monimutkaistuneet entisestään globalisoituneessa maailmassa. EU on viime vuosina tehnyt työtä sellaisen uuden kattavan toimintamallin luomiseksi, jolla voidaan taata turvallisuus ja ylläpitää sitä vaarantamatta EU:n arvoja ja perusvapauksia. Näissä toimenpiteissä on keskeistä, että tietoja voidaan vaihtaa tehokkaasti kansallisten lainvalvontaviranomaisten kesken ja jäsenvaltioiden ja asiaankuuluvien EU:n virastojen välillä.[910] EU:n nykyisissä rajaturvallisuutta ja sisäistä turvallisuutta käsittelevissä tietojärjestelmissä on kullakin omat tavoitteensa, institutionaalinen rakenteensa, rekisteröitynsä ja käyttäjänsä. EU on pyrkinyt korjaamaan puutteita, jotka liittyvät EU:n tiedonhallinnan hajanaisuuteen eri tietojärjestelmien, kuten SIS II:n, VIS:n ja Eurodacin, välillä, selvittämällä mahdollisuuksia yhteentoimivuuteen.[911] Päätavoitteena on varmistaa, että toimivaltaisilla poliisi-, tulli- ja oikeusviranomaisilla on järjestelmällisesti käytössään kaikki tehtäviensä suorittamiseen tarvittavat tiedot ja että samalla säilytetään yksityisyyden suojaa ja tietosuojaa koskevien oikeuksien ja muiden perusoikeuksien kunnioittamista koskeva tasapaino.

910 Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille ja neuvostolle: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi, COM(2016) 205 final, Bryssel, 6.4.2016, Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle ja neuvostolle: Lisää turvallisuutta liikkuvuuden maailmassa: parannuksia tiedonvaihtoon terrorismin torjumiseksi ja vahvemmat ulkorajat, COM(2016) 602 final, Bryssel, 14.9.2016, Euroopan komissio (2016), ehdotus Euroopan parlamentin ja neuvoston asetukseksi Schengenin tietojärjestelmän käytöstä laittomasti oleskelevien kolmansien maiden kansalaisten palauttamisessa. Ks. myös komission tiedonanto Euroopan parlamentille, Eurooppa-neuvostolle ja neuvostolle: Seitsemäs raportti edistymisestä kohti toimivaa ja todellista turvallisuusunionia, COM(2017) 261 final, Bryssel, 16.5.2017.

911 Euroopan unionin neuvosto (2005), Haagin ohjelma: vapauden, turvallisuuden ja oikeuden lujittaminen Euroopan unionissa, EUVL 2005, C 53, Euroopan komissio (2010), komission tiedonanto Euroopan parlamentille ja neuvostolle: Katsaus tiedonhallintaan vapauden, turvallisuuden ja oikeuden alueella, COM(2010) 385 final, Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille ja neuvostolle: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi, COM(2016) 205 final, Bryssel, 6.4.2016, Euroopan komissio (2016), komission päätös, annettu 17 päivänä kesäkuuta 2016, tietojärjestelmiä ja niiden yhteentoimivuutta käsittelevän korkean tason asiantuntijaryhmän perustamisesta, EUVL 2016, C 257.

Yhteentoimivuudella tarkoitetaan ”mahdollisuutta vaihtaa ja jakaa tietoja tietojärjestelmien välillä”[912]. Tällä vaihdolla ei saa heikentää tietoihin pääsyä ja niiden käyttöä koskevia välttämättömän tiukkoja sääntöjä, jotka on taattu yleisessä tietosuoja-asetuksessa, poliisi- ja rikosoikeusviranomaisia koskevassa tietosuojadirektiivissä, EU:n perusoikeuskirjassa ja kaikissa muissa asiaankuuluvissa säännöissä. Mikään yhdennetty tiedonhallintajärjestelmä ei saa vaikuttaa käyttötarkoituksen rajoittamisen periaatteeseen, sisäänrakennettuun tietosuojaan tai oletusarvoiseen tietosuojaan[913].

Näiden kolmen keskeisen tietojärjestelmän – SIS II, VIS ja Eurodac – toimintojen parantamisen lisäksi komissio on ehdottanut neljännen keskitetyn kolmansien maiden kansalaisia käsittelevän rajavalvontajärjestelmän, rajanylitystietojärjestelmän (EES)[914], perustamista. Järjestelmä oli määrä ottaa käyttöön vuoteen 2020 mennessä.[915] Komissio on myös antanut ehdotuksen Euroopan matkustustieto- ja -lupajärjestelmän (ETIAS) perustamisesta[916]. Tässä järjestelmässä kerätään tietoa matkustajista, jotka eivät tarvitse viisumia EU:hun, jotta voidaan edistää tarkastuksia laittomasta maahantulosta sekä turvallisuustarkastuksia.

912 Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille ja neuvostolle: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi, COM(2016) 205 final, Bryssel, 6.4.2016, s. 14.

913 *Ibid.*, s. 4–5.

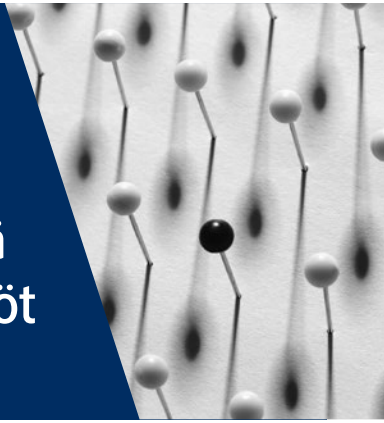
914 Euroopan komissio (2016), ehdotus Euroopan parlamentin ja neuvoston asetukseksi rajanylitystietojärjestelmän (EES) perustamisesta Euroopan unionin jäsenvaltioiden ulkorajat ylittävien kolmansien maiden kansalaisten maahantuloa, maastalähtöä ja pääsyn epäämistä koskevien tietojen rekisteröimiseksi ja edellytysten määrittämisestä pääsylle EES:n tietoihin lainvalvontatarkoituksissa sekä asetuksen (EY) N:o 767/2008 ja asetuksen (EU) N:o 1077/2011 muuttamisesta, COM(2016) 194 final, Bryssel, 6.4.2016.

915 Euroopan komissio (2016), komission tiedonanto Euroopan parlamentille ja neuvostolle: Vahvemmat ja älykkäämmät tietojärjestelmät rajaturvallisuuden ja sisäisen turvallisuuden tueksi, COM(2016) 205 final, Bryssel, 6.4.2016, s. 5.

916 Euroopan komissio (2016), ehdotus Euroopan parlamentin ja neuvoston asetukseksi EU:n matkustustieto- ja -lupajärjestelmän (ETIAS) perustamisesta ja asetusten (EU) No 515/2014, (EU) 2016/399, (EU) 2016/794 ja (EU) 2016/1624 muuttamisesta, COM(2016) 731 final, 16.11.2016.

9

Erityiset tietotyypit ja niitä koskevat tietosuojasäännöt



EU	Käsiteltävät asiat	EN
Yleinen tietosuoja-asetus Sähköisen viestinnän tietosuojadirektiivi	**Sähköinen viestintä**	Uudistettu yleissopimus 108 Televiestintäpalveluja koskeva suositus
Yleinen tietosuoja-asetus, 88 artikla	**Työelämän suhteet**	Uudistettu yleissopimus 108 Työelämää koskeva suositus EIT, *Copland v. Yhdistynyt kuningaskunta*, nro 62617/00, 2007
Yleinen tietosuoja-asetus, 9 artiklan 2 kohdan h ja i alakohta	**Lääketieteelliset tiedot**	Uudistettu yleissopimus 108 Lääketieteellisiä tietoja koskeva suositus EIT, *Z v. Suomi*, nro 22009/93, 1997
Kliinisiä tutkimuksia koskeva asetus	**Kliiniset tutkimukset**	
Yleinen tietosuoja-asetus, 6 artiklan 4 kohta ja 89 artikla	**Tilastotiedot**	Uudistettu yleissopimus 108 Tilastotietoja koskeva suositus
Asetus (EY) N:o 223/2009 Euroopan tilastoista EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 2008	**Viralliset tilastot**	Uudistettu yleissopimus 108 Tilastotietoja koskeva suositus

EU	Käsiteltävät asiat	EN
Direktiivi 2014/65/EU rahoitusvälineiden markkinoista Asetus (EU) N:o 648/2012 OTC-johdannaisista, keskusvastapuolista ja kauppatietorekistereistä Asetus (EY) N:o 1060/2009 luottoluokituslaitoksista Direktiivi 2007/64/EY maksupalveluista sisämarkkinoilla	**Rahataloudelliset tiedot**	Uudistettu yleissopimus 108 Maksutapahtumia ja niihin liittyviä toimintoja koskeva suositus 90 (19) EIT, *Michaud v. Ranska*, nro 12323/11, 2012

Monin paikoin on Euroopan tasolla hyväksytty erityisiä oikeudellisia välineitä, joilla uudistetun yleissopimuksen 108 ja yleisen tietosuoja-asetuksen yleisiä sääntöjä sovelletaan yksityiskohtaisemmin tarkoin määritellyillä aloilla.

9.1 Sähköinen viestintä

Keskeiset kohdat

- Euroopan neuvoston vuonna 1995 antama suositus sisältää erityisiä tietosuojasääntöjä televiestintää ja etenkin puhelinpalveluja varten.
- Viestintäpalveluihin EU:n tasolla liittyvää henkilötietojen käsittelyä säännellään sähköisen viestinnän tietosuojadirektiivillä.
- Sähköisen viestinnän luottamuksellisuus ei kata ainoastaan viestinnän sisältöä vaan myös metatiedot, kuten tiedon viestinnän osapuolista, ajankohdasta ja kestosta, ja paikannustiedot, kuten sen, mistä tiedot ovat peräisin.

Viestintäverkoissa on tavallista suurempi riski siitä, että käyttäjien oikeuteen nauttia yksityisyyden suojaa puututaan perusteettomasti, koska niissä tapahtuvan viestinnän kuunteluun ja seurantaan on paljon teknisiä mahdollisuuksia. Siksi on katsottu tarpeelliseksi antaa erityisiä tietosuoja-asetuksia, joilla torjutaan viestintäpalvelujen käyttäjille aiheutuvia riskejä.

Euroopan neuvosto antoi vuonna 1995 suosituksen henkilötietojen suojasta televiestintäpalveluiden alalla ja erityisesti puhelinpalveluiden alalla[917]. Suosituksen

917 Euroopan neuvosto, ministerikomitea (1995), suositus Rec(95)4 henkilötietojen suojasta televiestintäpalveluiden alalla ja erityisesti puhelinpalveluiden alalla, 7.2.1995.

mukaan henkilötietoja tulisi televiestinnän alalla kerätä ja käsitellä ainoastaan seuraaviin tarkoituksiin: käyttäjän yhdistäminen verkkoon, tietyn televiestintäpalvelun tarjoaminen käyttöön, laskutus, varmennus, tekniikan mahdollisimman hyvän toiminnan varmistaminen sekä verkon ja palvelun kehittäminen.

Televiestintäverkkojen käyttöön suoramarkkinoinnissa kiinnitettiin myös erityistä huomiota. Yleissääntönä on, että suoramarkkinointiviestejä ei saa lähettää tilaajalle, joka on tehnyt selväksi, että hän ei halua vastaanottaa mainosviestejä. Automaattisia soittolaitteita, jotka lähettävät valmiiksi tallennettuja viestejä, voidaan käyttää vain, jos tilaaja on nimenomaisesti antanut suostumuksensa. Kansallisessa lainsäädännössä säädetään alalla sovellettavista yksityiskohtaisista säännöistä.

EU:n oikeudellisessa kehyksessä sähköisen viestinnän tietosuojadirektiiviä ehdotettiin ensimmäisen kerran vuonna 1997, se hyväksyttiin vuonna 2002, ja sitä muutettiin vuonna 2009. Se tehtiin aiemman tietosuojadirektiivin säännösten täydentämiseksi ja täsmentämiseksi televiestinnän osalta.[918]

Sähköisen viestinnän tietosuojadirektiiviä sovelletaan ainoastaan julkisissa sähköisissä verkoissa tarjottaviin viestintäpalveluihin.

Sähköisen viestinnän tietosuojadirektiivissä on jaettu viestinnän aikana tuotetut tiedot kolmeen pääluokkaan:

- viestinnän aikana lähetettyjen viestien sisällön muodostavat tiedot, jotka ovat täysin luottamuksellisia
- viestinnän muodostamiseen ja ylläpitämiseen tarvittavat tiedot – niin sanotut metatiedot eli direktiivissä tarkoitetut ”liikennetiedot” – kuten tiedot viestinnän osapuolista, ajankohdasta ja kestosta
- metatietojen osana tiedot, jotka liittyvät viestintävälineen sijaintiin, eli niin sanotut paikkatiedot; nämä tiedot kertovat myös viestintälaitteiden käyttäjien

918 Euroopan parlamentin ja neuvoston direktiivi 2002/58/EY, annettu 12 päivänä heinäkuuta 2002, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla (sähköisen viestinnän tietosuojadirektiivi), EYVL 2002, L 201, sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY muuttamisesta ja Euroopan parlamentin ja neuvoston asetus (EY) N:o 2006/2004, annettu 27 päivänä lokakuuta 2004, kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä, EUVL 2009, L 337.

sijainnin, ja ne ovat erityisen tärkeitä kannettavien viestintälaitteiden käyttäjien osalta.

Palvelun tarjoaja voi käyttää liikennetietoja ainoastaan laskutusta ja palvelun teknistä tarjoamista varten. Rekisteröidyn suostumuksella nämä tiedot voidaan kuitenkin luovuttaa muille rekisterinpitäjille, jotka tarjoavat lisäarvopalveluja, kuten kertovat käyttäjälle lähimmän metroaseman tai apteekin tai kyseisen alueen sääennusteen.

Kaiken muun sähköisissä verkoissa tapahtuvaa viestintää koskevan tiedon käytön on sähköisen viestinnän tietosuojadirektiivin 15 artiklan nojalla täytettävä ihmisoikeussopimuksen 8 artiklan 2 kohdassa asetetut ja perusoikeuskirjan 8 ja 52 artiklassa vahvistetut vaatimukset oikeutetulle puuttumiselle henkilön tietosuojaan. Kyse voi olla esimerkiksi rikostutkinnasta.

Sähköisen viestinnän tietosuojadirektiiviin vuonna 2009 tehdyillä muutoksilla[919] direktiiviin lisättiin seuraavat säännöt:

- Sähköpostiviestien lähettämistä suoramarkkinointitarkoituksiin koskevat rajoitukset ulotettiin kattamaan tekstiviesti- ja multimediaviestipalvelut sekä muut vastaavat sovellukset. Markkinointisähköpostiviestit ovat kiellettyjä ilman ennalta saatua suostumusta. Ilman ennakkosuostumusta markkinointisähköpostiviestejä voidaan lähettää vain aiemmille asiakkaille, jos he ovat antaneet sähköpostiosoitteensa saataville eivätkä vastusta sitä.

- Jäsenvaltiot velvoitettiin varmistamaan oikeussuojakeinot tilanteisiin, joissa ei-toivotun viestinnän kieltoa rikotaan[920].

- Evästeiden, eli tietokoneen käyttäjän toimia seuraavien ja tallentavien ohjelmistojen, asentaminen ilman tietokoneen käyttäjän lupaa kiellettiin. Kansallisessa

919 Euroopan parlamentin ja neuvoston direktiivi 2009/136/EY, annettu 25 päivänä marraskuuta 2009, yleispalvelusta ja käyttäjien oikeuksista sähköisten viestintäverkkojen ja -palvelujen alalla annetun direktiivin 2002/22/EY, henkilötietojen käsittelystä ja yksityisyyden suojasta sähköisen viestinnän alalla annetun direktiivin 2002/58/EY ja kuluttajansuojalainsäädännön täytäntöönpanosta vastaavien kansallisten viranomaisten yhteistyöstä annetun asetuksen (EY) N:o 2006/2004 muuttamisesta, EUVL 2009, L 337.

920 Ks. muutettu direktiivi, 13 artikla.

lainsäädännössä tulisi yksityiskohtaisesti määritellä, miten suostumus annetaan riittävän suojan varmistamiseksi.[921]

Jos luvaton käyttö tai tietojen häviäminen tai tuhoaminen aiheuttaa tietoturvaloukkauksen, asiasta on välittömästi ilmoitettava toimivaltaiselle valvontaviranomaiselle. Tilaajille on kerrottava, jos tietoturvaloukkauksesta saattaa aiheutua heille vahinkoa.[922]

Tietojen säilyttämistä koskeva direktiivi[923] velvoitti viestintäpalvelujen tarjoajat pitämään metatiedot saatavilla. Unionin tuomioistuin kuitenkin kumosi tämän direktiivin (lisätietoa on 8.3 kohdassa).

Tulevaisuudennäkymät

Euroopan komissio antoi tammikuussa 2017 uuden ehdotuksen sähköisen viestinnän tietosuoja-asetuksesta, jolla korvattaisiin vanha sähköisen viestinnän tietosuojadirektiivi. Tavoitteena olisi edelleen ”luonnollisten henkilöiden ja oikeushenkilöiden perusoikeuksien ja -vapauksien suojelu [...] sähköisten viestintäpalvelujen tarjoamisessa ja käytössä, mukaan lukien erityisesti oikeudet yksityiselämän ja viestien kunnioittamiseen ja luonnollisten henkilöiden suojelu henkilötietojen käsittelyssä”. Uudella ehdotuksella on lisäksi määrä varmistaa sähköisen viestinnän tietojen ja sähköisten viestintäpalvelujen vapaa liikkuvuus unionissa.[924] Kun yleisessä tietosuoja-asetuksessa käsitellään pääasiassa EU:n perusoikeuskirjan 8 artiklaa, ehdotetun asetuksen tavoitteena on sisällyttää perusoikeuskirjan 7 artikla EU:n sekundäärilainsäädäntöön.

Asetuksella mukautettaisiin aiemman direktiivin säännöksiä uusiin teknologioihin ja markkinarealiteetteihin ja rakennettaisiin kattava ja yleisen tietosuoja-asetuksen kanssa yhdenmukainen kehys. Tässä mielessä sähköisen viestinnän

921 Ks. *Ibid.*, 5 artikla; ks. myös tietosuojatyöryhmä (2012), *lausunto 04/2012 evästeisiin liittyvää suostumusta koskevasta vapautuksesta*, WP 194, Bryssel, 7.6.2012.

922 Ks. myös tietosuojatyöryhmä (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Bryssel, 5.4.2011.

923 Euroopan parlamentin ja neuvoston direktiivi 2006/24/EY, annettu 15 päivänä maaliskuuta 2006, yleisesti saatavilla olevien sähköisten viestintäpalvelujen tai yleisten viestintäverkkojen yhteydessä tuotettavien tai käsiteltävien tietojen säilyttämisestä ja direktiivin 2002/58/EY muuttamisesta, EUVL 2006, L 105.

924 Ehdotus Euroopan parlamentin ja neuvoston asetukseksi yksityiselämän kunnioittamisesta ja henkilötietojen suojasta sähköisessä viestinnässä ja direktiivin 2002/58/EY kumoamisesta (sähköisen viestinnän tietosuoja-asetus), COM(2017) 10 final, 1 artikla.

tietosuoja-asetus olisi erityissäädös (lex specialis) suhteessa yleiseen tietosuoja-asetukseen, jota sillä täsmennetään. Uusi asetus koskee ”sähköisen viestinnän tietojen” käsittelyä. Se tarkoittaa muun muassa sähköisen viestinnän sisältöä ja metatietoja, jotka eivät ole välttämättä henkilötietoja. Alueellinen soveltamisala rajoittuu EU:hun myös silloin, kun EU:ssa saatua tietoa käsitellään sen ulkopuolella, ja koskee myös internetin kautta välitettävän viestinnän palveluntarjoajia. Nämä ovat palveluntarjoajia, jotka toimittavat sisältöä, palveluja tai sovelluksia internetissä ilman verkko-operaattorin tai internetpalveluntarjoajan suoraa osallistumista. Tällaisia palveluntarjoajia ovat esimerkiksi Skype (ääni- ja videopuhelut), WhatsApp (viestipalvelu), Google (hakupalvelu), Spotify (musiikkipalvelu) ja Netflix (videosisältö). Yleisen tietosuoja-asetuksen täytäntöönpanomekanismeja sovellettaisiin uuteen asetukseen.

Sähköisen viestinnän tietosuoja-asetus oli määrä hyväksyä ennen 25. toukokuuta 2018, johon mennessä yleistä tietosuoja-asetusta sovelletaan kaikissa 28 jäsenvaltiossa. Se kuitenkin edellyttää sekä Euroopan parlamentin että neuvoston hyväksyntää.[925]

9.2 Työsuhdetta koskevat tiedot

Keskeiset kohdat

- Euroopan neuvoston työelämää koskevassa suosituksessa esitetään erityiset säännöt työelämän suhteita koskevalle tietosuojalle.
- Yleisessä tietosuoja-asetuksessa työsuhdetta käsitellään nimenomaisesti vain arkaluonteisten tietojen käsittelyn yhteydessä.
- Suostumuksen, joka on annettava vapaaehtoisesti, jotta se voisi toimia oikeudellisena perusteena työntekijän tietojen käsittelylle, pätevyys voidaan kyseenalaistaa, kun otetaan huomioon työnantajan ja työntekijöiden välinen taloudellinen epätasapaino. Suostumuksen antamisen olosuhteet on arvioitava huolellisesti.

925 Lisätietoa, ks. Euroopan komissio (2017), ”Komissio ehdottaa korkeatasoisen yksityisyydensuojan varmistavia sääntöjä kaikkeen sähköiseen viestintään ja päivittää EU:n toimielimiä koskevia tietosuojasääntöjä”, lehdistötiedote, 10.1.2017.

Tietojenkäsittelyyn työsuhteen yhteydessä sovelletaan henkilötietojen suojaa koskevaa yleistä EU:n lainsäädäntöä. Yhdessä asetuksessa[926] käsitellään kuitenkin nimenomaisesti EU:n toimielinten suorittaman henkilötietojen käsittelyn suojaa (muun muassa) työsuhteen yhteydessä. Yleisessä tietosuoja-asetuksessa viitataan nimenomaisesti työelämän suhteisiin 9 artiklan 2 kohdassa, jossa todetaan, että henkilötietoja voidaan käsitellä rekisterinpitäjän tai rekisteröidyn velvoitteiden ja erityisten oikeuksien noudattamiseksi työlainsäädännön alalla.

