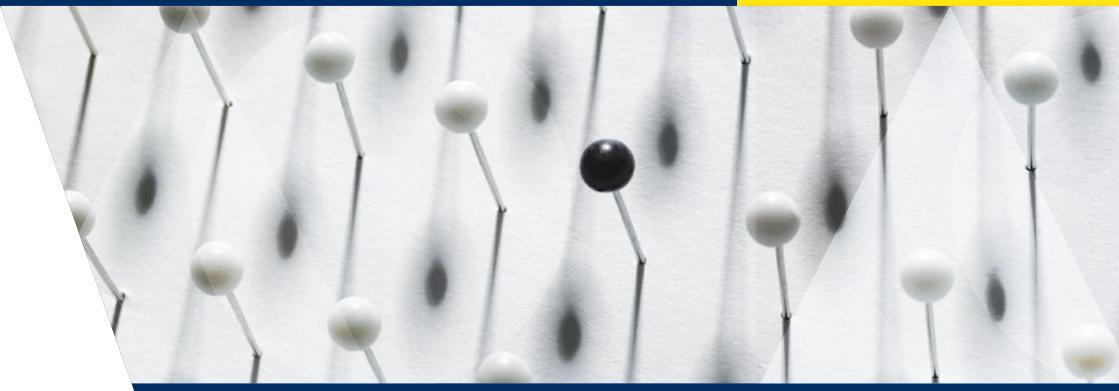
PODRĘCZNIK



Podręcznik europejskiego prawa o ochronie danych

wydanie z 2018 r.

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

Pracę nad tekstem podręcznika zakończono w kwietniu 2018 r.

Przyszłe aktualizacje będą dostępne na stronie internetowej FRA pod adresem fra.europa.eu, na stronie internetowej Rady Europy pod adresem coe.int/dataprotection, na stronie internetowej Europejskiego Trybunału Praw Człowieka w menu Case-Law [„Orzecznictwo"] pod adresem echr.coe.int oraz na stronie Europejskiego Inspektora Ochrony Danych pod adresem edps.europa.eu.

Zdjęcia (okładka i wnętrze): © iStockphoto

Luksemburg: Urząd Publikacji Unii Europejskiej, 2020

Rada Europy:	ISBN 978-92-871-9842-6		
FRA – print:	ISBN 978-92-9474-297-1	doi:10.2811/2046	TK-05-17-225-PL-C
FRA – pdf:	ISBN 978-92-9474-289-6	doi:10.2811/69584	TK-05-17-225-PL-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

Podręcznik europejskiego prawa o ochronie danych

wydanie z 2018 r.

Przedmowa

Postępująca cyfryzacja społeczeństw jest faktem. Tempo rozwoju technologicznego i sposób przetwarzania danych osobowych wpływają na każdego z nas codziennie i na różne sposoby. Ramy prawne Unii Europejskiej i Rady Europy zapewniające ochronę prywatności i danych osobowych poddano ostatnio przeglądowi.

Europa jest światowym liderem pod względem ochrony danych. U podstaw unijnych standardów ochrony danych leży konwencja nr 108 Rady Europy, instrumenty unijne, w tym ogólne rozporządzenie o ochronie danych i dyrektywa o ochronie danych w obszarze działań policji i wymiaru sprawiedliwości w sprawach karnych, a także orzecznictwo Europejskiego Trybunału Praw Człowieka oraz Trybunału Sprawiedliwości Unii Europejskiej.

Reformy dotyczące ochrony danych wprowadzane przez UE i Radę Europy mają szeroki zakres i nierzadko złożony charakter, zapewniając różnego rodzaju korzyści i wpływając zarówno na osoby indywidualne, jak i na przedsiębiorstwa. Niniejszy podręcznik powstał z myślą o zwiększaniu świadomości i wiedzy na temat przepisów dotyczących ochrony danych, w szczególności wśród prawników, którzy mają do czynienia z kwestiami ochrony danych, chociaż nie jest to obszar ich specjalizacji.

Podręcznik przygotowała Agencja Praw Podstawowych Unii Europejskiej wraz z Radą Europy (we współpracy z sekretariatem Europejskiego Trybunału Praw Człowieka) i Europejskim Inspektorem Ochrony Danych. Stanowi on aktualizację wydania z 2014 r. i należy do serii podręczników prawnych publikowanych wspólnie przez FRA i Radę Europy.

Dziękujemy organom ochrony danych Belgii, Estonii, Francji, Gruzji, Irlandii, Monako, Szwajcarii, Węgier, Zjednoczonego Królestwa i Włoch za cenne opinie na temat wstępnej wersji podręcznika. Ponadto pragniemy wyrazić uznanie dla Działu Ochrony Danych oraz Działu Międzynarodowych Przepływów Danych i Bezpieczeństwa Komisji Europejskiej. Dziękujemy Trybunałowi Sprawiedliwości Unii Europejskiej za udzielone nam wsparcie i udostępnienie dokumentów niezbędnych do opracowania podręcznika. Pragniemy również wyrazić naszą wdzięczność dla Urzędu

Ochrony Danych Osobowych za wsparcie w zakresie weryfikacji polskiej wersji językowej podręcznika.

Christos Giakoumopoulos	**Giovanni Buttarelli**	**Michael O'Flaherty**
Dyrektor generalny ds. praw człowieka i praworządności Rady Europy	Europejski Inspektor Ochrony Danych	Dyrektor Agencji Praw Podstawowych Unii Europejskiej

Spis treści

Skróty i akronimy

BCR	Wiążące reguły korporacyjne
CCTV	Telewizja przemysłowa
CETS	Seria Traktatów Rady Europy
CRM	Zarządzanie kontaktami z klientami
C-SIS	System centralny systemu informacyjnego Schengen
DPA	Organ ochrony danych
Dz.U.	Dziennik Urzędowy Unii Europejskiej
EAW	Europejski nakaz aresztowania
EFSA	Europejski Urząd ds. Bezpieczeństwa Żywności
EFTA	Europejskie Stowarzyszenie Wolnego Handlu
EIOD	Europejski Inspektor Ochrony Danych
EKPC	Europejska konwencja praw człowieka
ENISA	Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji
ENU	Jednostka krajowa Europolu
EOG	Europejski Obszar Gospodarczy
EPPO	Prokuratura Europejska
EROD	Europejska Rada Ochrony Danych
ESMA	Europejski Urząd Nadzoru Giełd i Papierów Wartościowych
eTEN	Transeuropejskie Sieci Telekomunikacyjne
ETPC	