Yleisen tietosuoja-asetuksen mukaan työntekijän pitäisi pystyä erottamaan selkeästi tiedot, joiden käsittelylle/tallentamiselle hän antaa vapaaehtoisesti suostumuksen, ja tarkoitukset, joita varten hänen tietojaan tallennetaan. Työntekijöille pitäisi kertoa heidän oikeuksistaan ja tietojen tallennusajasta ennen kuin suostumus voidaan antaa. Jos henkilötietojen tietoturvaloukkaus todennäköisesti aiheuttaa suuren riskin luonnollisen henkilön oikeuksille ja vapauksille, työnantajan on ilmoitettava loukkauksesta työntekijälle. Asetuksen 88 artiklan nojalla jäsenvaltiot voivat antaa yksityiskohtaisempia sääntöjä työntekijöiden oikeuksien ja vapauksien suojan varmistamiseksi henkilötietojen käsittelyssä työsuhteen yhteydessä.

Esimerkki: Asiassa *Worten*[927] oli kyse tiedoista, joihin kuului työaikarekisteri, joka sisältää päivittäisiä työaikoja ja lepojaksoja, ja nämä tiedot ovat henkilötietoja. Kansallisessa lainsäädännössä voidaan edellyttää, että työnantaja antaa työaikarekisterin kansallisten työsuojeluviranomaisten saataville. Näin asianomaisiin henkilötietoihin pääsisi välittömästi. Henkilötietoihin pääsy on kuitenkin välttämätöntä, jotta kansallinen viranomainen voi valvoa työsuojelulainsäädäntöä.[928]

Euroopan neuvoston työelämää koskeva suositus annettiin vuonna 1989 ja sitä tarkistettiin vuonna 2015[929]. Suositus koskee henkilötietojen käsittelyä työsuhteen hoitamista varten sekä yksityisellä että julkisella sektorilla. Käsittelyssä on noudatettava tiettyjä periaatteita ja rajoituksia, kuten avoimuuden periaatetta ja

926 Euroopan parlamentin ja neuvoston asetus (EY) N:o 45/2001, annettu 18 päivänä joulukuuta 2000, yksilöiden suojelusta yhteisöjen toimielinten ja elinten suorittamassa henkilötietojen käsittelyssä ja näiden tietojen vapaasta liikkuvuudesta (EYVL 2001, L 8).

927 EUT, C-342/12, *Worten – Equipamentos para o Lar SA vastaan Autoridade para as Condições de Trabalho (ACT)*, 30.5.2013, 19 kohta.

928 *Ibid.*, 43 kohta.

929 Euroopan neuvosto, ministerikomitea (2015), suositus Rec(2015)5, jäsenvaltioille henkilötietojen käsittelystä työsuhteen yhteydessä, huhtikuuta 2015.

työntekijöiden edustajien kuulemista ennen valvontalaitteiden asettamista työpaikalle. Suosituksessa myös todetaan, että työnantajien olisi käytettävä ennalta ehkäiseviä toimenpiteitä, kuten suodattimia, työntekijöiden internetin käytön valvonnan sijasta.

Tietosuojatyöryhmän valmisteluasiakirjassa on tutkimus yleisimmistä työsuhteelle ominaisista tietosuojaongelmista[930]. Tietosuojatyöryhmä analysoi suostumuksen merkitystä työsuhdetta koskevien tietojen käsittelyn oikeudellisena perusteena[931]. Se totesi, että suostumusta pyytävän työnantajan ja suostumuksen antavan työntekijän välinen taloudellinen epätasapaino herättää usein epäilyjä suostumuksen vapaaehtoisuudesta. Siksi olosuhteet, joissa suostumusta käytetään tietojenkäsittelyn oikeudellisena perusteena, olisi otettava huolellisesti huomioon arvioitaessa suostumuksen pätevyyttä työsuhteen yhteydessä.

Nykyään tavallinen tietosuojaongelma tyypillisessä työympäristössä liittyy oikeuteen valvoa työntekijöiden sähköistä viestintää työpaikalla. Usein esitetään, että ongelma olisi helppo ratkaista kieltämällä viestintävälineiden käyttö yksityisiin tarkoituksiin työtä tehtäessä. Tällainen yleinen kielto voisi kuitenkin olla suhteeton ja epärealistinen. Euroopan ihmisoikeustuomioistuimen tuomiot asioissa *Copland v. Yhdistynyt kuningaskunta* ja *Bărbulescu v. Romania* ovat erityisen kiinnostavia tässä yhteydessä.

Esimerkki: Asiassa *Copland v. Yhdistynyt kuningaskunta*[932] korkeakoulun työntekijän puhelimen, sähköpostin ja internetin käyttöä oli seurattu sen selvittämiseksi, käyttikö hän korkeakoulun palveluja liian paljon henkilökohtaisiin tarkoituksiin. Euroopan ihmisoikeustuomioistuin katsoi, että työpaikalla soitetut puhelut kuuluivat yksityiselämän ja kirjesalaisuuden piiriin. Siksi tällaiset työpaikalla soitetut puhelut ja kirjoitetut sähköpostiviestit samoin kuin yksityisen internetin käytön seurannasta saadut tiedot olivat suojattuja ihmisoikeussopimuksen 8 artiklan nojalla. Kantajan tapauksessa ei ollut olemassa mitään säännöksiä, joilla olisi säädetty, missä olosuhteissa työnantajat

930 Tietosuojatyöryhmä (2017), *lausunto 2/2017 tietojenkäsittelystä työpaikalla*, WP 249, Bryssel, 8.6.2017.

931 Tietosuojatyöryhmä (2005), *valmisteluasiakirja 24. lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*, WP 114, Bryssel, 25.11.2005.

932 EIT, *Copland v. Yhdistynyt kuningaskunta*, nro 62617/00, 3.4.2007.

voivat seurata työntekijöiden puhelimen, sähköpostin ja internetin käyttöä. Oikeuteen puuttuminen ei siten ollut lainmukaista. Tuomioistuin totesi, että ihmisoikeussopimuksen 8 artiklaa oli rikottu.

Esimerkki: Asiassa *Bărbulescu v. Romania*[933] kantaja oli irtisanottu, koska hän oli käyttänyt työnantajansa verkkoyhteyttä työaikana sisäisten määräysten vastaisesti. Työnantaja oli seurannut hänen viestintäänsä. Kansallisessa oikeudenkäynnissä esitettiin asiakirjoja täysin yksityisistä viesteistä. Euroopan ihmisoikeustuomioistuin katsoi, että 8 artiklaa voidaan soveltaa, mutta jätti avoimeksi kysymyksen siitä, jättivätkö työnantajan rajoittavat määräykset kantajalle kohtuullisin syihin perustuvan oikeuden edellyttää yksityisyyttä. Joka tapauksessa se totesi, että yksityistä sosiaalista elämää työpaikalla ei voida työnantajan ohjeilla vähentää olemattomaan.

Pääasian osalta sopimuspuolille piti antaa laaja harkintavalta sen arvioimiseksi, onko laadittava oikeudellinen kehys ehdoille, joiden mukaan työnantaja voisi säännellä työntekijöidensä sähköistä tai muuta työhön kuulumatonta viestintää työpaikalla. Kansallisten viranomaisten piti joka tapauksessa varmistaa, että jos työnantaja ottaa käyttöön toimenpiteitä, joilla valvotaan kirjeenvaihtoa ja muuta viestintää, toimenpiteisiin on niiden laajuudesta ja kestosta riippumatta kuuluttava asianmukaiset ja riittävät takeet väärinkäyttöä vastaan. Suhteellisuus ja menettelytakeet mielivaltaisuudelta olivat olennaisen tärkeitä, ja Euroopan ihmisoikeustuomioistuin yksilöi useita olosuhteiden kannalta merkityksellisiä tekijöitä. Tällaisia tekijöitä olivat esimerkiksi se, miten kattavasti työnantaja valvoo työntekijöitä ja miten paljon työntekijän yksityisyyteen puututaan, seuraukset työntekijälle sekä se, onko riittävät suojatoimet otettu käyttöön. Kansallisten viranomaisten piti lisäksi varmistaa, että työntekijällä, jonka viestintää oli valvottu, oli saatavillaan oikeussuojakeinoja oikeusviranomaisessa, jonka valtuuksiin kuului määrittää, ainakin pääkohdiltaan, miten annettuja kriteereitä noudatettiin ja olivatko kiistanalaiset toimenpiteet lainmukaisia.

Tässä tapauksessa Euroopan ihmisoikeustuomioistuin totesi, että 8 artiklaa oli rikottu, koska kansalliset viranomaiset eivät olleet taanneet riittävää suojaa kantajan oikeudelle nauttia yksityis- ja perhe-elämään ja kirjeenvaihtoon kohdistuvaa kunnioitusta eivätkä siksi olleet pystyneet löytämään oikeaa tasapainoa kyseessä olevien intressien välille.

933 EIT, *Bărbulescu v. Romania* [suuri jaosto], nro 61496/08, 5.9.2017, 121 kohta.

Euroopan neuvoston työelämää koskevan suosituksen mukaan työntekijää koskevat henkilötiedot olisi kerättävä suoraan työntekijältä itseltään.

Rekrytointia varten kerättävien henkilötietojen on rajoituttava tietoihin, joita tarvitaan hakijoiden soveltuvuuden ja uramahdollisuuksien arviointiin.

Suosituksessa myös nimenomaisesti mainitaan yksittäisten työntekijöiden työsuoritukseen tai mahdollisuuksiin liittyvät arviointitiedot. Arviointitietojen on perustuttava oikeudenmukaisiin ja rehellisiin arviointeihin, eikä niitä saa laatia loukkaavaan muotoon. Tätä edellyttävät tietojen asianmukaisen käsittelyn ja täsmällisyyden periaatteet.

Erityinen tietosuojalainsäädäntöön liittyvä näkökohta työnantajan ja työntekijän välisessä suhteessa on työntekijöiden edustajien asema. Nämä edustajat voivat saada työntekijöiden henkilötietoja vain siinä määrin kuin he tarvitsevat niitä voidakseen ajaa työntekijöiden etuja tai siinä tapauksessa, että tiedot ovat tarpeen työehtosopimuksessa esitettyjen velvollisuuksien täyttämiseksi tai valvomiseksi.

Työsuhteen hoitamista varten kerättyjä arkaluonteisia henkilötietoja voidaan käsitellä vain tarkoin määritellyissä tapauksissa ja kansallisessa lainsäädännössä asetettujen suojatoimien puitteissa. Työnantajat voivat kysyä työntekijöiltä tai työnhakijoilta tietoja heidän terveydentilastaan tai suorittaa heille lääkärintarkastuksen vain, jos se on tarpeen. Tämä voi olla tarpeen työtehtäviin soveltuvuuden ratkaisemiseksi, ennalta ehkäisevän terveydenhuollon vaatimusten täyttämiseksi, rekisteröidyn tai muiden työntekijöiden ja henkilöiden elintärkeiden etujen suojaamiseksi, sosiaaliturvaetuuksien myöntämiseksi tai oikeuden pyyntöihin vastaamiseksi. Terveydentilaa koskevia tietoja ei saa kerätä muualta kuin työntekijältä itseltään, ellei tämä ole antanut nimenomaisesti tietoista suostumusta tai ellei asiasta ole säädetty lailla.

Työelämää koskevan suosituksen mukaan työntekijöille tulisi ilmoittaa, mitä tarkoitusta varten heidän henkilötietojaan käsitellään, millaisia tietoja heistä kerätään ja keille tietoja luovutetaan säännöllisesti sekä tällaisen luovuttamisen tarkoitus ja oikeudellinen peruste. Sähköiseen viestintään voi päästä työpaikalla vain turvallisuussyistä tai muista laillisista syistä. Tällainen pääsy on sallittua vasta, kun työntekijöille on ilmoitettu siitä, että työnantajalla voi olla pääsy tällaiseen viestintään.

Työntekijöillä on oltava oikeus tarkastaa työsuhdettaan koskevat tiedot sekä oikeus pyytää tietojen korjaamista tai poistamista. Jos arviointitietoja käsitellään,

työntekijöillä on lisäksi oltava oikeus kiistää arvion oikeellisuus. Näitä oikeuksia voidaan kuitenkin tilapäisesti rajoittaa sisäisten tutkimusten suorittamista varten. Jos työnantaja kieltäytyy antamasta tarkastusoikeutta tai korjaamasta tai poistamasta tietoja työntekijän vaatimuksen mukaisesti, kansallisessa lainsäädännössä on säädettävä asianmukaiset menettelyt tämän kieltäytymisen riitauttamiseen.

9.3 Terveydentilaa koskevat tiedot

Keskeinen kohta

- Terveydentilaa koskevat tiedot ovat arkaluonteisia ja siksi niitä suojellaan erityisen tarkasti.

Rekisteröidyn terveydentilaa koskevat henkilötiedot määritellään yleisen tietosuoja-asetuksen 9 artiklan 1 kohdassa ja uudistetun yleissopimuksen 108 6 artiklassa arkaluonteisiksi. Terveydentilaa koskeviin tietoihin sovelletaankin tiukempaa tietosuojajärjestelmää kuin tietoihin, jotka eivät ole arkaluonteisia. Yleisessä tietosuoja-asetuksessa kielletään ”terveyttä koskevien henkilötietojen” (joilla tarkoitetaan kaikkia tietoja, ”jotka koskevat rekisteröidyn terveydentilaa ja paljastavat tietoja rekisteröidyn entisestä, nykyisestä tai tulevasta fyysisen terveyden tai mielenterveyden tilasta”)[934] sekä geneettisten tietojen ja biometristen tietojen käsittely, ellei sitä sallita 9 artiklan 2 kohdassa. Molemmat tietotyypit kuuluvat ”erityisten henkilötietoryhmien”[935] luetteloon.

Esimerkki: Asiassa *Z v. Suomi*[936] kantajan entinen aviomies, jolla oli HIV-tartunta, oli syyllistynyt lukuisiin seksuaalirikoksiin. Hänet tuomittiin taposta sillä perusteella, että hän oli tietoisesti asettanut uhrinsa alttiiksi HIV-tartunnalle. Kansallinen tuomioistuin määräsi tuomion koko tekstin ja asiaan liittyvät asiakirjat pidettäviksi salassa kymmenen vuotta, vaikka kantaja pyysi pidempää salassapitoaikaa. Muutoksenhakutuomioistuin eväsi pyynnön ja

934 Yleinen tietosuoja-asetus, johdanto-osan 35 kappale.

935 *Ibid.*, 2 artikla.

936 EIT, *Z v. Suomi*, nro 22009/93, 25.2.1997, 94 ja 112 kohta; ks. myös EIT, *M.S. v. Ruotsi*, nro 20837/92, 27.8.1997; EIT, *L.L. v. Ranska*, nro 7508/02, 10.10.2006; EIT, *I v. Suomi*, nro 20511/03, 17.7.2008; EIT, *K.H. ym. v. Slovakia*, nro 32881/04, 28.4.2009; EIT, *Szuluk v. Yhdistynyt kuningaskunta*, nro 36936/05, 2.6.2009.

esitti tuomiossaan sekä kantajan että hänen entisen aviomiehensä koko nimet. Euroopan ihmisoikeustuomioistuin katsoi, ettei oikeuteen puuttuminen ollut ollut välttämätöntä demokraattisessa yhteiskunnassa, koska terveydentilaa koskevien tietojen suojaaminen on olennainen edellytys mahdollisuudelle nauttia oikeudesta yksityis- ja perhe-elämään kohdistuvaa kunnioitusta, erityisesti silloin kun on kyse HIV-tartunnasta, johon liittyy monissa yhteiskunnassa vahva leima. Näin ollen tuomioistuin totesi, että kantajan henkilöllisyyttä ja terveydentilaa koskevien tietojen saattaminen saataville muutoksenhakutuomioistuimen tuomiossa esitetyllä tavalla vain kymmenen vuoden kuluttua tuomiosta, rikkoisi ihmisoikeussopimuksen 8 artiklaa.

EU:n oikeudessa yleisen tietosuoja-asetuksen 9 artiklan 2 kohdan h alakohdassa sallitaan terveydentilaa koskevien tietojen käsittely, kun se on tarpeen ehkäisevää terveydenhuoltoa tai lääketieteellisiä diagnooseja varten, hoidon tai käsittelyn suorittamiseksi taikka terveyshuollon palvelujen ja järjestelmien hallintoa varten. Käsittely on kuitenkin sallittua vain, kun siitä vastaa ammattilainen, jolla on lakisääteinen salassapitovelvollisuus, tai toinen henkilö, jota niin ikään sitoo lakisääteinen salassapitovelvollisuus.

Euroopan neuvoston oikeudessa vuonna 1997 annetussa terveydentilaa koskevia tietoja koskevassa suosituksessa sovelletaan yleissopimuksen 108 periaatteita tietojenkäsittelyyn erityisesti lääketieteen alalla[937]. Ehdotetut säännöt ovat yhdenmukaiset yleisen tietosuoja-asetuksen sääntöjen kanssa terveydentilaa koskevien tietojen käsittelyn laillisten tarkoitusten, terveydentilaa koskevia tietoja käsittelevien henkilöiden salassapitovelvollisuuden sekä tietojenkäsittelyn avoimuutta, tarkastusoikeutta ja tietojen korjaamista ja poistamista koskevien oikeuksien osalta. Lisäksi terveydenhuollon ammattilaisten laillisesti käsittelemiä terveydentilaa koskevia tietoja ei voida luovuttaa lainvalvontaviranomaisille, ellei ole toteutettu riittäviä suojatoimia ihmisoikeussopimuksen 8 artiklassa taattua yksityiselämän kunnioitusta rikkovan luovuttamisen estämiseksi.[938] Myös kansallinen lainsäädäntö on muotoiltava riittävän täsmällisesti, ja siinä on taattava riittävä oikeusturva mielivaltaisuudelta[939].

937 Euroopan neuvosto, ministerikomitea (1997), suositus Rec(97)5, jäsenvaltioille lääketieteellisten tietojen tietosuojasta, 13.2.1997. Tätä suositusta tarkistetaan parhaillaan.

938 EIT, *Avilkina ym. v. Venäjä*, nro 1585/09, 6.6.2013, 53 kohta. Ks. Myös EIT, *Biriuk v. Liettua*, nro 23373/03, 25.11.2008.

939 EIT, *L.H. v. Latvia*, nro 52019/07, 29.4.2014, 59 kohta.

Terveydentilaa koskevia tietoja koskeva suositus sisältää vielä erityisiä sääntöjä syntymättömien lasten ja vajaakykyisten henkilöiden terveydentilaa koskevia tietoja sekä geneettisten tietojen käsittelyä varten. Tieteellinen tutkimus tunnustetaan selkeästi syyksi säilyttää tietoja pidempään kuin on tarpeen, mutta tiedot on yleensä tehtävä anonyymeiksi. Terveydentilaa koskevia tietoja koskevan suosituksen 12 artiklassa ehdotetaan yksityiskohtaisia sääntöjä tilanteisiin, joissa tutkijat tarvitsevat henkilötietoja, eivätkä anonyymit tiedot riitä.

Pseudonymisoinnin avulla voi olla mahdollista täyttää tieteelliset tarpeet siten, että potilaiden edut pysyvät suojattuina. Tietojen pseudonymisointia tietosuojan edistämiseksi käsitellään tarkemmin 2.1.1 kohdassa.

Vuonna 2016 annettua Euroopan neuvoston suositusta geenitesteistä saatavista tiedoista sovelletaan myös tietojenkäsittelyyn lääketieteen alalla[940]. Suositus on erittäin tärkeä sähköiselle terveydenhuollolle, jossa käytetään tieto- ja viestintätekniikkaa terveydenhoidon helpottamiseen. Esimerkkinä tästä on potilaan vanhemmuustestin tulosten lähettäminen yhdeltä terveydenhuollon tarjoajalta toiselle. Suosituksen tarkoituksena on myös suojella niiden henkilöiden oikeuksia, joiden henkilötietoja käsitellään vakuutustarkoituksiin henkilön terveyteen, fyysiseen kuntoon, ikään tai kuolemaan liittyviltä riskeiltä vakuuttamiseksi. Vakuutusyhtiöiden on perusteltava terveydentilaa koskevien tietojen käsittely, ja sen pitäisi olla oikeassa suhteessa käsiteltävänä olevan riskin luonteeseen ja merkitykseen. Tällaisten tietojen käsittely edellyttää rekisteröidyn suostumusta. Vakuutusyhtiöillä on myös oltava käytössä suojatoimia terveydentilaa koskevien tietojen säilyttämistä varten.

Kliinisiin tutkimuksiin eli uusien lääkkeiden testaamiseen potilailla dokumentoidussa tutkimusympäristössä liittyy merkittäviä tietosuojakysymyksiä. Ihmisille tarkoitettujen lääkkeiden kliinisiä tutkimuksia säännellään ihmisille tarkoitettujen lääkkeiden kliinisistä lääketutkimuksista ja direktiivin 2001/20/EY kumoamisesta 16 päivänä huhtikuuta 2014 annetulla Euroopan parlamentin ja neuvoston asetuksella (EU) N:o 536/2014 (kliinisiä tutkimuksia koskeva asetus)[941]. Kliinisiä tutkimuksia koskevan asetuksen päätekijät ovat

940 Euroopan neuvosto, ministerikomitea (2016), suositus Rec(2016)8 jäsenvaltioille vakuutustarkoituksiin käytettävien terveydentilaa koskevien henkilötietojen, myös geenitesteistä saatavien tietojen, käsittelystä, 26.10.2016.

941 Euroopan parlamentin ja neuvoston asetus (EU) N:o 536/2014, annettu 16 päivänä huhtikuuta 2014, ihmisille tarkoitettujen lääkkeiden kliinisistä lääketutkimuksista ja direktiivin 2001/20/EY kumoamisesta (kliinisiä tutkimuksia koskeva asetus), EUVL 2014, L 158.

- tehostettu hakumenettely EU-portaalin kautta[942]
- määräajat kliinisten lääketutkimusten lupahakemusten arvioinnille[943]
- jäsenvaltioiden lainsäädännön mukaisesti arviointiin osallistuva eettinen komitea (jonka osalta EU:n oikeudessa määritetään asianomaiset ajanjaksot)[944] ja
- kliinisten lääketutkimusten ja niiden tulosten avoimuuden parantaminen[945].

Yleisessä tietosuoja-asetuksessa täsmennetään, että suostumukseen osallistua kliinisiin lääketutkimuksiin liittyviin tieteellisiin tutkimustoimiin olisi sovellettava asetusta (EU) N:o 536/2014[946].

EU:ssa on käsiteltävänä lukuisia muitakin lainsäädännöllisiä ja muita aloitteita, jotka liittyvät henkilötietojen käyttöön terveydenhoitoalalla.[947]

Sähköinen terveyskertomus

Sähköisellä terveyskertomuksella tarkoitetaan ”kattavia potilastietoja tai vastaavaa dokumentaatiota henkilön menneestä ja nykyisestä fyysisestä ja psyykkisestä terveydentilasta sähköisessä muodossa siten, että tiedot ovat valmiiksi käytettävissä lääkinnällistä hoitoa ja muuta tähän tiiviisti liittyvää tarkoitusta varten”[948]. Sähköinen terveyskertomus on sähköinen versio potilaan terveydentilasta ja terveydellisestä taustasta, ja siihen voi kuulua kyseiseen henkilöön liittyviä kliinisiä tietoja, kuten aiempi terveydentila ja terveydellinen tausta, ongelmat ja sairaudet, lääkkeet ja hoidot sekä tutkimus- ja laboratoriotulokset ja raportit. Nämä sähköiset tiedostot, joihin voi kuulua koko kertomus tai vain otteita ja tiivistelmiä, ovat lääkärin, farmaseutin

942 Kliinisiä tutkimuksia koskeva asetus, 5 artiklan 1 kohta.

943 *Ibid.*, 5 artiklan 2–5 kohta.

944 *Ibid.*, 2 artiklan 2 kohdan 11 alakohta.

945 *Ibid.*, 9 artiklan 1 kohta ja johdanto-osan 67 kappale.

946 Yleinen tietosuoja-asetus, johdanto-osan 156 ja 161 kappale.

947 EDPS (2013), *Opinion of the European Data Protection Supervisor on the Communication from the Commission on 'eHealth Action Plan 2012–2020 – Innovative healthcare for the 21st century*, Bryssel, 27.3.2013 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee komission tiedonantoa ”Sähköisen terveydenhuollon toimintasuunnitelma 2012–2020 – innovatiivista terveydenhuoltoa 21. vuosisadalle”).

948 Komission suositus, annettu 2 päivänä heinäkuuta 2008, sähköisten terveyskertomusjärjestelmien rajatylittävästä yhteentoimivuudesta, 3 kohdan e alakohta.

ja muiden terveydenhoidon ammattilaisten saatavissa. Myös ”sähköisen terveydenhuollon” käsite liittyy tähän terveyskertomukseen.

> Esimerkki: Henkilö A on ottanut vakuutuksen vakuutusyhtiöltä B. Vakuutusyhtiö kerää A:lta joitakin terveydentilaa koskevia tietoja, kuten nykyiset terveysongelmat tai sairaudet. Vakuutusyhtiön pitäisi säilyttää A:n terveydentilaa koskevia tietoja erillään muista tiedoista. Vakuutusyhtiön on myös säilytettävä terveyteen liittyviä henkilötietoja erillään muista tiedoista. Tämä tarkoittaa, että vain A:n tapauksenkäsittelijällä on pääsy A:n terveydentilaa koskeviin tietoihin.

Sähköiset terveystiedostot herättävät kuitenkin tiettyjä tietosuojakysymyksiä, muun muassa niiden saatavuudesta, asianmukaisesta säilytyksestä ja siitä, voiko rekisteröity tutustua niihin.

Sähköistä terveyskertomusta koskevan suosituksen lisäksi Euroopan komissio julkaisi 10. huhtikuuta 2014 vihreän kirjan terveysalan mobiilisovelluksista (”mHealth”), koska terveysalan mobiilisovellukset ovat uusi ja nopeasti kehittyvä ala, joka voi osaltaan edesauttaa terveydenhuollon uudistumista sekä lisätä terveydenhuollon laatua ja tehokkuutta. Käsitteellä viitataan lääketieteellisiin ja kansanterveydellisiin käytäntöihin, joissa hyödynnetään mobiililaitteita, kuten matkapuhelimia, potilaiden seurantalaitteita, kämmentietokoneita ja muita langattomia laitteita, sekä sovelluksiin (esim. elämäntapa- ja hyvinvointisovelluksiin) jotka voidaan yhdistää lääkinnällisiin laitteisiin tai antureihin.[949] Asiakirjassa esitellään riskejä, joita terveysalan mobiilisovellusten kehitys voi aiheuttaa henkilötietojen suojalle, ja säädetään, että terveystietojen arkaluonteisuuden vuoksi kehitykseen olisi sisällyttävä erityisiä ja tarkoitukseen soveltuvia turvallisuustakeita turvallisuusriskien vähentämiseksi, kuten potilastietojen salaus ja asianmukainen henkilöllisyyden todentamisjärjestelmä. Henkilötietojen suojaa koskevien sääntöjen noudattaminen, myös velvollisuus informoida rekisteröityä, tietoturva sekä henkilötietojen laillisen käsittelyn periaate ovat näin ollen erittäin tärkeitä asioita, jotta terveysalan mobiilisovellusratkaisuihin voidaan luottaa.[950] Tätä varten toimialalla on laadittu käytännesäännöt terveysalan mobiilisovellusten yksityisyydensuojasta. Niiden laatimiseen on osallistunut edustajia useista sidosryhmistä, muun muassa tietosuojan, itse- ja

949 Euroopan komissio (2014), *vihreä kirja terveysalan mobiilisovelluksista (”mHealth”)*, COM(2014) 219 final, Bryssel, 10.4.2014.

950 *Ibid.*, s. 8.

yhteissääntelyn, tieto- ja viestintätekniikan sekä terveydenhuollon asiantuntijoita.[951] Käsikirjan laatimisen aikaan käytännesääntöjen luonnos oli toimitettu lausuntoja varten tietosuojatyöryhmään odottamaan sen virallista hyväksyntää.

9.4 Tietojenkäsittely tutkimustarkoituksiin ja tilastollisiin tarkoituksiin

Keskeiset kohdat

- Tilastollisia tarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia varten kerättyjä tietoja ei voida käyttää mihinkään muuhun tarkoitukseen.
- Muihin tarkoituksiin laillisesti kerättyjä tietoja voidaan käyttää tilastollisiin tarkoituksiin taikka tieteellisiin tai historiallisiin tutkimustarkoituksiin, mikäli käytössä on riittävät suojatoimet. Tätä varten tulisi erityisesti harkita tietojen tekemistä anonyymeiksi tai pseudonyymeiksi ennen niiden luovuttamista kolmansille osapuolille

EU:n oikeudessa sallitaan tietojen käsittely tilastollisia tarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia varten, jos käytössä on rekisteröidyn oikeuksia ja vapauksia koskevat asianmukaiset suojatoimet. Niitä voi olla esimerkiksi pseudonymisointi.[952] Unionin oikeudessa tai jäsenvaltion lainsäädännössä voidaan säätää poikkeuksista rekisteröityjen oikeuksiin, jos tällaiset oikeudet todennäköisesti estävät tutkimuksen oikeutetun tarkoituksen saavuttamisen tai vaikeuttavat sitä suuresti[953]. Poikkeuksia voidaan soveltaa rekisteröidyn oikeuteen saada pääsy tietoihinsa, oikaista tiedot, rajoittaa käsittely ja vastustaa käsittelyä.

Vaikka tiedot laillisesti kerännyt rekisterinpitäjä voi käyttää tietoja uudelleen mihin tahansa tarkoitukseen omia tilastollisia tarkoituksiaan taikka tieteellisiä tai historiallisia tutkimustarkoituksiaan varten, tiedot on tilanteen mukaan anonymisoitava tai niille on tehtävä pseudonymisoinnin kaltaisia toimenpiteitä ennen kuin niitä välitetään kolmannelle osapuolelle tilastollisia tarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia varten, paitsi jos rekisteröity on antanut siihen suostumuksen tai jos siitä säädetään nimenomaisesti kansallisessa lainsäädännössä.

951 Draft Code of Conduct on privacy for mobile health applications, 7.6.2016.

952 Yleinen tietosuoja-asetus, 89 artiklan 1 kohta.

953 *Ibid.*, 89 artiklan 2 kohta.

Rekisteröidyn pseudonymisoituihin tietoihin sovelletaan edelleen yleistä tietosuoja-asetusta toisin kuin anonyymeihin tietoihin.[954]

Asetuksessa myönnetään näin ollen tutkimukselle erityiskohtelu yleisten tietosuojasääntöjen osalta, jotta voidaan välttää rajoittamasta tutkimuksen kehitystä ja noudattaa SEUT-sopimuksen 179 artiklassa esitettyä tavoitetta eurooppalaisen tutkimusalueen toteuttamisesta. Siinä säädetään tieteellisiä tutkimustarkoituksia varten tehtävän henkilötietojen käsittelyn laajasta tulkinnasta. Se sisältää muun muassa teknologian kehittämisen ja esittelyn, perustutkimuksen, soveltavan tutkimuksen ja yksityisin varoin rahoitetun tutkimuksen. Siinä tunnustetaan myös, että on tärkeää koota tietoja rekistereihin tutkimustarkoituksia varten ja että tieteellisiä tutkimustarkoituksia varten tehtävän käsittelyn tarkoitusta ei ole ehkä mahdollista täysin määrittää siinä vaiheessa, kun henkilötietoja kerätään.[955] Tämän vuoksi asetuksessa sallitaan tietojen käsittely näitä tarkoituksia varten ilman rekisteröidyn suostumusta, jos asianmukaiset suojatoimet ovat käytössä.

Tärkeä esimerkki tietojen käytöstä tilastollisia tarkoituksia varten ovat viralliset tilastot, joita saadaan kansallisilta ja EU:n tilastotoimistoilta virallisia tilastoja koskevien kansallisten ja EU:n säädösten mukaisesti. Näiden säädösten mukaan kansalaisten ja yritysten on tavallisesti luovutettava tietoja asiaankuuluville tilastoviranomaisille. Tilastotoimistoissa työskenteleviä virkailijoita velvoittavat erityiset salassapitovelvollisuudet, joita on noudatettava asianmukaisesti, koska ne ovat keskeisiä kansalaisten luottamukselle, jos heidän on annettava tietojaan tilastoviranomaisille.[956]

Euroopan tilastoista annettu asetus (EY) N:o 223/2009 (tilastoasetus) sisältää virallisten tilastojen tietosuojaa koskevat keskeiset säännöt, ja sillä on siten vaikutusta myös virallisten tilastojen sääntelyyn kansallisella tasolla.[957] Asetuksessa vahvistetaan

954 *Ibid.*, johdanto-osan 26 kappale.

955 *Ibid.*, johdanto-osan 33, 157 ja 159 kappale.

956 *Ibid.*, 90 artikla.

957 Euroopan parlamentin ja neuvoston asetus (EY) N:o 223/2009, annettu 11 päivänä maaliskuuta 2009, Euroopan tilastoista sekä salassapidettävien tilastotietojen luovuttamisesta Euroopan yhteisöjen tilastotoimistolle annetun Euroopan parlamentin ja neuvoston asetuksen (EY, Euratom) N:o 1101/2008, yhteisön tilastoista annetun neuvoston asetuksen (EY) N:o 322/97 ja Euroopan yhteisöjen tilastoohjelmakomitean perustamisesta tehdyn neuvoston päätöksen 89/382/ETY, Euratom kumoamisesta, EUVL 2009, L 87, sellaisena kuin se on muutettuna Euroopan tilastoista annetun asetuksen (EY) N:o 223/2009 muuttamisesta 29 päivänä huhtikuuta 2015 annetulla Euroopan parlamentin ja neuvoston asetuksella (EU) 2015/759, EUVL 2015, L 123.

periaate, jonka mukaan virallisten tilastojen käsittelyyn on oltava riittävän tarkoin määritelty oikeudellinen peruste[958].

Esimerkki: Asiassa *Huber vastaan Bundesrepublik Deutschland*[959] Saksaan muuttanut itävaltalainen liikemies valitti, että hänen tietosuojadirektiivillä vahvistettuja oikeuksiaan loukattiin, kun Saksan viranomaiset keräsivät ulkomaalaisten henkilötietoja keskusrekisteriin (AZR) myös tilastollisia tarkoituksia varten ja säilyttivät niitä rekisterissä. Koska direktiivin 95/46/EY tarkoituksena on taata kaikissa jäsenvaltioissa sama suojan taso, unionin tuomioistuin katsoi, että korkean suojan tason varmistamiseksi EU:ssa 7 artiklan e alakohdan mukainen tarpeellisuuden käsite ei voi olla sisällöltään erilainen eri jäsenvaltioissa. Se on näin ollen EU:n oikeuden itsenäinen käsite, jota on tulkittava siten, että se vastaa täysimääräisesti direktiivin 95/46/EY tavoitetta. Unionin tuomioistuin huomautti, että tilastollisia tarkoituksia varten pitäisi vaatia vain anonyymeja tietoja, ja totesi, että Saksan rekisteri ei ollut yhteensopiva 7 artiklan e alakohdan mukaisen tarpeellisuuden käsitteen kanssa.

Euroopan neuvoston mukaan tietoja voidaan käsitellä edelleen tieteellisiä, historiallisia tai tilastollisia tarkoituksia varten, kun se on yleisen edun mukaista ja kun siihen sovelletaan asianmukaisia suojatoimia[960]. Rekisteröityjen oikeuksia voidaan myös rajoittaa, kun tietoja käsitellään tilastollisia tarkoituksia varten, mikäli heidän oikeuksiensa ja vapauksiensa rikkomiseen ei ole tunnistettavaa riskiä[961].

Euroopan neuvoston vuonna 1997 antama tilastotietoja koskeva suositus kattaa tilastojen laadinnan niin julkisella kuin yksityiselläkin sektorilla[962].

Tietoja, jotka rekisterinpitäjä on kerännyt tilastollisiin tarkoituksiin, ei voida käyttää muihin tarkoituksiin, mutta tietoja, jotka on kerätty muihin tarkoituksiin, voidaan

958 Tätä periaatetta tarkennetaan Eurostatin käytännesäännöissä, joissa annetaan Euroopan tilastoista annetun asetuksen 11 artiklan mukaisesti eettisiä ohjeita virallisten tilastojen laadintaan, mukaan lukien henkilötietojen harkitsevainen käyttö.

959 EUT, C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland* [suuri jaosto], 16.12.2008; ks. erityisesti 68 kohta.

960 Uudistettu yleissopimus 108, 5 artiklan 4 kohdan b alakohta.

961 *Ibid.*, 11 artiklan 2 kohta.

962 Euroopan neuvosto, ministerikomitea (1997), suositus Rec(97)18 jäsenvaltioille tilastollisiin tarkoituksiin kerättyjen ja käsiteltyjen henkilötietojen suojelusta, 30.9.1997.

ottaa tilastolliseen käyttöön. Tilastotietoja koskevassa suosituksessa sallitaan jopa tietojen luovuttaminen kolmansille osapuolille silloin, kun se tapahtuu yksinomaan tilastollisiin tarkoituksiin. Tällöin osapuolien tulisi sopia ja dokumentoida laillisen tilastokäytön laajuus. Koska tällä tavalla ei voida ohittaa rekisteröidyn suostumusta – jos sitä tarvitaan – kansallisessa lainsäädännössä on vahvistettava riittävät suojatoimet henkilötietojen väärinkäytön riskien minimoimiseksi, kuten velvollisuus tehdä tiedot anonyymeiksi tai pseudonyymeiksi ennen niiden luovuttamista.

Tilastotutkimusta ammattimaisesti harjoittaville henkilöille tulisi asettaa kansallisessa lainsäädännössä salassapitovelvollisuus – kuten virallisten tilastojen kohdalla yleensä on tehty. Salassapitovelvollisuus tulisi ulottaa myös haastattelijoihin ja muihin henkilötietojen kerääjiin, jos he osallistuvat työssään tietojen keräämiseen rekisteröidyiltä tai muilta henkilöiltä.

Jos henkilötietoja käsitellään tilastollisessa tarkoituksessa eikä siitä ole säädetty lailla, vaaditaan tällaisen tilastollisen tutkimuksen lailliseen tekemiseen joko rekisteröidyn suostumus tai heille on mahdollisesti annettava oikeus vastustaa käsittelyä. Jos henkilötietoja kerätään tilastollisiin tarkoituksiin haastattelemalla, haastateltaville on kerrottava selkeästi, onko tietojen luovuttaminen kansallisen lain mukaan pakollista.

Jos tilastotutkimusta ei voida toteuttaa anonyymeillä tiedoilla, vaan tarvitaan henkilötietoja, tätä tarkoitusta varten kerätyt tiedot tulisi tehdä anonyymeiksi heti, kun se on mahdollista. Tilastotutkimuksen tuloksista ei ainakaan pidä voida tunnistaa yhtään rekisteröityä, ellei se ole selvästi täysin riskitöntä.

Kun tilastoanalyysi on tehty, siinä käytetyt henkilötiedot tulisi joko poistaa tai tehdä anonyymeiksi. Tilastotietoja koskevassa suosituksessa ehdotetaan, että jälkimmäisessä tapauksessa tunnistetiedot säilytettäisiin erillään muista henkilötiedoista. Tämä tarkoittaa esimerkiksi, että joko salauksen avain tai luettelo tunnistetiedoista on tallennettava eri paikkaan kuin muut tiedot.

9.5 Rahataloudelliset tiedot

Keskeiset kohdat

- Vaikka rahataloudelliset tiedot eivät ole arkaluonteisia tietoja uudistetussa yleissopimuksessa 108 tai yleisessä tietosuoja-asetuksessa tarkoitetulla tavalla, niiden käsittelyssä on noudatettava erityisiä suojatoimia tietojen täsmällisyyden ja tietoturvan varmistamiseksi.
- Etenkin sähköisissä maksujärjestelmissä on oltava sisäänrakennettu tietosuoja eli sisäänrakennettu ja oletusarvoinen yksityisyyden suoja tai tietosuoja.
- Asianmukaisten todentamisjärjestelmien tarve voi aiheuttaa tällä alalla erityisiä tietosuojaongelmia.

Esimerkki: Asiassa *Michaud v. Ranska*[963] kantaja, ranskalainen asianajaja, riitautti hänelle Ranskan lainsäädännössä asetetun velvollisuuden ilmoittaa hänen asiakkaidensa mahdollista rahanpesutoimintaa koskevista epäilyistä. Euroopan ihmisoikeustuomioistuimen näkemyksen mukaan se, että asianajajia vaaditaan ilmoittamaan hallintoviranomaisille muita henkilöitä koskevia tietoja, jotka he ovat saaneet yhteydenpidossaan näiden henkilöiden kanssa, rajoittaa asianajajien ihmisoikeussopimuksen 8 artiklan mukaista oikeutta nauttia kirjeenvaihtoon ja yksityiselämään kohdistuvaa kunnioitusta, joka kattaa ammatti- ja liiketoiminnan. Oikeuden rajoittaminen oli kuitenkin lainmukaista ja sillä oli laillinen tarkoitus, joka oli epäjärjestyksen ja rikosten ehkäiseminen. Koska asianajajilla on velvollisuus ilmoittaa epäilyistään vain tarkoin rajatuissa tilanteissa, tuomioistuin katsoi, että velvollisuus oli oikeasuhteinen. Näin ollen se totesi, ettei 8 artiklaa ollut rikottu.

Esimerkki: Asiassa *M.N. ym. v. San Marino*[964] kantaja, Italian kansalainen, teki omaisuudenhoitosopimuksen, tutkittavana olevan yrityksen kanssa. Tutkinta tarkoitti, että yrityksen (sähköisten) asiakirjojen jäljennöksiä etsittiin ja takavarikoitiin. Kantaja teki valituksen sanmarinolaiseen tuomioistuimeen, koska hänen mukaansa hänen ja väitettyjen rikosten välillä ei ollut yhteyttä. Tuomioistuin ei kuitenkaan ottanut hänen valitustaan käsiteltäväksi, koska hän ei ollut ”asianomainen osapuoli”. Euroopan ihmisoikeustuomioistuin katsoi,

963 EIT, *Michaud v. Ranska*, nro 12323/11, 6.12.2012. Ks. myös EIT, *Niemietz v. Ranska*, nro 13710/88, 16.12.1992, 29 kohta, ja EIT, *Halford v. Yhdistynyt kuningaskunta*, nro 20605/92, 25.6.1997, 42 kohta.

964 EIT, *M.N. ym. v. San Marino*, nro 28005/12, 7.7.2015.

että kantaja oli joutunut oikeusturvan kannalta huomattavan epäedulliseen asemaan verrattuna ”asianomaiseen osapuoleen”, vaikka hänenkin tietonsa olivat hakujen ja takavarikointien kohteena. Tuomioistuin katsoi näin ollen, että 8 artiklaa oli rikottu.

Esimerkki: Asiassa *G.S.B. v. Sveitsi*[965] kantajan pankkitilin tiedot lähetettiin Yhdysvaltojen viranomaisille Sveitsin ja Yhdysvaltojen välisen hallinnollista yhteistyötä koskevan sopimuksen perusteella. Euroopan ihmisoikeustuomioistuin totesi, että tietojen siirtämisellä ei rikottu ihmisoikeussopimuksen 8 artiklaa, koska puuttumisesta kantajan yksityisyyden suojaa koskevaan oikeuteen säädettiin laissa, sillä oli oikeutettu tarkoitus ja se oli oikeassa suhteessa kyseessä olevaan yleiseen etuun nähden.

Yleissopimukseen 108 sisältyvää tietosuojan yleistä oikeudellista kehystä on sovellettu maksujen alalla vuonna 1990 annetussa **Euroopan neuvoston** suosituksessa Rec(90)19[966]. Suosituksessa selvennetään tietojen laillisen keruun ja käytön rajoja maksujen ja erityisesti maksukorteilla tehtävien maksujen yhteydessä. Lisäksi siinä ehdotetaan kansallisille lainsäätäjille yksityiskohtaisia sääntöjä, jotka koskevat maksutietojen luovuttamista kolmansille osapuolille, tietojen säilytysaikoja, avoimuutta, tietoturvaa ja rajan yli tapahtuvaa tietojen siirtoa sekä valvontaa ja oikeussuojakeinoja. Euroopan neuvosto on myös antanut lausunnon verotietojen siirtämisestä[967]. Siinä esitetään suosituksia ja kysymyksiä, jotka on otettava huomioon verotietojen siirtämisessä.

Euroopan ihmisoikeustuomioistuin sallii rahataloudellisten tietojen – erityisesti henkilön pankkitilin tietojen – siirtämisen ihmisoikeussopimuksen 8 artiklan nojalla, jos siitä on säädetty laissa, sillä on oikeutettu tarkoitus ja se on oikeassa suhteessa kyseessä olevaan yleiseen etuun nähden[968].

EU:n oikeuden mukaan sähköisten maksujärjestelmien, joihin kuuluu henkilötietojen käsittelyä, on noudatettava yleistä tietosuoja-asetusta. Järjestelmissä on näin ollen varmistettava sisäänrakennettu ja oletusarvoinen tietosuoja. Sisäänrakennettu

965 EIT, *G.S.B. v. Sveitsi*, nro 28601/11 22.12.2015.

966 Euroopan neuvoston ministerikomitea (1990), suositus Rec(90)19 maksuihin ja niihin liittyviin operaatioihin käytettävien henkilötietojen suojaamisesta, 13.9.1990.

967 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea (2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4.6.2014.

968 EIT, *G.S.B. v. Sveitsi*, nro 28601/11, 22.12.2015.

tietosuoja velvoittaa rekisterinpitäjän ottamaan käyttöön asianmukaiset tekniset ja organisatoriset toimenpiteet tietosuojaperiaatteiden täytäntöön panemiseksi. Oletusarvoinen tietosuoja tarkoittaa, että rekisterinpitäjän on varmistettava, että oletusarvoisesti voidaan käsitellä vain tiettyä tarkoitusta varten tarvittavia henkilötietoja (ks. 4.4 kohta). Unionin tuomioistuin on todennut rahataloudellisista tiedoista, että siirretyt verotiedot voivat olla henkilötietoja[969]. Tietosuojatyöryhmä antoi tästä aiheesta jäsenvaltioille ohjeita, muun muassa kriteerit, joilla varmistetaan tietosuojasääntöjen noudattaminen, kun henkilötietoja vaihdetaan automaattisesti verotarkoituksiin[970]. Lisäksi rahoitusmarkkinoiden sekä luottolaitosten ja sijoituspalveluyritysten toiminnan säätelemiseksi on otettu käyttöön erilaisia oikeudellisia instrumentteja[971]. Toisilla oikeudellisilla instrumenteilla tuetaan sisäpiirikauppojen ja markkinoiden manipuloinnin torjuntaa[972]. Tärkeimmät tietosuojaan liittyvät kysymykset näillä aloilla ovat seuraavat:

- rahataloustoimia koskevien asiakirjojen säilytys
- henkilötietojen siirto kolmansiin maihin
- puhelinkeskustelujen ja sähköisen viestinnän tallentaminen, mukaan lukien toimivaltaisten viranomaisten valtuus pyytää puhelin- ja televiestintätietoja
- henkilötietojen luovuttaminen, mukaan lukien seuraamusten julkaiseminen
- toimivaltaisten viranomaisten valvonta- ja tutkintavaltuudet, mukaan lukien paikan päällä tehtävät tarkastukset ja pääsy yksityisiin tiloihin asiakirjojen takavarikointia varten

969 EUT, C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 1.10.2015, 29 kohta.

970 Tietosuojatyöryhmä (2015), Statement of the WP29 on automatic inter-state exchanges of personal data for tax purposes, 14/EN WP 230.

971 Euroopan parlamentin ja neuvoston direktiivi 2014/65/EU, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä direktiivin 2002/92/EY ja direktiivin 2011/61/EU muuttamisesta, EUVL 2014, L 173; Euroopan parlamentin ja neuvoston asetus (EU) N:o 600/2014, annettu 15 päivänä toukokuuta 2014, rahoitusvälineiden markkinoista sekä asetuksen (EU) N:o 648/2012 muuttamisesta, EUVL 2014, L 173; Euroopan parlamentin ja neuvoston direktiivi 2013/36/EU, annettu 26 päivänä kesäkuuta 2013, oikeudesta harjoittaa luottolaitostoimintaa ja luottolaitosten ja sijoituspalveluyritysten vakavaraisuusvalvonnasta, direktiivin 2002/87/EY muuttamisesta sekä direktiivien 2006/48/EY ja 2006/49/EY kumoamisesta, EUVL 2013, L 176.

972 Euroopan parlamentin ja neuvoston asetus (EU) N:o 596/2014, annettu 16 päivänä huhtikuuta 2014, markkinoiden väärinkäytöstä (markkinoiden väärinkäyttöasetus) sekä Euroopan parlamentin ja neuvoston direktiivin 2003/6/EY ja komission direktiivien 2003/124/EY, 2003/125/EY ja 2004/72/EY kumoamisesta, EUVL 2014, L 173.

- rikkomuksista ilmoittamisen mekanismit eli väärinkäytösten paljastamisen mekanismit

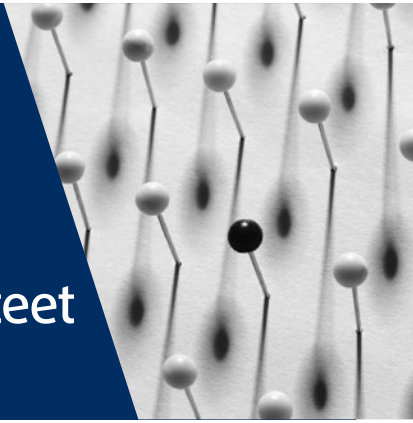
- jäsenvaltioiden toimivaltaisten viranomaisten ja Euroopan arvopaperimarkkina-viranomaisen (ESMA) välinen yhteistyö.

Näillä aloilla on muitakin kysymyksiä, joita on käsitelty tarkemmin, kuten tietojen kerääminen rekisteröityjen taloudellisesta tilanteesta[973] tai rajat ylittävät tilisiirrot, jotka väistämättä johtavat henkilötietojen siirtoon[974].

973 Euroopan parlamentin ja neuvoston asetus (EY) N:o 1060/2009, annettu 16 päivänä syyskuuta 2009, luottoluokituslaitoksista, EUVL 2009, L 302, sellaisena kuin se on viimeksi muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2014/51/EU, annettu 16 päivänä huhtikuuta 2014, direktiivien 2003/71/EY ja 2009/138/EY sekä asetusten (EY) N:o 1060/2009, (EU) N:o 1094/2010 ja (EU) N:o 1095/2010 muuttamisesta Euroopan valvontaviranomaisen (Euroopan vakuutus- ja lisäeläkeviranomainen) ja Euroopan valvontaviranomaisen (Euroopan arvopaperimarkkinaviranomainen) toimivaltuuksien osalta, EUVL 2014, L 153; Euroopan parlamentin ja neuvoston asetus (EU) N:o 462/2013, annettu 21 päivänä toukokuuta 2013, luottoluokituslaitoksista annetun asetuksen (EY) N:o 1060/2009 muuttamisesta, EUVL 2013, L 146.

974 Euroopan parlamentin ja neuvoston direktiivi 2007/64/EY, annettu 13 päivänä marraskuuta 2007, maksupalveluista sisämarkkinoilla, direktiivien 97/7/EY, 2002/65/EY, 2005/60/EY ja 2006/48/EY muuttamisesta ja direktiivin 97/5/EY kumoamisesta, EUVL 2007, L 319, sellaisena kuin se on muutettuna Euroopan parlamentin ja neuvoston direktiivillä 2009/111/EY, annettu 16 päivänä syyskuuta 2009, direktiivien 2006/48/EY, 2006/49/EY ja 2007/64/EY muuttamisesta keskuslaitoksiin kuuluvien pankkien, tiettyjen omien varojen erien, suurten riskikeskittymien, valvontajärjestelyjen ja kriisinhallinnan osalta, EUVL 2009, L 302.

10 Henkilötietojen suojaa koskevat nykyajan haasteet



Digitaaliajalle tai tietotekniikan ajalle on ominaista tietokoneiden, internetin ja digitaaliteknologioiden laaja käyttö. Siihen kuuluu suurien tietomäärien, myös henkilötietojen, käsittelyä. Henkilötietojen kerääminen ja käsittely globaalissa taloudessa tarkoittavat, että tietoja liikkuu rajojen yli jatkuvasti enemmän. Tällainen käsittely voi tuoda arkielämään huomattavia ja näkyviä etuja: Hakukoneiden ansiosta saatavilla on helposti valtavia tietomääriä, verkkoyhteisöpalveluissa ihmiset voivat olla yhteydessä toisiinsa ympäri maailmaa, ilmaista mielipiteitään ja hankkia tukea yhteiskuntaan, ympäristöön ja politiikkaan liittyville asioille. Yritykset ja kuluttajat puolestaan hyötyvät tehokkaista ja vaikuttavista markkinointitekniikoista, jotka vauhdittavat taloutta. Teknologia ja henkilötietojen käsittely ovat valtion viranomaisten välttämättömiä välineitä rikollisuuden ja terrorismin torjunnassa. Myös massadata – suurten tietomäärien kerääminen, säilyttäminen ja analysointi mallien määrittämiseksi ja käytöksen ennakoimiseksi – voi olla yhteiskunnalle erittäin arvokas lähde, joka parantaa tuottavuutta, julkisen sektorin suorituskykyä ja sosiaalista osallistumista.[975]

Monista eduistaan huolimatta digitaaliaika aiheuttaa myös haasteita yksityisyyden suojalle ja tietosuojalle, koska valtavia määriä henkilötietoja kerätään ja käsitellään yhä monimutkaisemmilla ja vaikeaselkoisemmilla tavoilla. Teknologian kehittyminen on johtanut sellaisten massiivisten tietokokonaisuuksien kehittymiseen, joita voidaan helposti ristiintarkastaa ja analysoida edelleen mallien havaitsemiseksi, sekä

975 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasbourg, 23.1.2017.

algoritmeihin perustuvaan päätöksentekoon, jonka avulla voidaan saada ennennäkemätön kuva ihmisen käyttäytymisestä ja yksityiselämästä[976].

Uudet teknologiat ovat voimakkaita, ja vääriin käsiin joutuessaan ne voivat olla erityisen vaarallisia. Huomattavasta vaikutuksesta, joka näillä teknologioilla voi olla yksilöiden oikeuksiin, ovat esimerkkinä valtion viranomaiset, jotka toteuttavat joukkovalvontatoimia, joissa näitä teknologioita voidaan hyödyntää. Vuonna 2013 Edward Snowdenin paljastukset laajamittaisten internet- ja puheluseurantaohjelmien käytöstä joidenkin maiden tiedustelupalveluissa herättivät huomattavaa huolta vaaroista, joita valvontatoimet aiheuttavat yksityisyydelle, demokraattiselle hallinnolle ja sananvapaudelle. Joukkovalvonta ja teknologiat, joiden avulla henkilötietoja voidaan säilyttää ja käsitellä maailmanlaajuisesti sekä saada tietoja lajittelemattomasti saataville, voivat vaikuttaa kielteisesti yksityisyyden suojan keskeiseen sisältöön.[977] Niillä voi olla kielteisiä vaikutuksia myös poliittiseen kulttuuriin, ja ne voivat heikentää demokratiaa, luovuutta ja innovointia[978]. Pelkästään pelko siitä, että valtio voi jatkuvasti seurata ja analysoida kansalaisten käyttäytymistä ja toimia, voi saada heidät vähentämään näkemystensä ilmaisemista ja johtaa varuillaanoloon ja varovaisuuteen[979]. Nämä haasteet ovat saaneet monet viranomaiset, tutkimuskeskukset ja kansalaisjärjestöt analysoimaan uusien teknologioiden mahdollisia vaikutuksia yhteiskuntaan. Vuonna 2015 Euroopan tietosuojavaltuutettu käynnisti useita aloitteita, joiden tavoitteena on arvioida massadatan ja esineiden internetin vaikutuksia etiikkaan. Se on muun muassa perustanut eettisen neuvonantajaryhmän, joka pyrkii kannustamaan avointa ja tietoon perustuvaa keskustelua digitaalietiikasta, joka sallii yhteiskunnalle ja taloudelle EU:ssa teknologian hyödyntämisen ja vahvistaa samalla yksilön oikeuksia ja vapautta, erityisesti yksityisyyden ja tietosuojan oikeuksien osalta[980].

976 Euroopan parlamentti (2017), päätöslauselma massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta (P8_TA-PROV(2017)0076, Strasbourg, 14.3.2017.

977 Ks. YK, yleiskokous, *Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism*, Ben Emmerson, A/69/397, 23.9.2014, 59 kohta. Ks. myös EIT, *Factsheet on Mass surveillance*, heinäkuu 2017.

978 EDPS (2015), *Meeting the challenges of big data*, lausunto 7/2015, Bryssel, 19.11.2015 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee massadatan haasteita ja tarvittavaa avoimuutta, käyttäjävalvontaa, sisäänrakennettua tietosuojaa ja vastuuvelvollisuutta).

979 Ks. erityisesti EUT, yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym. ja Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014, 37 kohta.

980 Euroopan tietosuojavaltuutetun 3 päivänä joulukuuta 2015 tekemä päätös ulkoisen neuvonantajaryhmän (’eettisen neuvonantajaryhmän’) perustamisesta käsittelemään tietosuojan eettisiä ulottuvuuksia, 3.12.2015, johdanto-osan 5 kappale.

Henkilötietojen käsittely on tehokas työkalu myös yritysten käsissä. Se voi nykyään paljastaa tietoja henkilön terveydentilasta tai taloudellisesta tilanteesta, ja yritys voi sitten näiden tietojen perusteella tehdä henkilöitä koskevia tärkeitä päätöksiä, kuten heiltä perittävistä vakuutusmaksuista tai heidän luottokelpoisuudestaan. Tietojenkäsittelytekniikoilla voi olla vaikutusta myös demokraattisiin prosesseihin, kun poliitikot tai yritykset käyttävät niitä vaaleihin vaikuttamiseksi – esimerkiksi äänestäjäyhteisöjen niin sanotulla mikrokohdentamisella. Kun yksityisyyden suojaa siis alun perin pidettiin oikeutena, jolla suojellaan yksilöitä viranomaisten perusteettomalta puuttumiselta, nykyään sitä voivat uhata myös yksityisten toimijoiden valtuudet. Tämä herättää kysymyksen teknologian ja ennusteanalyysin käytöstä päätöksissä, jotka vaikuttavat ihmisten jokapäiväiseen elämään. Sen vuoksi on myös entistä tärkeämpää varmistaa, että kaikessa henkilötietojen käsittelyssä noudatetaan perusoikeuksia koskevia vaatimuksia.

Tietosuoja on teknologisen, yhteiskunnallisen ja poliittisen muutoksen olennainen osa. Tulevista haasteista on siksi mahdotonta laatia kattavaa luetteloa. Tässä luvussa käsitellään valittuja aloja, jotka koskevat massadataa, internetin verkkoyhteisöjä ja EU:n digitaalisia sisämarkkinoita. Se ei ole näiden alojen tyhjentävä arviointi tietosuojan näkökulmasta, vaan siinä korostetaan, että monenlainen vuorovaikutus on mahdollista uusien tai tarkistettujen ihmisen toimien ja tietosuojan välillä.

10.1 Massadata, algoritmit ja tekoäly

Keskeiset kohdat

- Tieto- ja viestintätekniikan murrokselliset innovaatiot muokkaavat uutta elämäntapaa, jossa sosiaaliset suhteet ja yksityiset ja julkiset palvelut liittyvät toisiinsa digitaalisesti, jolloin tuotetaan jatkuvasti enemmän tietoja, joista useat ovat henkilötietoja.
- Viranomaisten, yritysten ja kansalaisten toiminta liittyy koko ajan enemmän datavetoiseen talouteen, jossa itse tiedoista on tullut arvokkaita hyödykkeitä.
- Massadatalla tarkoitetaan sekä tietoja että niiden analysointia.
- Henkilötietojen käsittely massadata-analytiikalla kuuluu EU:n ja Euroopan neuvoston oikeuden soveltamisalaan.
- Poikkeukset tietosuojasäännöistä ja -oikeuksista rajoitetaan valittuihin oikeuksiin ja erityistilanteisiin, joissa oikeuden täytäntöönpano olisi mahdotonta tai vaatisi kohtuutonta vaivaa rekisterinpitäjiltä.

- Täysin automaattinen päätöksenteko on yleisesti kiellettyä erityistilanteita lukuun ottamatta.
- Oikeuksien täytäntöönpanon varmistamisessa keskeistä on se, että yksilöt ovat tietoisia oikeuksistaan ja valvovat niitä.

Jatkuvasti digitalisoituvassa maailmassamme kaikista toimista jää digitaalinen jälki, joka voidaan kerätä ja jota voidaan käsitellä ja arvioida tai analysoida. Uusien tieto- ja viestintätekniikoiden avulla kerätään ja tallennetaan yhä enemmän tietoa.[981] Aivan viime aikoihin asti millään tekniikalla ei ole pystytty analysoimaan tai arvioimaan tietomassoja tai tekemään hyödyllisiä johtopäätöksiä. Tietoja oli yksinkertaisesti liikaa, jotta niitä olisi voitu arvioida, ne olivat liian monimutkaisia, heikosti jäsenneltyjä ja ne liikkuivat liian nopeasti, jotta suuntauksia ja tapoja olisi voitu havaita.

10.1.1 Massadata, algoritmien ja tekoälyn määrittely

Massadata

Massadata ja iso data ovat muotisanoja, jotka voivat viitata useisiin käsitteisiin tilanteen mukaan. Niillä tarkoitetaan tavallisesti kasvavaa teknologista kykyä kerätä, käsitellä ja poimia uutta ja ennakoivaa tietoa suuresta määrästä erilaista ja liikkuvaa tietoa[982]. Massadatalla tarkoitetaan sekä tietoja että niiden analysointia.

Tiedoilla on monenlaisia **lähteitä**, muun muassa ihmiset ja heidän henkilötietonsa, koneet tai anturit, ilmastotiedot, satelliittikuvat, digitaaliset kuvat ja videot ja GPS-signaalit. Huomattava osuus tiedoista on kuitenkin henkilötietoja – nimiä, valokuvia, sähköpostiosoitteita, pankkitietoja, GPS-seurantatietoja, julkaisuja sosiaalisessa mediassa, terveystietoja tai tietokoneiden IP-osoitteita.[983]

981 Euroopan komissio, komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kohti menestyvää datavetoista taloutta COM(2014) 442 final, Bryssel, 2.7.2014.

982 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 2; Euroopan komissio, komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kohti menestyvää datavetoista taloutta COM(2014) 442 final, Bryssel, 2.7.2014, s. 4; Kansainvälinen televiestintäliitto (2015), suositus Y.3600. Big Data – Cloud computing based requirements and capabilities.

983 EU:n komission tiedote: EU:n tietosuojauudistus ja massadata; Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea: Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 2.

Massadata tarkoittaa myös tietomassojen ja saatavilla olevien tietojen **käsittelyä**, analysointia ja arviointia eli hyödyllisten tietojen hankkimista massadata-analyysia varten. Tämä tarkoittaa, että kerättyjä tietoa voidaan käyttää muihin kuin alkuperäisiin tarkoituksiin, esimerkiksi tilastosuuntauksiin tai yksilöllisempiin palveluihin, kuten mainontaan. Kun massadatan keräämiseen, käsittelyyn ja arviointiin on olemassa teknologioita, voidaan itse asiassa kerätä ja arvioida uudelleen mitä tahansa tietoja: rahoitustapahtumia, luottokelpoisuutta, lääkehoitoa, yksityistä kulutusta, ammattitoimintaa, seurantaa ja kuljettuja reittejä, internetin käyttöä, elektronisia kortteja ja älypuhelimia, videoita tai viestinnän seurantaan. Massadata-analyysi tuo tietoihin uuden määrällisen ulottuvuuden, jonka ansiosta tietoja voidaan arvioida ja käyttää reaaliajassa esimerkiksi toimittamaan yksilöllisiä palveluja kuluttajille.

Algoritmit ja tekoäly

Tekoäly (artificial intelligence, AI) tarkoittaa ”älykkäinä toimijoina” toimivien koneiden älykkyyttä. Älykkäänä toimijana tietyt laitteet pystyvät ohjelmiston tuella havainnoimaan ympäristöä ja ryhtymään toimenpiteisiin algoritmien mukaisesti. Tekoälyn käsitettä käytetään, kun kone jäljittelee ”kognitiivisia” toimintoja – kuten oppimista tai ongelmanratkaisua – jotka liittyvät tavallisesti luonnollisiin henkilöihin.[984] Päätöksenteon jäljittelyä varten nykyaikaisissa teknologioissa ja ohjelmistoissa käytetään algoritmeja, joita laitteet käyttävät ”automaattisten päätösten” tekemiseen. Algoritmia voidaan kuvata parhaiten laskentaa, tietojenkäsittelyä, arviointia sekä automaattista päättelyä ja päätöksentekoa koskevaksi yksityiskohtaiseksi menettelyksi.

Massadata-analytiikan tapaan tekoäly ja sen tuottama automaattinen päätöksenteko edellyttävät suurien tietomäärien kokoamista ja käsittelyä. Nämä tiedot voivat olla peräisin itse laitteesta (jarrujen kuumentuminen, polttoaine jne.) tai ympäristöstä. Esimerkiksi profilointi on prosessi, jossa voidaan käyttää automatisoitua päätöksentekoa ennalta määritettyjen mallien tai tekijöiden mukaisesti.

984 Stuart Russel ja Peter Norvig, *Artificial Intelligence: A Modern Approach (2. painos.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, s. 27, 32–58, 968–972; Stuart Russel ja Peter Norvig, *Artificial Intelligence: A Modern Approach (3. painos.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

Esimerkki: Profilointi ja kohdennettu mainonta

Massadataan perustuvassa profiloinnissa etsitään malleja, jotka perustuvat ”persoonallisuustyypin ominaisuuksiin” – kun esimerkiksi verkkokauppayritykset ehdottavat tuotteita, joista ”saattaisit myös pitää”, se perustuu asiakkaan ostoskoriinsa aiemmin panemista tuotteista kerättyihin tietoihin. Tietojen määrän kasvu selkeyttää kuvaa. Esimerkiksi älypuhelin on tehokas kyselylomake, jonka ihmiset täyttävät jokaisella käyttökerralla tietoisesti ja tiedostamattaan.

Modernissa psykografiassa – joka on persoonallisuutta tutkiva tiedonala – käytetään OCEAN-menetelmää, jonka perusteella määritetään käsiteltävät luonnetyypit. Viisi suurta persoonallisuuden piirrettä ovat avoimuus eli Openness (miten avoimesti henkilö suhtautuu uusiin asioihin), tunnollisuus eli Conscientiousness (miten täydellisyyttä tavoitteleva henkilö on), ulospäin suuntautuneisuus eli Extraversion (miten sosiaalinen henkilö on), sovinnollisuus eli Agreeableness (miten sovinnollinen henkilö on) ja neuroottisuus eli Neuroticism (miten herkkä henkilö on). Näillä tiedoilla profiloidaan kyseessä oleva henkilö, hänen tarpeensa ja pelkonsa, se, miten hän käyttäytyy jne. Sitten kuvaa täydennetään muilla henkilöä koskevilla tiedoilla, jotka on hankittu mistä tahansa saatavilla olevista lähteistä, kuten tietojenvälittäjiltä, sosiaalisesta mediasta (muun muassa julkaisujen tykkäyksistä ja julkaistuista kuvista), verkossa kuunnellusta musiikista tai GPS- ja seurantatiedoista.

Sitten massadatan analyysitekniikkojen avulla luotujen profiilien massaa vertaillaan, jotta voidaan havaita samanlaiset mallit ja laatia persoonallisuusryhmiä. Seuraavaksi tiettyjen persoonallisuuksien käytöstä ja asenteita koskevat tiedot muutetaan käänteisiksi. Massadataa käyttämällä persoonallisuustesti käännetään toisinpäin, jolloin käytöstä ja asenteita koskevia tietoja käytetään kuvaamaan yksilön persoonallisuutta. Kun sosiaalisen median tykkäyksistä, seurantatiedoista, kuunnellusta musiikista tai katsotuista elokuvista saadut tiedot yhdistetään, yksilön persoonallisuudesta voidaan saada selkeä kuva, jonka avulla yritykset voivat kohdistaa mainontaa ja/tai tietoja kyseisen henkilön ”persoonallisuuden” mukaan. Lisäksi tätä tietoa voidaan käsitellä reaaliajassa.[985]

985 Käsittelytekniikoilla ja uusilla ohjelmistoilla arvioidaan reaaliajassa tietoja siitä, mistä henkilö pitää tai mitä hän etsii verkkokaupoista tai lisää verkkokaupan ostoskoriin, ja ne voivat ehdottaa ”tuotteita”, jotka voisivat kiinnostaa häntä kerättyjen tietojen perusteella.

10.1.2 Massadatan etujen ja riskien punninta

Nykyaikaisilla käsittelytekniikoilla voidaan käsitellä suuria tietomassoja, tuoda nopeasti uusia tietoja, käsitellä tietoja reaaliajassa, koska vastausaika on lyhyt (myös monimutkaisissa pyynnöissä), ja lisäksi voidaan antaa mahdollisuus useisiin samanaikaisiin pyyntöihin ja voidaan analysoida erityyppisiä tietoja (kuvia, tekstejä tai numeroita). Näiden teknisten innovaatioiden ansiosta tietomassoja voidaan jäsentää, käsitellä ja arvioida reaaliajassa.[986] Koska käytettävissä ja analysoitavissa olevien tietojen määrä lisääntyy räjähdysmäisesti, nyt voidaan saavuttaa tuloksia, jotka eivät olisi mahdollisia pienimuotoisemmassa analyysissa. Massadata on auttanut luomaan uuden liiketoiminta-alan, jolla voi kehittyä uusia palveluja sekä yrityksille että kuluttajille. EU:n kansalaisten henkilötietojen arvo voi kasvaa vuodessa lähes biljoonaan euroon vuoteen 2020 mennessä.[987] Massadata tarjoaa näin ollen uusia **mahdollisuuksia**, jotka johtuvat massadatan arvioinnista sellaisia uusia sosiaalisia, taloudellisia tai tieteellisiä päätelmiä varten, joista voivat hyötyä sekä yksilöt että yritykset ja viranomaiset.[988]

Massadata-analytiikka voi paljastaa eri lähteiden ja tietokokonaisuuksien välisiä malleja, jolloin luonnontieteiden ja lääketieteen kaltaisilla aloilla voidaan tehdä hyödyllisiä päätelmiä. Tämä koskee esimerkiksi terveydenhuoltoa, elintarviketurvallisuutta, älykkäitä liikennejärjestelmiä, energiatehokkuutta tai kaavoitusta. Tällä tietojen reaaliaikaisella analyysilla voidaan parantaa käyttöön otettuja järjestelmiä. Tutkimuksessa voidaan tehdä uusia päätelmiä yhdistelemällä suuria tietomääriä ja tilastollisia arvioita, erityisesti aloilla, joilla suuri tiedoista on tähän mennessä arvioitu manuaalisesti. Yksittäisille potilaille muokattuja uusia hoitoja voidaan kehittää vertailemalla saatavilla olevaa suurta tietomäärää. Yritykset toivovat saavansa massadatan analysoinnin avulla kilpailuedun ja mahdollisesti yleisiä säästöjä sekä

986 Ohjelmiston kehittäminen massadatan käsittelyä varten on edelleen alkutekijöissään. Viime aikoina on kuitenkin kehitetty analyysiohjelmia erityisesti ihmisten toimiin liittyvien massadatan ja tietojen reaaliaikaiseen analysointiin. Mahdollisuus massadatan analysointiin ja käsittelyyn jäsennellysti on luonut uuden tavan profilointiin ja kohdennettuun mainontaan. Euroopan komissio, komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kohti menestyvää datavetoista taloutta COM(2014) 442 final, Bryssel, 2.7.2014; EU:n komission tiedote: EU:n tietosuojauudistus ja massadata; Euroopan neuvosto, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 2.

987 EU:n komission tiedote: EU:n tietosuojauudistus ja massadata.

988 Kansainvälinen tietosuojaviranomaisten maailmankokous (2014): Resolution on Big Data; Euroopan komissio, komission tiedonanto Euroopan parlamentille, neuvostolle, Euroopan talous- ja sosiaalikomitealle ja alueiden komitealle: Kohti menestyvää datavetoista taloutta COM(2014) 442 final, Bryssel, 2.7.2014; EU:n komission tiedote: EU:n tietosuojauudistus ja massadata; Euroopan neuvosto, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 1.

pystyvänsä luomaan uusia liiketoiminta-aloja suoralla ja yksilöllisellä asiakaspalvelulla. Viranomaiset toivovat saavansa parannuksia aikaan rikosoikeudessa. Komission laatimassa digitaalisten sisämarkkinoiden strategiassa Euroopalle otetaan huomioon datavetoisten teknologioiden ja palveluiden sekä massadatan mahdollisuudet toimia talouskasvun, innovoinnin ja digitalisoinnin alullepanijoina EU:ssa[989].

Massadata aiheuttaa kuitenkin myös **riskejä**. Ne liittyvät tavallisesti sen kolmeen V:hen, volyymiin, vauhtiin ja vaihtelevuuteen (englanniksi volume, velocity ja variety). Volyymi tarkoittaa käsiteltyjen tietojen määrää, vaihtelevuus eri tietotyyppien moninaisuutta ja vauhti tietojenkäsittelyn nopeutta. Tietosuoja herättää erityisiä huolenaiheita etenkin, kun massadata-analytiikkaa käytetään suurissa tietokokonaisuuksissa, jotta saadaan uutta ja ennakoivaa tietämystä yksilöitä ja/tai ryhmiä koskevaa päätöksentekoa varten[990]. Massadatan liittyviä riskejä tietosuojalle ja yksityisyyden suojalle on otettu esiin Euroopan tietosuojavaltuutetun ja tietosuojatyöryhmän lausunnoissa, Euroopan parlamentin päätöslauselmissa ja Euroopan neuvoston politiikka-asiakirjoissa[991].

Riskejä voi aiheutua muun muassa siitä, että suuriin tietomääriin pääsevät tahot käyttävät niitä väärin yksilöiden tai yhteiskunnan tiettyjen ryhmien manipulointiin, syrjintään tai sortamiseen[992]. Kun yksilön käyttäytymisestä kerätään suuria määriä henkilötietoja tai muita tietoja ja niitä käsitellään ja arvioidaan, niiden hyväksikäyttö voi johtaa merkittäviin perusoikeuksien ja -vapauksien rikkomisiin, jotka ylittävät oikeuden yksityisyyteen. Yksityisyydelle ja henkilötiedoille aiheutuvaa haittaa ei voida mitata tarkasti. Euroopan parlamentti totesi, ettei ole olemassa menetelmää, jolla voitaisiin tehdä näyttöön perustuva arviointi

989 Euroopan parlamentin päätöslauselma, annettu 14 päivänä maaliskuuta 2017, massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta (2016/2225 (INI)).

990 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 2.

991 Ks. esim. EDPS (2015), *Meeting the Challenges of big data*, lausunto 7/2015, 19.11.2015 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee massadatan haasteita ja tarvittavaa avoimuutta, käyttäjävalvontaa, sisäänrakennettua tietosuojaa ja vastuuvelvollisuutta); EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, lausunto 8/2016, 23.9.2016 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee tehokasta lainvalvontaa digitaalitaloudessa); Euroopan parlamentin päätöslauselma, annettu 14 päivänä maaliskuuta 2017, massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta, P8_TA(2017)0076, Strasbourg, 14.3.2017; Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, T-PD(2017)01, Strasbourg, 23.1.2017.

992 Kansainvälinen tietosuojaviranomaisten maailmankokous (2014): Resolution on Big Data.

massadatan kokonaisvaikutuksesta, mutta on olemassa näyttöä siitä, että massadata-analytiikalla voi olla merkittävä horisontaalinen vaikutus sekä julkisella että yksityisellä sektorilla[993].

Yleisessä tietosuoja-asetuksessa on säännöksiä siitä, että rekisteröidyllä on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn, kuten profilointiin[994]. Yksityisyyttä koskeva ongelma nousee esiin, kun vastustamisoikeuden käytössä vaaditaan, että tiedot käsittelee luonnollinen henkilö, jolloin rekisteröidyt voivat esittää kantansa ja riitauttaa päätöksen[995]. Tämä voi hankaloittaa henkilötietojen suojan asianmukaisen tason varmistamista, jos esimerkiksi luonnollisen henkilön suorittama käsittely ei ole mahdollista tai jos algoritmit ovat liian monimutkaisia ja asiaankuuluvien tietojen määrä on liian suuri, jotta henkilöille voidaan perustella tietyt päätökset ja/tai antaa ennakkotietoa heidän suostumuksensa saamiseksi. Tekoälyn ja automaattisen päätöksenteon käyttämisestä käy esimerkiksi viimeaikainen kehitys lainahakemuksissa tai rekrytointiprosesseissa. Hakemuksia hylätään tai torjutaan sen perusteella, että hakijat eivät täytä etukäteen määritettyjä muuttujia tai tekijöitä.

10.1.3 Tietosuojaan liittyvät kysymykset

Tietosuojan kannalta tärkeimpiä kysymyksiä ovat toisaalta käsiteltävien henkilötietojen määrä ja moninaisuus ja toisaalta käsittely ja sen tulokset. Kun otetaan käyttöön monimutkaisia algoritmeja ja ohjelmistoja, joilla massadata muunnetaan päätöksenteon aineistoksi, se vaikuttaa erityisesti yksilöihin ja ryhmiin, etenkin profiloinnissa ja tietoturvaluokituksessa, ja herättää loppujen lopuksi monia kysymyksiä tietosuojasta.[996]

Rekisterinpitäjien ja henkilötietojen käsittelijöiden henkilöllisyys ja heidän vastuunsa

Massadata ja tekoäly herättävät useita kysymyksiä rekisterinpitäjien ja henkilötietojen käsittelijöiden henkilöllisyydestä ja heidän vastuustaan: Kun kerätään ja käsitellään näin suuria tietomääriä, kuka omistaa tiedot? Kun tietoja käsitellään älykkäillä

993 Euroopan parlamentin päätöslauselma, annettu 14 päivänä maaliskuuta 2017, massadatan vaikutuksista perusoikeuksiin: yksityisyys, tietosuoja, syrjimättömyys, turvallisuus ja lainvalvonta (2016/2225(INI)).

994 Yleinen tietosuoja-asetus, 22 artikla.

995 *Ibid.*, 22 artiklan 3 kohta.

996 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23.1.2017, s. 2.

koneilla ja ohjelmistoilla, kuka on rekisterinpitäjä? Mitä velvollisuuksia käsittelyn kullakin toimijalla on? Entä mihin tarkoituksiin massadataa käytetään?

Vastuukysymykset tekoälyn yhteydessä hankaloituvat entisestään, kun tekoäly tekee päätöksen itse kehittämänsä tietojenkäsittelyn perusteella. Yleisessä tietosuoja-asetuksessa säädetään rekisterinpitäjän ja henkilötietojen käsittelijän vastuuta koskevasta oikeudellisesta kehyksestä. Rekisterinpitäjä ja henkilötietojen käsittelijä ovat vastuussa henkilötietojen lainvastaisesta käsittelystä.[997] Tekoäly ja automaattinen päätöksenteko herättävät kysymyksiä siitä, kuka on vastuussa rekisteröityjen yksityisyyteen vaikuttavista rikkomuksista, kun sitä ei voida määrittää tarkasti käsiteltyjen tietojen monimutkaisuuden ja määrän vuoksi. Kun tekoäly ja algoritmit katsotaan tuotteiksi, se herättää kysymyksiä siitä, onko kyseessä henkilökohtainen vastuu, josta säädetään yleisessä tietosuoja-asetuksessa, vai tuotevastuu, josta siinä ei säädetä.[998] Tämä vaatisi vastuuta koskevia sääntöjä, jotta voidaan kuroa umpeen henkilökohtaisen vastuun ja tuotevastuun välinen ero robotiikassa ja tekoälyssä, esimerkiksi automaattisessa päätöksenteossa[999].

Vaikutus tietosuojaperiaatteisiin

Edellä kuvatut massadatan luonne, analyysi ja käyttö kyseenalaistavat EU:n tietosuojalainsäädännön joidenkin perinteisten perusperiaatteiden soveltamisen[1000]. Se koskee pääasiassa lainmukaisuuden, tietojen minimoinnin, käyttötarkoitussidonnaisuuden ja avoimuuden periaatteita.

Tietojen minimoinnin periaatteen mukaan henkilötietojen on oltava asianmukaisia ja olennaisia, ja niiden on rajoituttava siihen, mikä on välttämätöntä tietojen käsittelyn tarkoituksen saavuttamiseksi. Massadataa koskeva liiketoimintamalli voi kuitenkin olla tietojen minimoinnin vastakohta, koska se vaatii koko ajan lisää tietoa, usein määrittämättömiin tarkoituksiin.

997 Yleinen tietosuoja-asetus, 77–79 artikla ja 82 artikla.

998 Euroopan parlamentti, European Civil Law Rules in Robotics, sisäasioiden pääosasto (lokakuu 2016), s. 14.

999 Roberto Violan puhe Euroopan parlamentissa pidetyssä mediaseminaarissa robotiikkaa käsittelevästä EU:n oikeudesta. (puhe 16.2.2017); Euroopan parlamentin ilmoitus komissiolle esitetystä pyynnöstä laatia ehdotus robotiikan ja tekoälyn vastuuvelvollisuutta koskevia sääntöjä.

1000 Euroopan neuvosto, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, T-PD (2017) 01, Strasbourg, 23.1.2017.

Sama koskee käyttötarkoitussidonnaisuuden periaatetta, jonka mukaan tietoja on käsiteltävä määrättyihin tarkoituksiin, eikä niitä saa käyttää tarkoituksiin, jotka ovat yhteensopimattomia keräämisen alkuperäisen tarkoituksen kanssa, paitsi jos kyseisellä käsittelyllä on oikeudellinen peruste – kuten muun muassa rekisteröidyn suostumus (ks. 4.1.1 kohta).

Massadata kyseenalaistaa myös tietojen täsmällisyyden periaatteen, koska massadatan käyttötarkoituksissa on yleensä tapana kerätä tietoja monista eri lähteistä ilman mahdollisuutta tarkastaa kerättyjen tietojen täsmällisyyttä ja/tai huolehtia siitä.[1001]

Erityissäännöt ja -oikeudet

Yleisenä sääntönä on edelleen, että massadata-analytiikan avulla käsiteltävät henkilötiedot kuuluvat tietosuojalainsäädännön soveltamisalaan. EU:n ja Euroopan neuvoston oikeudessa on kuitenkin otettu käyttöön erityisiä sääntöjä tai poikkeuksia erityistapauksissa, jotka koskevat monimutkaista tietojenkäsittelyä algoritmien perusteella.

Euroopan neuvoston oikeudessa uudistetussa yleissopimuksessa 108 rekisteröidylle annetaan uudet oikeudet valvoa henkilötietojaan entistä tehokkaammin massadatan aikakaudella. Juuri tästä on kyse esimerkiksi uudistetun yleissopimuksen 9 artiklan 1 kohdan a, c ja d alakohdassa, jotka koskevat rekisteröidyn oikeutta siihen, että häntä koskevia päätöksiä ei tehdä ainoastaan automaattisen käsittelyn perusteella ottamatta hänen omia näkemyksiään huomioon, sekä oikeutta saada pyynnöstä tietoja tietojenkäsittelyn perustaa koskevista tiedoista, kun kyseisen käsittelyn tuloksia sovelletaan häneen, ja lisäksi vastustamisoikeutta. Muut uudistetun yleissopimuksen 108 säännökset erityisesti avoimuudesta ja lisävelvollisuuksista ovat täydentäviä tekijöitä suojamekanismissa, joka on perustettu uudistetun yleissopimuksen 108 nojalla digitaalisiin haasteisiin vastaamiseksi.

EU:n oikeuden mukaan kaikessa henkilötietojen käsittelyssä on varmistettava **läpinäkyvyys** yleisen tietosuoja-asetuksen 23 artiklassa lueteltuja tapauksia lukuun ottamatta. Se on erityisen tärkeää internetpalveluissa ja muussa monimutkaisessa automaattisessa tietojenkäsittelyssä, kuten algoritmien käytössä päätöksentekoa varten. Siinä tietojenkäsittelyjärjestelmien on oltava ominaisuuksiltaan sellaisia, että

1001 EDPS (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, lausunto 8/2016, 23.9.2016, s. 8 (suomenkielinen tiivistelmä Euroopan tietosuojavaltuutetun lausunnosta, joka koskee tehokasta lainvalvontaa digitaalitaloudessa).

rekisteröidyt voivat ymmärtää kunnolla, mitä heidän tiedoilleen tapahtuu. Oikeudenmukaisen ja läpinäkyvän käsittelyn varmistamiseksi yleisessä tietosuoja-asetuksessa edellytetään, että rekisterinpitäjä antaa rekisteröidylle merkityksellistä tietoa automaattiseen päätöksentekoon, muun muassa profilointiin, liittyvästä logiikasta[1002]. Suosituksessaan sananvapauden ja yksityis- ja perhe-elämän suojaa koskevan oikeuden suojelusta ja edistämisestä verkon neutraaliuden yhteydessä Euroopan neuvoston ministerikomitea suositteli, että internetpalveluntarjoajat antavat käyttäjille selkeää, täydellistä ja julkisesti saatavilla olevaa tietoa kaikista heihin mahdollisesti vaikuttavista liikenteenhallintakäytännöistä[1003]. Toimivaltaisten viranomaisten kaikissa jäsenvaltioissa liikenteenhallintakäytännöistä laatimat raportit olisi laadittava avoimesti ja läpinäkyvästi, ja ne olisi annettava veloituksetta julkisesti saataville[1004].

Rekisterinpitäjien on **informoitava** rekisteröityjä – joko silloin, kun tietoja kerättiin heiltä, tai silloin, kun niitä ei kerätty – kerättyjä tietoja ja suunniteltua käsittelyä koskevien erityistietojen lisäksi (ks. 6.1.1 kohta) tarvittaessa myös automaattisten päätöksentekoprosessien olemassaolosta ja annettava heille ”merkityksselliset tiedot käsittelyyn liittyvästä logiikasta”[1005], tavoitteista ja kyseisen käsittelyn mahdollisista seurauksista. Yleisessä tietosuoja-asetuksessa täsmennetään myös (vain tapauksissa, joissa henkilötietoja ei ole saatu suoraan rekisteröidyltä), että rekisterinpitäjän ei tarvitse antaa rekisteröidylle kyseisiä tietoja, kun ”kyseisten tietojen toimittaminen osoittautuu mahdottomaksi tai vaatisi kohtuutonta vaivaa”[1006]. Kuten tietosuojatyöryhmä korosti *suuntaviivoissaan automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi*, monimutkaisuuden ei itsessään kuitenkaan pitäisi olla peruste olla antamatta rekisteröidylle selkeää selitystä tietojenkäsittelyn tavoitteista ja siinä käytetystä analytiikasta[1007].

Rekisteröityjen oikeudet saada **pääsy** henkilötietoihinsa, **oikaista** niitä ja **poistaa** ne sekä oikeus **rajoittaa** niiden käsittelyä eivät sisällä samanlaista poikkeusta. Rekisterinpitäjän velvollisuus ilmoittaa rekisteröidylle kaikista tämän henkilötietojen

1002 Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta.

1003 Euroopan neuvosto, ministerikomitea (2016), Recommendation CM/Rec(2016)1 of the Committee of Ministers to the member states on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, 13.1.2016, 5.1 kohta.

1004 *Ibid.*, 5.2 kohta.

1005 Yleinen tietosuoja-asetus, 13 artiklan 2 kohdan f alakohta ja 14 artiklan 2 kohdan g alakohta.

1006 *Ibid.*, 14 artiklan 5 kohdan b alakohta.

1007 Tietosuojatyöryhmä, *suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi*, WP251, 3.10.2017, s. 14.

oikaisuista tai poistamisista (ks. 6.1.4 kohta) voidaan kuitenkin myös kumota, jos kyseinen ilmoittaminen ”osoittautuu mahdottomaksi tai vaatii kohtuutonta vaivaa”[1008].

Rekisteröidyillä on yleisen tietosuoja-asetuksen 21 artiklan mukaan myös oikeus **vastustaa** (ks. 6.1.6 kohta) mitä tahansa henkilötietojensa käsittelyä, myös massadata-analytiikan yhteydessä. Vaikka rekisterinpitäjät voidaan vapauttaa tästä velvollisuudesta, jos ne pystyvät osoittamaan, että siihen on huomattavan tärkeitä ja perusteltuja syitä, samanlaista vapautusta ei voida soveltaa suoramarkkinointitarkoituksiin.

Rekisterinpitäjät voivat soveltaa erityisiä poikkeuksia näihin oikeuksiin myös, kun henkilötietoja käsitellään yleisen edun mukaisia arkistointitarkoituksia taikka tieteellisiä tai historiallisia tutkimustarkoituksia tai tilastollisia tarkoituksia varten[1009].

Yleisessä tietosuoja-asetuksessa on otettu **profilointia ja automaattista päätöksentekoa** varten käyttöön erityisiä sääntöjä: Asetuksen 22 artiklan 1 kohdassa säädetään, että rekisteröidyllä ”on oikeus olla joutumatta sellaisen päätöksen kohteeksi, joka perustuu pelkästään automaattiseen käsittelyyn […] ja jolla on häntä koskevia oikeusvaikutuksia”. Kuten tietosuojatyöryhmä korostaa, tällä artiklalla kielletään yleisesti täysin automaattinen päätöksenteko[1010]. Rekisterinpitäjä voidaan vapauttaa kyseisestä kiellosta vain kolmessa erityistapauksessa: kun päätös 1) on välttämätön rekisteröidyn ja rekisterinpitäjän välisen sopimuksen tekemistä tai täytäntöönpanoa varten, 2) on hyväksytty unionin oikeudessa tai jäsenvaltion lainsäädännössä tai 3) perustuu rekisteröidyn nimenomaiseen suostumukseen[1011].

Yksilön suorittama valvonta

Massadata-analytiikan monimutkaisuus ja siihen liittyvä avoimuuden puute voivat edellyttää, että yksilön suorittamaa henkilötietojen valvontaa koskevia käsityksiä harkitaan uudelleen. Tätä pitäisi mukauttaa kyseessä olevaan sosiaaliseen ja teknologiseen taustaan ja ottaa huomioon yksilöiden tietämyksen puute. Massadatan yhteydessä tietosuojassa pitäisi siksi omaksua kattavampi käsitys tietojen käytön

1008 Yleinen tietosuoja-asetus, 19 artikla.

1009 *Ibid.*, 89 artiklan 2 ja 3 kohta.

1010 Tietosuojatyöryhmä, *suuntaviivat automatisoiduista yksittäispäätöksistä ja profiloinnista asetuksen (EU) 2016/679 täytäntöön panemiseksi*, WP 251, 3.10.2017, s. 9.

1011 Yleinen tietosuoja-asetus, 22 artiklan 2 kohta.

valvonnasta. Sen mukaan yksilöllisestä valvonnasta kehittyy monimutkaisempi prosessi, joka sisältää useita vaikutustenarviointeja tietojen käyttöön liittyvistä riskeistä.[1012]

Massadatan käytön hyödyllisyys riippuu siitä, miten hyvin sillä pystytään ennustamaan koehenkilöiden (tai kuluttajien) haluja tai käytöstä. Massadata-analytiikkaan perustuvia nykyisiä ennustemalleja hiotaan jatkuvasti. Sen lisäksi, että tietoja käytetään luokittelemaan persoonallisuuksia (eli käytöstä ja asenteita), uusimpaan kehitykseen kuuluu myös käytöksen analysointi analysoimalla äänikuvioita ja viestien kirjoittamisen kiihkeyttä sekä ruumiinlämpötilaa. Kaikkea tätä tietoa voidaan käyttää reaaliajassa massadata-arvioinneista saadun tietämyksen perusteella esimerkiksi luottokelpoisuuden arviointiin tapaamisessa pankin edustajan kanssa. Arviointia ei tehdä lainaa hakevan henkilön ansioiden perusteella vaan massadatan tietojen analysoinnista ja arvioinnista saatujen käyttäytymisominaisuuksien perusteella eli sen perusteella, puhuuko hakija kovalla äänellä vai imartelevasti, sekä hänen kehonkielensä ja ruumiinlämpötilansa perusteella.

Profilointi ja kohdennettu mainonta eivät välttämättä aiheuta ongelmaa, jos henkilöt ovat **tietoisia** siitä, että he ovat yksilöityjen mainosten kohteena. Profilointi aiheuttaa ongelman silloin, kun sitä käytetään ihmisten manipulointiin, esimerkiksi kun poliittisessa kampanjassa otetaan kohteeksi tiettyjä persoonallisuustyyppejä tai ihmisryhmiä. Esimerkiksi päätöstään vielä miettivien äänestäjien ryhmiin voidaan ottaa yhteyttä poliittisilla viesteillä, joita on muokattu heidän ”persoonallisuutensa” ja asenteidensa mukaan. Ongelman voi aiheuttaa myös tällaisen profiloinnin käyttö tavaroiden tai palvelujen epäämiseen tietyiltä henkilöiltä. Pseudonymisointi voi tarjota suojakeinon massadatan ja henkilötietojen väärinkäyttöä vastaan (ks. 2.1.1 kohta).[1013] Kun henkilötiedot on anonymisoitu kokonaan eli rekisteröidystä ei ole tiedoissa jäljellä mitään, joka johtaisi häneen, nämä tapaukset eivät enää kuulu yleisen tietosuoja-asetuksen soveltamisalaan. Myös rekisteröityjen ja yksilöiden suostumus aiheuttaa massadatan käsittelyssä haasteen tietosuojalainsäädännölle. Se koskee suostumusta yksilölliseen mainontaan ja profilointiin, joita voidaan perustella asiakaskokemukseen liittyvistä syistä, ja suostumusta henkilötietojen suurten määrien käyttöön tietoihin perustuvien analyysityökalujen parantamiseksi ja kehittämiseksi. Tietoisuus tai tietämättömyys massadatan käsittelystä herättää useita kysymyksiä keinoista, joilla rekisteröidyt voivat käyttää näitä oikeuksiaan, koska massadatan

1012 Euroopan neuvosto, yleissopimuksen 108 neuvoa-antava komitea, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasbourg, 23.1.2017.

1013 *Ibid.*, s. 2.

käsittelyssä voidaan käyttää sekä pseudonymisoituja että anonymisoituja tietoja algoritmien perusteella. Vaikka pseudonymisoidut tiedot kuuluvat yleisen tietosuoja-asetuksen soveltamisalaan, asetusta ei sovelleta anonymisoituihin tietoihin. Yksilön suorittama valvonta ja tietoisuus omien henkilötietojen käsittelystä ovat ratkaisevan tärkeitä massadata-analytiikassa: ilman niitä yksilöllä ei ole selvää käsitystä siitä, kuka rekisterinpitäjä tai henkilötietojen käsittelijä on, ja tämä estää heitä käyttämästä oikeuksiaan tehokkaasti.

10.2 Web 2.0 ja 3.0: verkkoyhteisöt ja esineiden internet

Keskeiset kohdat

- Sosiaaliset yhteisöverkkopalvelut ovat internetin viestintäkanavia, joiden avulla henkilöt voivat liittyä samanmielisten käyttäjien verkostoihin tai luoda omia verkostoja.
- Esineiden internet tarkoittaa esineiden yhteyttä internetiin ja itse esineiden välistä yhteyttä.
- Rekisteröityjen suostumus on tavallisin oikeudellinen peruste rekisterinpitäjien suorittamalle lainmukaiselle tietojenkäsittelylle verkkoyhteisöissä.
- Verkkoyhteisöjen käyttäjiä suojataan tavallisesti ”kotitaloutta koskevalla poikkeuksella”, mutta tämä poikkeus voidaan poistaa tietyissä tilanteissa.
- Kotitaloutta koskeva poikkeus ei suojaa verkkoyhteisöpalvelujen tarjoajia.
- Sisäänrakennettu ja oletusarvoinen tietosuoja ovat ratkaisevan tärkeitä tämän alan tietoturvan varmistamisessa.

10.2.1 Web 2.0:n ja web 3.0:n määritelmät

Sosiaaliset verkkoyhteisöpalvelut

Internet suunniteltiin alun perin verkoksi, joka yhdistää tietokoneet toisiinsa ja välittää viestejä. Sen tiedonvälitysvalmiudet olivat rajalliset, ja verkkosivustoilla ihmiset pystyivät vain katselemaan passiivisesti niiden sisältöä.[1014] Web 2.0 -ajalla internet muuttui foorumiksi, jolla käyttäjät ovat keskenään vuorovaikutuksessa, tekevät

1014 Euroopan komissio (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

yhteistyötä ja luovat sisältöä. Tälle ajalle on ominaista verkkoyhteisöpalvelujen valtava menestys ja laajalle levinnyt käyttö. Ne ovat keskeinen osa miljoonien ihmisten jokapäiväistä elämää.

Sosiaaliset verkkoyhteisöpalvelut (SNS-palvelu) tai ”sosiaalinen media” voidaan yleisesti määritellä ”internetin viestintäkanavaksi, jonka avulla henkilöt voivat liittyä samanmielisten käyttäjien verkostoihin tai luoda omia verkostoja”[1015]. Verkostoon liittymistä tai sen luomista varten käyttäjiä kehotetaan esittämään henkilötietoja ja luomaan profiili. SNS-palvelussa käyttäjät voivat luoda digitaalista ”sisältöä”, kuten valokuvia ja videoleikkeitä, linkkejä sanomalehtiin ja omia julkaisuja näkemystensä esittämiseksi. Näiden internetin viestintäkanavien avulla käyttäjät voivat olla vuorovaikutuksessa ja yhteydessä useiden muiden käyttäjien kanssa. Merkittävää on, että suosituimmissa SNS-palveluissa ei ole liittymismaksuja. SNS-palvelujen tarjoajat saavat suurimman osan tuloistaan kohdennetusta mainonnasta, eivätkä ne pyydä käyttäjiä maksamaan verkostoon liittymisestä. Mainostajat voivat saada valtavaa hyötyä näillä sivustoilla päivittäin julkaistuista henkilötiedoista. Ne saavat tietoa käyttäjän iästä, sukupuolesta, sijainnista ja mielenkiinnon kohteista ja pystyvät siten saavuttamaan mainoksillaan ”oikeat” ihmiset.

Euroopan neuvoston ministerikomitea antoi suosituksen ihmisoikeuksien suojelusta sosiaalisten verkkoyhteisöpalvelujen yhteydessä.[1016] Siinä on erityinen jakso tietosuojasta ja sitä täydennettiin vuonna 2018 toisella suosituksella internetin välittäjien tehtävistä ja vastuista.[1017]

Esimerkki: Nora on erittäin onnellinen, koska hänen kumppaninsa kosi häntä. Hän haluaa jakaa hyvät uutiset ystävilleen ja perheelleen ja päättää kirjoittaa verkkoyhteisöön tunteellisen julkaisun onnestaan ja vaihtaa parisuhdetilanteekseen ”kihloissa”. Kun Nora seuraavina päivinä kirjautuu tililleen, hän näkee hääpukujen ja kukkakauppojen mainoksia. Miksi?

1015 Tietosuojatyöryhmä (2009), *lausunto 5/2009 internetin sosiaalisista verkkoyhteisöistä*, WP 163, 12.6.2009, s. 4.

1016 Euroopan neuvosto, ministerikomitea, Recommendation CM/Rec(2012)4 of the Committee of Ministers to member states on the protection of human rights with regard to social networking services, 4.4.2012.

1017 Euroopan neuvosto, ministerikomitea, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, 7.3.2018.

Kun hääpuku- ja kukkayritykset luovat mainoksen Facebookiin, ne valitsevat tiettyjä parametreja Noran kaltaisten ihmisten tavoittamiseksi. Kun Noran profiilista käy ilmi, että hän on kihloissa oleva nainen, joka asuu Pariisissa lähellä aluetta, jolla mainostavat puku- ja kukkakaupat sijaitsevat, hän näkee välittömästi mainokset.

Esineiden internet

Esineiden internet (Internet of Things, IoT), on seuraava vaihe internetin kehityksessä: web 3.0 -aika. Esineiden internetissä laitteet voidaan yhdistää toisiin laitteisiin ja ne voivat olla vuorovaikutuksessa internetin kautta. Näin esineet ja ihmiset voidaan liittää toisiinsa viestintäverkkojen avulla ja raportoida niiden tilasta ja/tai ympäristön tilasta.[1018] Esineiden internet ja liitetyt laitteet ovat jo todellisuutta, ja niiden odotetaan lisääntyvän huomattavasti muutaman seuraavan vuoden aikana, kun luodaan ja kehitetään edelleen älykkäitä laitteita, joiden avulla voidaan luoda älykkäitä kaupunkeja, älykkäitä koteja ja älykkäitä yrityksiä.

Esimerkki: Esineiden internet voi olla erityisen hyödyllinen terveydenhuollossa. Yritykset ovat jo luoneet laitteita, antureita ja sovelluksia, joiden avulla voidaan seurata potilaiden terveyttä. Käyttämällä puettavaa hälytyspainiketta ja muita kodin ympärille sijoitettuja langattomia antureita voidaan seurata yksin asuvien iäkkäiden ihmisten päivittäistä rutiinia ja tehdä hälytys, jos heidän päiväohjelmassaan havaitaan vakavia häiriöitä. Iäkkäät ihmiset käyttävät paljon esimerkiksi kaatumisen havaitsevia antureita. Nämä anturit pystyvät havaitsemaan kaatumisen tarkasti ja ilmoittamaan siitä henkilön lääkärille ja/tai perheelle.

Esimerkki: Barcelona on tunnetuimpia esimerkkejä älykkäästä kaupungista. Kaupungissa on vuodesta 2012 lähtien otettu käyttöön innovatiivisia teknologioita, joiden tarkoituksena on luoda julkisen liikenteen, jätehuollon, pysäköinnin ja katuvalaistuksen älykäs järjestelmä. Kaupungissa esimerkiksi käytetään älykkäitä jäteastioita jätehuollon parantamiseksi. Niin voidaan seurata jätetasoja ja optimoida keräysreittejä. Kun jäteastiat ovat täynnä, ne lähettävät mobiiliviestintäverkon kautta signaaleja, jotka lähetetään

1018 Euroopan komissio, komission yksiköiden valmisteluasiakirja, *Advancing the Internet of Things in Europe*, SWD(2016) 110, 19.4.2016.

jätehuoltoyrityksen käyttämään ohjelmasovellukseen. Yritys voi näin suunnitella parhaan reitin jätteenkeräystä varten tyhjentämällä ensin ja/tai pelkästään astiat, jotka todella on tyhjennettävä.

10.2.2 Etujen ja riskien punninta

SNS-palvelujen nopea leviäminen ja menestyminen viime vuosikymmenellä antavat ymmärtää niiden saavan aikaan **merkittäviä etuja**. Esimerkiksi kohdennettu mainonta (joka kuvataan edellä olevassa esimerkissä) on yrityksille erityisen innovatiivinen tapa tavoittaa yleisönsä tarjoamalla sille aiempaa täsmällisemmät markkinat. Voi myös olla kuluttajien etujen mukaista saada näkyviin mainoksia, jotka ovat heidän kannaltaan entistä merkityksellisempiä ja mielenkiintoisempia. Vielä tärkeämpää kuitenkin on, että sosiaalisilla verkkoyhteisöpalveluilla ja sosiaalisella medialla voi olla myönteinen vaikutus yhteiskuntaan ja muutoksen aikaansaamiseen. Niiden avulla käyttäjät pystyvät viestimään, toimimaan vuorovaikutuksessa ja perustamaan ryhmiä ja tapahtumia heihin vaikuttavista kysymyksistä.

Myös esineiden internetin odotetaan tuovan merkittäviä etuja taloudelle, ja se kuuluu EU:n strategiaan digitaalisten sisämarkkinoiden kehittämiseksi. Arvioiden mukaan esineiden internetin yhteyksien määrä kasvaa EU:ssa vuonna 2020 kuuteen miljardiin. Tämän liitettävyyden laajenemisen odotetaan tuovan merkittäviä taloudellisia etuja, kun voidaan kehittää innovatiivisia palveluja ja sovelluksia, parantaa terveydenhuoltoa, lisätä ymmärrystä kuluttajien tarpeista ja lisätä tehokkuutta.

Koska sosiaalisen median käyttäjät luovat valtavan määrän henkilökohtaisia tietoja, joita palveluntarjoajat sitten käsittelevät, SNS-palvelujen laajeneminen myös **lisää huolta** siitä, millä tavoin yksityisyyttä ja henkilötietoja voidaan suojata. SNS-palvelut voivat uhata oikeutta yksityis- ja perhe-elämään ja oikeutta sananvapauteen. Näitä uhkia voivat olla prosessien oikeudellisten ja menettelyllisten suojatoimien puute, joka voi johtaa käyttäjien poissulkemiseen, lasten ja nuorten riittämätön suojelu haitalliselta sisällöltä tai käytökseltä, muiden ihmisten oikeuksien kunnioituksen puute, yksityisyyden kannalta suotuisien vakioasetusten puute, henkilötietojen keräämis- ja käsittelytarkoituksia koskevan avoimuuden puute[1019]. Euroopan tietosuojalainsäädännössä on pyritty vastaamaan sosiaalisen median aikaansaamiin yksityisyyden suojaa / tietosuojaa koskeviin haasteisiin. Suostumuksen, sisäänrakennetun ja

1019 Euroopan neuvosto, Recommendation Rec(2012)4 to member states on the protection of human rights with regard to social networking services, 4.4.2012.

oletusarvoisen yksityisyyden suojan / tietosuojan kaltaiset periaatteet ovat erityisen tärkeitä sosiaalisen median ja verkkopalvelujen yhteydessä.

Esineiden internetin yhteydessä erilaisista yhteenliitetyistä laitteista tuotettujen henkilötietojen valtava määrä sisältää myös riskejä yksityisyyden suojalle ja tietosuojalle. Vaikka läpinäkyvyys on Euroopan tietosuojalainsäädännön tärkeä periaate, liitettyjen laitteiden suuren määrän vuoksi ei ole aina selvää, kuka pystyy keräämään esineiden internetin laitteista tietoa, saamaan siihen pääsyn ja käyttämään sitä.[1020] EU:n ja Euroopan neuvoston oikeudessa läpinäkyvyyden periaate edellyttää kuitenkin, että rekisterinpitäjät tiedottavat rekisteröidyille siitä, miten näiden tietoja käytetään, selkeällä ja yksinkertaisella kielellä. Kyseessä oleville yksilöille on esitettävä selkeästi heidän henkilötietojensa käsittelyyn liittyvät riskit, säännöt, suojatoimet ja oikeudet. Esineiden internetin liitetyt laitteet ja niihin liittyvät monet käsittelytoimet ja tiedot voivat myös kyseenalaistaa vaatimuksen selkeästä ja tietoisesta suostumuksesta tietojenkäsittelyyn – kun tällainen käsittely perustuu suostumukseen. Ihmiset eivät usein ymmärrä kyseisen käsittelyn teknistä toimintaa eivätkä siten suostumuksensa seurauksia.

Toinen merkittävä huolenaihe on turvallisuus, koska liitetyt laitteet ovat erityisen alttiita turvallisuusriskeille. Liitettyjen laitteiden turvallisuuden taso vaihtelee. Koska niitä ei käytetä tietotekniikan vakioinfrastruktuurissa, niissä ei ehkä ole riittävästi käsittelytehoa ja tallennusvalmiuksia, jotta niissä voitaisiin käyttää turvallisuusohjelmistoa tai salauksen, pseudonymisoinnin tai anonymisoinnin kaltaisia tekniikoita käyttäjien henkilötietojen suojaamiseksi.

Esimerkki: Saksassa sääntelyviranomaiset päättivät kieltää internetiin yhdistetyn lelun, koska lelun vaikutuksesta lasten yksityiselämään oltiin erittäin huolissaan. Sääntelyviranomaiset katsoivat, että internetiin yhdistetty Cayla-niminen nukke oli tosiasiallisesti salainen vakoilulaite. Nukke lähetti sillä leikkivän lapsen ääneen esittämiä kysymyksiä digitaalisessa laitteessa olevaan sovelluksen, joka muunsi ne tekstiksi ja haki internetistä vastausta. Sitten sovellus lähetti vastauksen nukelle, joka kertoi sen lapselle. Sovellus pystyi tallentamaan ja välittämään nuken avulla lapsen sekä lähellä olevien aikuisten viestinnän. Jos nuken valmistajat eivät olisi ottaneet käyttöön riittäviä turvatoimenpiteitä, kuka tahansa olisi voinut käyttää nukkea keskustelujen kuuntelemiseen.

1020 Euroopan tietosuojavaltuutettu (2017), *Understanding the Internet of Things.*

10.2.3 Tietosuojaan liittyvät kysymykset

Suostumus

Euroopassa henkilötietojen käsittely on lainmukaista vain, jos se on sallittu Euroopan tietosuojalainsäädännössä. SNS-palvelujen tarjoajien kannalta rekisteröityjen suostumus on tavallisesti laillinen peruste tietojenkäsittelylle. Suostumus on annettava vapaaehtoisesti, ja sen on oltava yksilöity, tietoinen ja yksiselitteinen (ks. 4.1.1 kohta).[1021] Vapaaehtoisuus tarkoittaa lähtökohtaisesti, että rekisteröityjen on voitava tehdä aito ja todellinen valinta. Suostumus on yksilöity ja tietoinen, kun se on ymmärrettävä ja siinä viitataan selkeästi ja täsmällisesti tietojenkäsittelyn koko soveltamisalaan, tarkoituksiin ja seurauksiin. Sosiaalisen median yhteydessä voidaan kyseenalaistaa, onko suostumus vapaaehtoinen, yksilöity ja tietoinen kaikkien SNS-palvelun tarjoajien ja kolmansien osapuolten suorittaman käsittelyn kaikkien tyyppien osalta.

Esimerkki: Sosiaaliseen verkkoyhteisöpalveluun liittymiseksi ja pääsemiseksi ihmisten on usein suostuttava henkilötietojensa erilaisiin käsittelyihin, usein ilman tarvittavia täsmennyksiä tai vaihtoehtoja. SNS-palveluun rekisteröitymiseksi on esimerkiksi annettava suostumus käyttötottumuksia seuraavan mainonnan vastaanottamiseen. Tietosuojatyöryhmä huomauttaa lausunnossaan suostumuksen määritelmästä seuraavaa: ”Kun otetaan huomioon joidenkin verkkoyhteisöjen tärkeä asema, eräät käyttäjäryhmät (kuten teini-ikäiset) hyväksyvät käyttötottumuksia seuraavan mainonnan, jotta niiltä ei evättäisi osaa sosiaalisen vuorovaikutuksen muodoista. Käyttäjällä on oltava mahdollisuus antaa vapaa ja yksilöity suostumus käyttötottumusten seurantaan perustuvan mainonnan vastaanottamiseen riippumatta hänen oikeudestaan käyttää verkkoyhteisöpalvelua.”[1022]

Yleisen tietosuoja-asetuksen mukaan alle 16-vuotiaiden lasten henkilötietoja ei voida periaatteessa käsitellä heidän suostumuksensa perusteella[1023]. Jos suostumus käsittelyyn on tarpeen, lapsen vanhemman tai huoltajan on annettava se. Lapset ansaitsevat erityistä suojaa, koska he eivät ehkä ole niin tietoisia tietojenkäsittelyyn

1021 Yleinen tietosuoja-asetus, 4 ja 7 artikla; uudistettu yleissopimus 108, 5 artikla.

1022 Tietosuojatyöryhmä (2011), *lausunto 15/2011 suostumuksen määritelmästä*, WP 187, Bryssel, 13.7.2011, s. 19.

1023 Ks. yleinen tietosuoja-asetus, 8 artikla. EU:n jäsenvaltiot voivat säätää alemmasta iästä, joka ei saa olla alle 13 vuotta.

liittyvistä riskeistä ja seurauksista. Tämä on erityisen tärkeää sosiaalisen median yhteydessä, koska lapset ovat alttiimpia joillekin tällaisen median mahdollisesti aiheuttamille kielteisille vaikutuksille, kuten nettikiusaamiselle, nettiahdistelulle tai identiteettivarkaudelle.

Sisäänrakennettu ja oletusarvoinen turvallisuus ja yksityisyyden suoja / tietosuoja

Henkilötietojen käsittelyyn kuuluu luonnostaan turvallisuusriskejä, koska siinä on jatkuvasti mahdollisuus tietoturvaloukkaukseen, jonka seurauksena on käsiteltyjen henkilötietojen vahingossa tapahtuva tai lainvastainen tuhoaminen, häviäminen, muuttaminen, luvaton luovuttaminen taikka pääsy tietoihin. Euroopan tietosuojalainsäädännön mukaan rekisterinpitäjien ja henkilötietojen käsittelijöiden on toteutettava tekniset ja organisatoriset toimenpiteet, joilla ehkäistään luvaton puuttuminen henkilötietojen käsittelytoimiin. Myös Euroopan tietosuojasääntöjen soveltamisalaan kuuluvien sosiaalisten verkkoyhteisöpalvelujen on noudatettava tätä velvollisuutta.

Sisäänrakennetun ja oletusarvoisen yksityisyyden suojan / tietosuojan periaatteiden mukaan rekisterinpitäjien on taattava turvallisuus tuotteidensa suunnittelussa ja sovellettava automaattisesti soveltuvia yksityisyyden suojaa ja tietosuojaa koskevia asetuksia. Tämä tarkoittaa, että kun henkilö päättää liittyä sosiaaliseen verkkoyhteisöön, palveluntarjoaja ei saa automaattisesti antaa kaikkea tietoa uudesta palvelun käyttäjästä kaikkien sen käyttäjien saataville. Palveluun liityttäessä näiden tietojen olisi oletusarvoisten yksityisyyden suojaa ja tietosuojaa koskevien asetusten perusteella oltava vain henkilön valitsemien yhteystahojen saatavilla. Tietojen saatavuuden laajentamisen heidän ulkopuolelleen pitäisi olla mahdollista vasta sen jälkeen, kun käyttäjä on manuaalisesti vaihtanut oletusarvoiset yksityisyyden suojaa ja tietosuojaa koskevat asetukset. Tämä voi vaikuttaa myös tapauksiin, joissa tietoturvaloukkaus tapahtuu käytössä olevista turvallisuustoimista huolimatta. Tällaisissa tapauksissa palveluntarjoajien on ilmoitettava asianomaisille käyttäjille, jos siihen todennäköisesti liittyy suuri riski rekisteröidyn oikeuksille ja vapauksille[1024].

Sisäänrakennettu ja oletusarvoinen yksityisyyden suoja / tietosuoja on erityisen tärkeää SNS-palvelujen yhteydessä, koska useimpiin käsittelyn tyyppeihin liittyvän luvattoman pääsyn riskien lisäksi henkilökohtaisten tietojen jakaminen sosiaalisessa mediassa aiheuttaa muita turvallisuusriskejä. Ne johtuvat usein siitä, että ihmiset

1024 *Ibid.*, 34 artikla.

eivät ymmärrä, *ketkä* voivat päästä heidän tietoihinsa ja miten nämä ihmiset voivat käyttää tietoja. Sosiaalisen median laajalle levinneen käytön myötä identiteettivarkauksien ja niiden uhrien määrä on kasvanut.

Esimerkki: Identiteettivarkaus on ilmiö, jossa henkilö saa toiselle henkilölle (uhrille) kuuluvia tietoja tai asiakirjoja ja esittää sitten näiden tietojen avulla uhria saadakseen tavaroita ja palveluita uhrin nimissä. Otetaan esimerkiksi Paul, jolla on tili sosiaalisen median verkkosivustolla. Paul on opettaja ja yhteisönsä aktiivinen jäsen, erittäin ulospäinsuuntautunut eikä kovin huolissaan sosiaalisen median tilinsä yksityisyys- ja tietosuoja-asetuksista. Hänellä on pitkä yhteystietoluettelo, johon kuuluu toisinaan myös ihmisiä, joita hän ei välttämättä tunne henkilökohtaisesti. Koska hän työskentelee isossa koulussa ja on saanut suosiota koulun jalkapallojoukkueen valmentajana, hän ajattelee näiden ihmisten olevan todennäköisesti koululaisten vanhempia tai koulun tukijoita. Paulin sähköpostiosoite ja syntymäpäivä ovat näkyvissä hänen sosiaalisen median tilillään. Paul myös julkaisee säännöllisesti kuvia koirastaan Tobysta ja kirjoittaa kuvatekstiksi esimerkiksi ”minä ja Toby aamulenkillä”. Paul ei ole tajunnut, että yksi yleisimmistä turvakysymyksistä sähköpostin tai matkapuhelintilin suojaamiseksi on: ”mikä on lemmikkisi nimi?” Nick pystyy helposti murtautumaan Paulin tileille käyttämällä Paulin sosiaalisen median profiilissa saatavilla olevia tietoja.

Yksilöiden oikeudet

SNS-palvelujen tarjoajien on kunnioitettava yksilöiden oikeuksia (ks. 6.1 kohta), myös oikeutta saada tietoa käsittelyn tarkoituksesta ja siitä, miten henkilötietoja voidaan käyttää suoramarkkinointitarkoituksiin. Yksilöille on myös annettava oikeus saada pääsy verkkoyhteisöalustalla tuottamiinsa henkilötietoihin ja pyytää niiden poistamista. Silloinkin, kun henkilöt ovat antaneet suostumuksensa henkilötietojensa käsittelyyn ja ladanneet tietoa verkkoon, heidän pitäisi voida ”tulla unohdetuiksi”, jos he eivät enää halua ottaa verkkoyhteisöpalveluja vastaan. Tietojen siirtämistä koskevan oikeuden ansiosta käyttäjät voivat saada jäljennöksen sosiaalisten verkkoyhteisöpalvelujen tarjoajalle antamistaan tiedoista jäsennellyssä, yleisesti käytetyssä ja koneellisesti luettavassa muodossa ja siirtää tietonsa yhdeltä sosiaalisten verkkoyhteisöpalvelujen tarjoajalta toiselle[1025].

1025 Yleinen tietosuoja-asetus, 21 artikla.

Rekisterinpitäjät

Sosiaalisen median yhteydessä usein esiin nouseva hankala kysymys koskee sitä, kuka rekisterinpitäjä on eli kuka on henkilö, jolla on velvollisuus ja vastuu noudattaa tietosuojasääntöjä. Euroopan tietosuojalainsäädännössä rekisterinpitäjiksi katsotaan sosiaalisten verkkoyhteisöpalvelujen tarjoajat. Tämä käy selväksi ”rekisterinpitäjän” laajasta määritelmästä sekä siitä, että nämä palveluntarjoajat määrittävät yksilöiden jakamien henkilötietojen käsittelyn tarkoituksen ja keinot. Jos rekisterinpitäjät tarjoavat palveluita EU:ssa oleville rekisteröidyille, niiden on EU:n oikeuden mukaan noudatettava yleisen tietosuoja-asetuksen säännöksiä, vaikka ne eivät olisi sijoittautuneita EU:hun.

Voidaanko kuitenkin myös sosiaalisten verkkoyhteisöpalvelujen käyttäjät katsoa rekisterinpitäjiksi? Jos yksityishenkilöt käsittelevät henkilötietoja ”yksinomaan henkilökohtaisessa tai kotitalouttaan koskevassa toiminnassa”, tietosuojasääntöjä ei sovelleta. Tätä sanotaan Euroopan tietosuojalainsäädännössä ”kotitaloutta koskevaksi poikkeukseksi”. Joissakin tapauksissa kotitaloutta koskeva poikkeus ei kuitenkaan koske sosiaalisten verkkoyhteisöpalvelujen käyttäjiä.

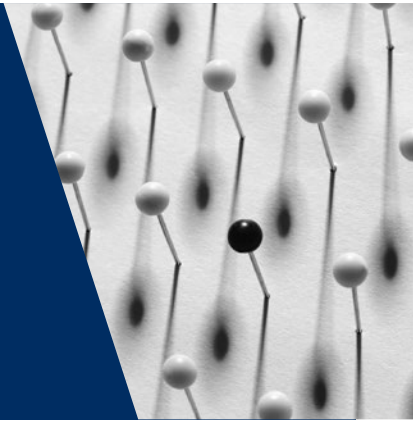
Käyttäjät jakavat tietojaan vapaaehtoisesti verkossa. Verkossa jaettaviin tietoihin sisältyy kuitenkin usein muiden henkilöiden henkilötietoja.

Esimerkki: Paulilla on tili erittäin suositulla verkkoyhteisöalustalla. Paul haluaa näyttelijäksi, ja hän käyttää tiliään taidetta kohtaan tuntemastaan intohimosta kertovien valokuvien, videoiden ja tarinoiden julkaisemiseen. Suosio on tärkeää hänen tulevaisuutensa kannalta. Hän on siksi päättänyt, että hänen profiilinsa pitäisi olla hänen lähimpien ystäviensä lisäksi kaikkien internetin käyttäjien saatavilla riippumatta siitä, ovatko he verkoston jäseniä vai eivät. Voiko Paul julkaista kuvia ja videoita itsestään ja ystävästään Sarahista ilman tämän suostumusta? Peruskoulunopettaja Sarah pyrkii pitämään yksityiselämänsä työnantajansa, oppilaidensa ja näiden vanhempien ulottumattomissa. Kuvitellaan tilanne, jossa Sarah, joka ei käytä sosiaalisia yhteisöjä, saa selville heidän yhteiseltä ystävältään Nickiltä, että verkossa oli julkaistu kuva hänestä juhlissa Paulin kanssa. Tällaisessa tapauksessa Paulin suorittama tietojenkäsittely ei kuulu EU:n oikeuden soveltamisalaan, koska tietojenkäsittelyyn sovelletaan ”kotitaloutta koskevaa poikkeusta”.

Käyttäjien on kuitenkin ratkaisevan tärkeää ymmärtää ja tiedostaa, että muita ihmisiä koskevien tietojen lataaminen ilman näiden suostumusta voi rikkoa näiden henkilöiden oikeuksia yksityisyyden suojaan ja tietosuojaan. Silloinkin, kun kotitaloutta koskevaa poikkeusta sovelletaan – jos esimerkiksi käyttäjällä on profiili, joka on annettu vain hänen valitsemiensa yhteystahojen luetteloon kuuluvien saataville – henkilökohtaisten tietojen julkaiseminen muista saattaa kuitenkin käyttäjän vastuuseen. Vaikka tietosuojasääntöjä ei sovellettaisi, jos kotitaloutta koskevaa poikkeusta sovelletaan, vastuu voi perustua muiden kansallisten sääntöjen noudattamiseen. Ne voivat koskea esimerkiksi kunnianloukkausta tai persoonallisuuden loukkausta. Kotitaloutta koskevat poikkeukset suojaavat lisäksi vain SNS-palvelujen käyttäjiä: kyseiseen yksityiseen käsittelyyn keinot tarjoavat rekisterinpitäjät ja henkilötietojen käsittelijät kuuluvat EU:n tietosuojaoikeuden piiriin[1026].

Sähköisen viestinnän tietosuojadirektiivin uudistuksen myötä nykyisessä oikeudellisessa kehyksessä televiestintäpalvelujen tarjoajiin sovellettavia tietosuojaa, yksityisyyden suojaa ja turvallisuutta koskevia sääntöjä sovellettaisiin myös koneiden väliseen viestintään ja sähköisiin viestintäpalveluihin, myös avoimen internetin kautta tapahtuviin jakelupalveluihin.

1026 *Ibid.*, johdanto-osan 18 kappale.



Kirjallisuutta

Luku 1

Araceli Mangas, M. (toim.) (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*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. ”Four fundamental rights: finding the balance”, *International Data Privacy Law*, nide 6, nro 3, s. 195–209.

EDRi, *An introduction to data protection*, Bryssel.

Frowein, J. ja Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berliini, N. P. Engel Verlag.

Grabenwarter, C. ja Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

González Fuster, G. ja 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*, nide 26 (1), s. 73–82.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. ja Nouwt, S. (toim.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. ja 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. ja Sobotta, C. (2013), "The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, nide 3, nro 4, s. 222–228.

Kranenborg, H. (2015), "Google and the Right to be Forgotten", *European Data Protection Law Review*, nide. 1, nro 1, s. 70–79.

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*, nide 63, nro 3, s. 569–597.

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. ja Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpen, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. ja Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bryssel, Emile Bruylant.

Simitis, S. (1997), ”Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?”, *Neue Juristische Wochenschrift*, nro 5, s. 281–288.

Warren, S. ja Brandeis, L. (1890), ”The right to privacy”, *Harvard Law Review,* nide 4, nro 5, s. 193–220.

White, R. ja Ovey, C. (2010), *The European Convention on Human Rights*, Oxford, Oxford University Press.

Luku 2

Acquisty, A., ja Gross R. (2009), ”Predicting Social Security numbers from public data”, *Proceedings of the National Academy of Science*, 7.7.2009.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oxford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M., ja Blondel V. D. (2013), ”Unique in the Crowd: the Privacy Bounds of Human Mobility”, *Nature Scientific Reports*, nide 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Pariisi, 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. ja Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Lontoo, Sweet & Maxwell.

Ohm, P. (2010), ”Broken promises of privacy: Responding to the surprising failure of anonymization”, *UCLA Law Review*, nide 57, nro 6, s. 1701–1777.

Samarati, P. ja Sweeney, L. (1998), "Protecting Privacy when Disclosing Information: k-Anonymity and Its Enforcement through Generalization and Suppression", 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*, nide 10, nro 5, s. 557–570.

Tinnefeld, M., Buchner, B. ja 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*.

Luvut 3–6

Brühann, U. (2012), "Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" teoksessa Grabitz, E., Hilf, M. ja Nettesheim, M. (toim.), *Das Recht der Europäischen Union*, Band IV, A. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. ja Kaye, J. (2010), "Revoking consent: a 'blind spot' in data protection law?", *Computer Law & Security Review*, nide 26, nro 3 s. 273–283.

Dammann, U. ja Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. ja Papakonstantinou, V. (2012), "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, nide 22, nro 6, s. 1–5.

De Hert, P. ja 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*, nide 28, nro 2, s. 130–142.

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*, nide 20, nro 2, s. 473–506.

FRA (Euroopan perusoikeusvirasto) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luxemburg, Euroopan unionin julkaisutoimisto.

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (painos konferenssia varten), Wien, FRA.

FRA (2011), Access to justice in Europe: an overview of challenges and opportunities, Luxemburg, Euroopan unionin julkaisutoimisto.

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. ja Saxby, S. (2011), "30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, nide 27, nro 3, s. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment*.

Luku 7

Euroopan tietosuojavaltuutettu (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. ja Nouwt, S. (2009), *Reinventing data protection?*, Berliini, 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.

Tietosuojatyöryhmä (2005), *valmisteluasiakirja 24. lokakuuta 1995 annetun direktiivin 95/46/EY 26 artiklan 1 kohdan yhteisestä tulkinnasta*.

Luku 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Lontoo, 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,* Berliini, Springer.

De Hert, P. ja Papakonstantinou, V. (2012), "The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, nide 22, nro 6, s. 1–5.

Drewer, D. ja Ellermann, J. (2012), "Europol's data protection framework as an asset in the fight against cybercrime"*, ERA Forum*, nide 13, nro 3, s. 381–395.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haag, Eurojust.

Europol (2012), *Data Protection at Europol*, Luxemburg, Euroopan unionin julkaisutoimisto.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berliini, Springer.

Gutwirth, S., Poullet, Y. ja De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. ja Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, 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*, nide 36, nro 5, s. 722–776.

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 External Relations, CLEER Working Papers 2013/2.

Luku 9

Büllesbach, A., Gijrath, S., Poullet, Y. ja Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Poullet, Y. ja De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. ja Leenes, R. (2011), *Computers, privacy and data protection: An element of choice*, Dordrecht, Springer.

Gutwirth, S., Leenes, R., De Hert, P. ja Poullet, Y. (2012), *European data protection: In good health?*, 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*, nide 36, nro 5, s. 722–776.

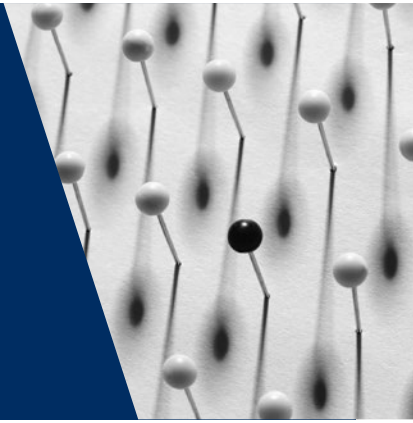
Rosemary, J. ja Hamilton, A. (2012), *Data protection law and practice*, London, Sweet & Maxwell.

Luku 10

El Emam, K. ja Álvarez, C. (2015), "A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, nide 5, nro 1, s. 73–87.

Mayer-Schönberger, V. ja Cate, F. (2013), "Notice and consent in a world of Big Data", *International Data Privacy Law*, nide 3, nro 2, s. 67–73.

Rubistein, I. (2013), "Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, nide 3, nro 2, s. 74–87.



Oikeuskäytäntö

Euroopan ihmisoikeustuomioistuimen valittu oikeuskäytäntö

Pääsy henkilötietoihin
Gaskin v. Yhdistynyt kuningaskunta, nro 10454/83, 7.7.1989
Godelli v. Italia, nro 33783/09, 25.9.2012
K.H. ym. v. Slovakia, nro 32881/04, 28.4.2009
Leander v. Ruotsi, nro 9248/81, 26.3.1987
M.K. v. Ranska, nro 19522/09, 18.4.2013
Odièvre v. Ranska [suuri jaosto], nro 42326/98, 13.2.2003

Tietosuojan punninta sananvapauden ja tiedonsaantioikeuden kanssa
Axel Springer AG v. Saksa [suuri jaosto], nro 39954/08, 7.2.2012
Bohlen v. Saksa, nro 53495/09, 19.2.2015
Coudec ja Hachette Filipacchi Associés v. Ranska [suuri jaosto], nro 40454/07, 10.11.2015
Magyar Helsinki Bizottság v. Unkari [suuri jaosto], nro 18030/11, 8.11.2016
Müller ym. v. Sveitsi, nro 10737/84, 24.5.1988
Satakunnan Markkinapörssi Oy ja Satamedia Oy v. Suomi [suuri jaosto], nro 931/13, 27.6.2017
Vereinigung bildender Künstler v. Itävalta, nro 68345/01, 25.1.2007
Von Hannover v. Saksa (nro 2) [suuri jaosto], nrot 40660/08 ja 60641/08, 7.2.2012

Tietosuojan ja uskonnonvapauden punninta
Sinan Işık v. Turkki, nro 21924/05, 2.2.2010

Verkkotietosuojan haasteet
K.U. v. Suomi, nro 2872/02, 2.12.2008

Rekisteröidyn suostumus
Elberte v. Latvia, nro 61243/08, 13.1.2015
Sinan Işık v. Turkki, nro 21924/05, 2.2.2010
Y v. Turkki, nro 648/10, 17.2.2015

Kirjeenvaihto
Amann v. Sveitsi [suuri jaosto], nro 27798/95, 16.2.2000
Association for European Integration and Human Rights ja Ekimdzhiev v. Bulgaria, nro 62540/00, 28.6.2007
Bernh Larsen Holding AS ym. v. Norja, nro 24117/08, 14.3.2013
Cemalettin Canli v. Turkki, nro 22427/04, 18.11.2008
D.L. v. Bulgaria, nro 7472/14, 19.5.2016
Dalea v. Ranska, nro 964/07, 2.2.2010
Gaskin v. Yhdistynyt kuningaskunta, nro 10454/83, 7.7.1989
Haralambie v. Romania, nro 21737/03, 27.10.2009
Khelili v. Sveitsi, nro 16188/07, 18.10.2011
Leander v. Ruotsi, nro 9248/81, 26.3.1987
Malone v. Yhdistynyt kuningaskunta, nro 8691/79, 2.8.1984
Rotaru v. Romania [suuri jaosto], nro 28341/95, 4.5.2000
S. ja Marper v. Yhdistynyt kuningaskunta [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008
Shimovolos v. Venäjä, nro 30194/09, 21.6.2011
Silver ym. v. Yhdistynyt kuningaskunta, nrot 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25.3.1983
The Sunday Times v. Yhdistynyt kuningaskunta, nro 6538/74, 26.4.1979

Rikosrekisteritietokannat
Aycaguer v. Ranska, nro 8806/12, 22.6.2017
B.B. v. Ranska, nro 5335/06, 17.12.2009
Brunet v. Ranska, nro 21010/10, 18.9.2014
M.K. v. Ranska, nro 19522/09, 18.4.2013
M.M. v. Yhdistynyt kuningaskunta, nro 24029/07, 13.11.2012

Tietoturva
Haralambie v. Romania, nro 21737/03, 27.10.2009
K.H. ym. v. Slovakia, nro 32881/04, 28.4.2009

Dna-tietokannat
S. ja Marper v. Yhdistynyt kuningaskunta [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008

GPS-tiedot
Uzun v. Saksa, nro 35623/05, 2.9.2010

Terveydentilaa koskevat tiedot
Avilkina ym. v. Venäjä, nro 1585/09, 6.6.2013
Biriuk v. Liettua, nro 23373/03, 25.11.2008
I v. Suomi, nro 20511/03, 17.7.2008
L.H. v. Latvia, nro 52019/07, 29.4.2014
L.L. v. Ranska, nro 7508/02, 10.10.2006
M.S. v. Ruotsi, nro 20837/92, 27.8.1997
Szuluk v. Yhdistynyt kuningaskunta, nro 36936/05, 2.6.2009
Y v. Turkki, nro 648/10, 17.2.2015
Z v. Suomi, nro 22009/93, 25.2.1997

Henkilöllisyys
Ciubotaru v. Moldova, nro 27138/04, 27.4.2010
Godelli v. Italia, nro 33783/09, 25.9.2012
Odièvre v. Ranska [suuri jaosto], nro 42326/98, 13.2.2003

Työelämää koskevat tiedot
G.S.B. v. Sveitsi, nro 28601/11, 22.12.2015
M.N. ym. v. San Marino, nro 28005/12, 7.7.2015
Michaud v. Ranska, nro 12323/11, 6.12.2012
Niemietz v. Saksa, nro 13710/88, 16.12.1992

Telekuuntelu
Amann v. Sveitsi [suuri jaosto], nro 27798/95, 16.2.2000
Brito Ferrinho Bexiga Villa-Nova v. Portugali, nro 69436/10, 1.12.2015
Copland v. Yhdistynyt kuningaskunta, nro 62617/00, 3.4.2007
Halford v. Yhdistynyt kuningaskunta, nro 20605/92, 25.6.1997
Iordachi ym. v. Moldova, nro 25198/02, 10.2.2009

Kopp v. Sveitsi, nro 23224/94, 25.3.1998
Liberty ym. v. Yhdistynyt kuningaskunta, nro 58243/00, 1.7.2008
Malone v. Yhdistynyt kuningaskunta, nro 8691/79, 2.8.1984
Mustafa Sezgin Tanrıkulu v. Turkki, nro 27473/06, 18.7.2017
Pruteanu v. Romania, nro 30181/05, 3.2.2015
Szuluk v. Yhdistynyt kuningaskunta, nro 36936/05, 2.6.2009

Sääntöjen noudattamisen valvojien velvollisuudet
B.B. v. Ranska, nro 5335/06, 17.12.2009
I v. Suomi, nro 20511/03, 17.7.2008
Mosley v. Yhdistynyt kuningaskunta, nro 48009/08, 10.5.2011

Henkilötiedot
Amann v. Sveitsi [suuri jaosto], nro 27798/95, 16.2.2000
Bernh Larsen Holding AS ym. v. Norja, nro 24117/08, 14.3.2013
Uzun v. Saksa, nro 35623/05, 2010

Valokuvat
Sciacca v. Italia, nro 50774/99, 11.1.2005
Von Hannover v. Saksa, nro 59320/00, 24.6.2004

Oikeus tulla unohdetuksi
Segerstedt-Wiberg ym. v. Ruotsi, nro 62332/00, 6.6.2006
Satakunnan Markkinapörssi Oy ja Satamedia Oy v. Suomi [suuri jaosto], nro 931/13, 27.6.2017

Vastustamisoikeus
Leander v. Ruotsi, nro 9248/81, 26.3.1987
M.S. v. Ruotsi, nro 20837/92, 27.8.1997
Mosley v. Yhdistynyt kuningaskunta, nro 48009/08, 10.5.2011
Rotaru v. Romania [suuri jaosto], nro 28341/95, 4.5.2000
Sinan Işık v. Turkki, nro 21924/05, 2.2.2010

Arkaluonteiset tietoryhmät
Brunet v. Ranska, nro 21010/10, 18.9.2014
I v. Suomi, nro 20511/03, 17.7.2008
Michaud v. Ranska, nro 12323/11, 6.12.2012
S. ja Marper v. Yhdistynyt kuningaskunta [suuri jaosto], nrot 30562/04 ja 30566/04, 4.12.2008

Valvonta ja täytäntöönpano (eri toimijoiden, myös valvontaviranomaisten, asema)
I v. Suomi, nro 20511/03, 17.7.2008
K.U. v. Suomi, nro 2872/02, 2.12.2008
Von Hannover v. Saksa, nro 59320/00, 24.6.2004
Von Hannover v. Saksa (nro 2) [suuri jaosto], nrot 40660/08 ja 60641/08, 7.2.2012

Seurantamenetelmät
Allan v. Yhdistynyt kuningaskunta, nro 48539/99, 5.11.2002
Association for European Integration and Human Rights ja Ekimdzhiev v. Bulgaria, nro 62540/00, 28.6.2007
Bărbulescu v. Romania [suuri jaosto], nro 61496/08, 5.9.2017
D.L. v. Bulgaria, nro 7472/14, 19.5.2016
Dragojević v. Kroatia, nro 68955/11, 15.1.2015
Karabeyoğlu v. Turkki, nro 30083/10, 7.6.2016
Klass ym. v. Saksa, nro 5029/71, 6.9.1978
Roman Zakharov v. Venäjä [suuri jaosto], nro 47143/06, 4.12.2015
Rotaru v. Romania [suuri jaosto], nro 28341/95, 4.5.2000
Szabó ja Vissy v. Unkari, nro 37138/14, 12.1.2016
Taylor-Sabori v. Yhdistynyt kuningaskunta, nro 47114/99, 22.10.2002
Uzun v. Saksa, nro 35623/05, 2.9.2010
Versini-Campinchi ja Crasnianski v. Ranska, nro 49176/11, 16.6.2016
Vetter v. Ranska, nro 59842/00, 31.5.2005
Vukota-Bojić v. Sveitsi, nro 61838/10, 18.10.2016

Videovalvonta
Köpke v. Saksa (päätös), nro 420/07, 5.10.2010
Peck v. Yhdistynyt kuningaskunta, nro 44647/98, 28.1.2003

Ääninäytteet
P.G. ja J.H. v. Yhdistynyt kuningaskunta, No. 44787/98, 25.9.2001
Wisse v. Ranska, nro 71611/01, 20.12.2005

Euroopan unionin tuomioistuimen valittu oikeuskäytäntö

Tietosuojadirektiiviin liittyvä oikeuskäytäntö

Yhdistetyt asiat C-468/10 ja C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) ja Federación de Comercio Electrónico y Marketing Directo (FECEMD) vastaan Administración del Estado*, 24.11.2011
[tietosuojadirektiivin 7 artiklan f alakohdan moitteeton soveltaminen – muiden oikeutetut edut – kansallisessa lainsäädännössä]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) vastaan Netlog NV*, 16.2.2012
[Sosiaalisten yhteisöverkkojen tarjoajien velvollisuus estää musiikkitallenteiden ja audiovisuaalisten tallenteiden lainvastainen käyttö]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce v. Salvatore Manni*, 9.3.2017
[oikeus henkilötietojen poistamiseen; oikeus vastustaa käsittelyä]

C-553/07, *College van burgemeester en wethouders van Rotterdam vastaan E. E. Rijkeboer*, 7.5.2009
[rekisteröidyn oikeus saada pääsy tietoihin]

C-543/09, *Deutsche Telekom AG vastaan Bundesrepublik Deutschland*, 5.5.2011
[suostumuksen uusimisen tarve]

Yhdistetyt asiat C-293/12 ja C-594/12, *Digital Rights Ireland Ltd vastaan Minister for Communications, Marine and Natural Resources ym.* ja *Kärntner Landesregierung ym.* [suuri jaosto], 8.4.2014
[EU:n primäärilainsäädännön loukkaaminen tietojen säilyttämistä koskevalla direktiivillä; lainmukainen käsittely; tarkoituksen ja säilytyksen rajoittaminen]

C-614/10, *Euroopan komissio vastaan Itävallan tasavalta* [suuri jaosto], 16.10.2012
[kansallisten valvontaviranomaisten riippumattomuus]

C-518/07, *Euroopan komissio vastaan Saksan liittotasavalta* [suuri jaosto], 9.3.2010
[kansallisten valvontaviranomaisten riippumattomuus]

C-288/12, *Euroopan komissio vastaan Unkari* [suuri jaosto], 8.4.2014
[kansallisen tietosuojaviranomaisen virasta poistamisen oikeutus]

C-212/13, *František Ryneš v. Úřad pro ochranu osobních údajů*, 11.12.2014
[tietojenkäsittelyn ja rekisterinpitäjän käsitteet]

C-131/12, *Google Spain SL ja Google Inc. vastaan Agencia Española de Protección de Datos (AEPD) ja Mario Costeja González* [suuri jaosto], 13.5.2014
[hakukoneen ylläpitäjän velvollisuudet pidättäytyä rekisteröidyn pyynnöstä näyttämästä henkilötietoja hakutuloksissa; tietosuojadirektiivin sovellettavuus; tietojenkäsittelyn käsite, rekisterinpitäjin merkitys; tietosuojan punninta sananvapauden kanssa; oikeus tulla unohdetuksi]

C-524/06, *Heinz Huber vastaan Bundesrepublik Deutschland [suuri jaosto]*, 16.12.2008
[oikeutus ulkomaalaisten tietojen pitämiselle tilastorekisterissä]

C-473/12, *Institut professionnel des agents immobiliers (IPI) vastaan Geoffrey Englebert ym.*, 7.11.2013
[oikeus saada tietoa henkilötietojen käsittelystä]

C-362/14, *Maximillian Schrems vastaan Data Protection Commissioner* [suuri jaosto], 6.10.2015
[lainmukaisen käsittelyn periaate; perusoikeudet; safe harbor -päätöksen pätemättömyys; riippumattomien valvontaviranomaisten toimivalta]

C-291/12, *Michael Schwarz v. Stadt Bochum*, 17.10.2013
[viittaus ennakkoratkaisuun; vapauden, turvallisuuden ja oikeuden alue; biometrinen passi; sormenjäljet; oikeusperusta; oikeasuhteisuus]

C-582/14, *Patrick Breyer v. Bundesrepublik Deutschland*, 19.10.2016
[henkilötietojen määritelmä; IP-osoitteet; verkkomediapalvelujen tarjoajan suorittama tietojen tallentaminen; kansallisessa lainsäädännössä ei sallita rekisterinpitäjän oikeutetun edun huomioon ottamista]

C-434/16, *Peter Nowak v. Data Protection Commissioner*, julkisasiamies Kokottin ratkaisuehdotus, 20.7.2017
[henkilötietojen käsite; pääsy omiin koetuloksiin; tarkastajan korjaukset]

T-462/12 R, *Pilkington Group Ltd vastaan Euroopan komissio*, unionin yleisen tuomioistuimen presidentin määräys, 11.3.2013

C-275/06, *Productores de Música de España (Promusicae) v. Telefónica de España SAU* [suuri jaosto], 29.1.2008

[henkilötietojen käsite; internetyhteyden tarjoajien velvollisuus julkaista KaZaA-tiedostonvaihto-ohjelmien käyttäjien henkilöllisyys teollis- ja tekijänoikeuksien suojeluyhdistykselle]

Yhdistetyt asiat C-465/00, C-138/01 ja C-139/01, *Rechnungshof vastaan Österreichischer Rundfunk ym. ja Christa Neukomm ja Joseph Lauermann vastaan Österreichischer Rundfunk*, 20.5.2003

[julkiseen sektoriin liittyvien laitosten tiettyjen työntekijäryhmien henkilökohtaisten palkkatietojen julkaisemista koskevan lakisääteisen velvollisuuden oikeasuhteisuus]

C-101/01, *Rikosoikeudenkäynti vastaan Bodil Lindqvist*, 6.11.2003

[erityiset henkilötietoryhmät]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24.11.2011

[tietoyhteiskunta; tekijänoikeus; internet; vertaisohjelmistot; internetpalveluntarjoajat; sähköistä viestintää suodattavan järjestelmän asentaminen tekijänoikeutta rikkovien tiedostojen jakamisen estämiseksi]

C-201/14, *Smaranda Bara ym. vastaan Casa Națională de Asigurări de Sănătate ym.*, 1.10.2015

[oikeus saada tietoa henkilötietojen käsittelystä]

Yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB vastaan Post- och telestyrelsen* ja *Secretary of State for the Home Department vastaan Tom Watson ym.* [suuri jaosto], 21.12.2016

[sähköisen viestinnän luottamuksellisuus; sähköisten viestintäpalvelujen tarjoajat; liikenne- ja sijaintitietojen yleistä ja syrjimätöntä säilyttämistä koskeva velvollisuus; ei tuomioistuimen tai itsenäisen hallinnollisen yksikön etukäteistä tarkastusta; Euroopan unionin perusoikeuskirja; yhteensopivuus EU:n oikeuden kanssa]

C-73/07, *Tietosuojavaltuutettu v. Satakunnan Markkinapörssi Oy ja Satamedia Oy* [suuri jaosto], 16.12.2008

[tietosuojadirektiivin 9 artiklassa tarkoitettujen journalististen toimintojen käsite]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde vastaan Rīgas pašvaldības SIA "Rīgas satiksme"*, 4.5.2017
[lainmukaisen käsittelyn periaate; kolmannen osapuolen oikeutettu etu]

Yhdistetyt asiat C-92/09 ja C-93/09, *Volker und Markus Schecke GbR ja Hartmut Eifert v. Land Hessen* [suuri jaosto], 9.11.2010
[henkilötietojen käsite; henkilötietojen julkaisemista tiettyjen EU:n maatalousrahastojen tuensaajista koskevan velvollisuuden oikeasuhteisuus]

C-230/14, *Weltimmo s. r. o. vastaan Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1.10.2015
[kansallisten valvontaviranomaisten toimivalta]

C-342/12, *Worten – Equipamentos para o Lar SA vastaan Autoridade para as Condições de Trabalho (ACT)*, 30.5.2013
[henkilötietojen käsite; työaikarekisteri; tietojen laatuun liittyvät periaatteet ja tietojenkäsittelyn lainmukaiseksi saattamista koskevat kriteerit; työsuojeluviranomaisen pääsy tietoihin; työnantajan velvollisuus antaa työaikarekisterit saataville välitöntä tutustumista varten]

Yhdistetyt asiat C-141/12 ja C-372/12, *YS vastaan Minister voor Immigratie, Integratie en Asiel ja Minister voor Immigratie, Integratie en Asiel vastaan M ja S*, 17.7.2014
[rekisteröidyn tietoihin pääsyä koskevan oikeuden soveltamisala; yksilöiden suojelu henkilötietojen käsittelyn yhteydessä; henkilötietojen käsite; oleskeluluvan hakijaan liittyvät tiedot ja päätöksen hallinnollisen valmisteluasiakirjan sisältämä oikeudellinen analyysi; Euroopan unionin perusoikeuskirja]

Direktiiviin (EU) 2016/681 liittyvä oikeuskäytäntö

Unionin tuomioistuimen lausunto 1/15 (suuri jaosto), 26.7.2017
[oikeusperusta; ehdotus Kanadan ja Euroopan unionin väliseksi sopimukseksi matkustajarekisteritietojen siirtämisestä ja käsittelemisestä; sopimusehdotuksen yhteensopivuus SEUT-sopimuksen 16 artiklan ja Euroopan unionin perusoikeuskirjan 7 ja 8 artiklan ja 52 artiklan 1 kohdan kanssa]

EU:n toimielinten tietosuoja-asetukseen liittyvä oikeuskäytäntö

C-615/13 P, *ClientEarth ja Pesticide Action Network Europe (PAN Europe) vastaan Euroopan elintarviketurvallisuusviranomainen, Euroopan komissio, 16.7.2015*
[asiakirjojen saatavuus]

C-28/08 P, *Euroopan komissio vastaan The Bavarian Lager Co. Ltd.* [suuri jaosto], 29.6.2010
[asiakirjojen saatavuus]

Direktiiviin 2002/58/EY liittyvä oikeuskäytäntö

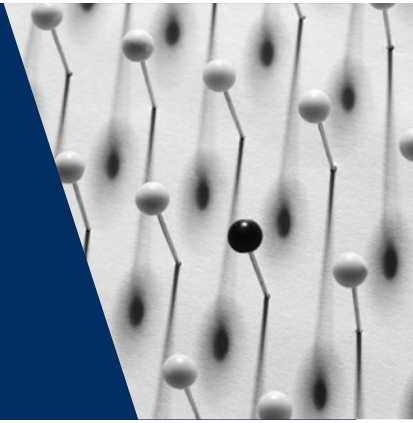
C-461/10, *Bonnier Audio AB ym. vastaan Perfect Communication Sweden AB*, 19.4.2012
[tekijänoikeus ja sen lähioikeudet; tietojenkäsittely internetissä; yksinoikeuden rikkominen; FTP-palvelimella internetissä internetpalveluntarjoajan toimittaman IP-osoitteen kautta saataville annetut äänikirjat; internetpalveluntarjoajalle annettu kieltomääräys, jolla määrätään se antamaan IP-osoitteen käyttäjän nimi ja osoite]

C-70/10, *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24.11.2011
[tietoyhteiskunta; tekijänoikeus; internet; vertaisohjelmistot; internetpalveluntarjoajat; sähköistä viestintää suodattavan järjestelmän asentaminen tekijänoikeutta rikkovien tiedostojen jakamisen estämiseksi]

C-536/15, *Tele2 (Netherlands) BV ym. vastaan Autoriteit Consument en Markt (AMC)*, 15.3.2017
[syrjimättömyysperiaate; tilaajia koskevien henkilötietojen antaminen saataville julkisesti saatavilla olevien numerotiedotus- ja puhelinluettelopalvelujen tarjoamista varten; tilaajan suostumus; erottelu sen jäsenvaltion perusteella, jossa julkisesti saatavilla olevat numerotiedotus- ja puhelinluettelopalvelut tarjotaan]

Yhdistetyt asiat C-203/15 ja C-698/15, *Tele2 Sverige AB vastaan Post- och telestyrelsen* ja *Secretary of State for the Home Department vastaan Tom Watson ym.* [suuri jaosto], 21.12.2016
[sähköisen viestinnän luottamuksellisuus; sähköisten viestintäpalvelujen tarjoajat; liikenne- ja sijaintitietojen yleistä ja syrjimätöntä säilyttämistä koskeva velvollisuus; ei tuomioistuimen tai itsenäisen hallinnollisen yksikön etukäteistä tarkastusta; Euroopan unionin perusoikeuskirja; yhteensopivuus EU:n oikeuden kanssa]

Hakemisto



Euroopan unionin tuomioistuimen oikeuskäytäntö

Euroopan ihmisoikeustuomioistuimen oikeuskäytäntö

Kansallisten tuomioistuinten oikeuskäytäntö

Euroopan unionin perusoikeusvirastosta on runsaasti tietoa internetissä. Siihen pääsee tutustumaan perusoikeusviraston (FRA) verkkosivustolla osoitteessa fra.europa.eu.

Euroopan ihmisoikeustuomioistuimen oikeuskäytännöstä on lisätietoa tuomioistuimen verkkosivustolla osoitteessa echr.coe.int. HUDOC-hakuportaalissa on tuomiot ja päätökset englanniksi ja/tai ranskaksi sekä käännöksiä muille kielille, tiivistelmiä, lehdistötiedotteita ja muuta tietoa tuomioistuimen työstä.

Miten hankkia Euroopan neuvoston julkaisuja?

Euroopan neuvoston kustantamo julkaisee teoksia kaikilta organisaation eri osa-alueilta, kuten ihmisoikeuksista, oikeustieteestä, terveydestä, etiikasta, sosiaaliasioista, ympäristöstä, koulutuksesta, kulttuurista, urheilusta, nuorisosta ja kulttuuriperinnöstä. Kirjoja ja elektronisia julkaisuja voi tilata laajasta luettelosta verkosta (http://book.coe.int/).

Virtuaalilukuhuoneessa käyttäjät voivat maksutta tutustua hiljattain ilmestyneiden tärkeimpien teosten lyhennelmiin tai tiettyihin virallisiin asiakirjoihin kokonaisuudessaan.

Tietoa Euroopan neuvoston yleissopimuksista sekä niiden tekstit kokonaisuudessaan ovat saatavilla sopimustoimiston verkkosivustolla osoitteessa http://conventions.coe.int/.

EU:n yhteystiedot

Henkilökohtaisesti

Ympäri Euroopan unionia on satoja Europe Direct -tiedotuskeskuksia. Lähimmän keskuksen osoitteen saa sivulta https://europa.eu/european-union/contact_fi.

Puhelimitse tai sähköpostitse

Europa Direct -palvelun avulla löydät vastaukset Euroopan unionia koskeviin kysymyksiisi. Palveluun voi ottaa yhteyttä
– maksuttomaan puhelinnumeroon 00 800 6 7 8 9 10 11 (jotkin operaattorit voivat veloittaa maksun näistä puheluista),
– seuraavaan tavanomaiseen puhelinnumeroon: +32 22999696 tai,
– sähköpostitse osoitteessa https://europa.eu/european-union/contact_fi.

Tietoa EU:sta

Verkossa

Euroopan unionista on tietoa kaikilla EU:n virallisilla kielillä Europa-verkkosivustolla osoitteessa https://europa.eu/european-union/index_fi.

EU:n julkaisut

EU:n maksuttomia ja maksullisia julkaisuja voi tilata osoitteesta https://op.europa.eu/fi/publications. Maksuttomista julkaisuista voi saada useita kappaleita ottamalla yhteyttä Europe Direct -palveluun tai paikalliseen tiedotuskeskukseen (ks. https://europa.eu/european-union/contact_fi).

EU:n oikeus ja siihen liittyvät asiakirjat

EU:sta saa oikeudellista tietoa, muun muassa EU:n lainsäädännöstä vuodesta 1952 lähtien kaikilla virallisilla kielillä, EUR-Lexistä osoitteessa http://eur-lex.europa.eu.

Avointa dataa EU:sta

EU:n avoimen datan portaalin (http://data.europa.eu/euodp/fi) kautta pääsee hyödyntämään EU:ta koskevaa dataa. Kaikki data on vapaasti käytettävissä kaupallisiin tai ei-kaupallisiin tarkoituksiin.

doi:10.2811/128160 TK-05-17-225-FI-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

Tieto- ja viestintätekniikoiden nopea kehitys on kasvattanut vankan tietosuojan tarvetta. Tämä oikeus vahvistetaan sekä Euroopan unionin (EU) että Euroopan neuvoston säädöksissä. Tekniikan kehittymisen myötä esimerkiksi tarkkailun, telepakkokeinojen ja tietojen säilyttämisen rajat ovat väljentyneet asettaen uusia ja merkittäviä haasteita tämän tärkeän oikeuden turvaamiselle. Tämän käsikirjan tarkoituksena on tarjota tietosuojaoikeuteen liittyvää tietoa oikeusalan ammattilaisille, jotka eivät ole erikoistuneet tähän kehittyvään oikeuden alaan. Siinä luodaan yleiskatsaus EU:n ja Euroopan neuvoston sovellettaviin oikeudellisiin kehyksiin. Siinä selitetään myös keskeistä oikeuskäytäntöä, ja tehdään yhteenveto sekä Euroopan ihmisoikeustuomioistuimen että Euroopan unionin tuomioistuimen tärkeimmistä tuomioista. Lisäksi siinä esitetään kuvitteellisia tilanteita, joissa havainnollistetaan käytännöllisesti tällä jatkuvasti kehittyvällä alalla kohdattavia erilaisia kysymyksiä.

EUROOPAN UNIONIN PERUSOIKEUSVIRASTO
Schwarzenbergplatz 11 – 1040 Wien – Itävalta
Puh. +43 (1) 580 30-0 – Faksi +43 (1) 580 30-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EUROOPAN IHMISOIKEUSTUOMIOISTUIN
EUROOPAN NEUVOSTO
67075 Strasbourg Cedex – Ranska
Puh. +33 (0) 3 88 41 20 18 – Faksi +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int – twitter.com/ECHR_CEDH

EUROOPAN TIETOSUOJAVALTUUTETTU
Rue Wiertz 60 – 1047 Bryssel – Belgia
Puh. +32 2 283 19 00
www.edps.europa.eu – edps@edps.europa.eu – twitter.com/EU_EDPS

Euroopan unionin julkaisutoimisto

ISBN 978-92-871-9832-7 (Euroopan neuvosto)
ISBN 978-92-9474-792-1 (FRA)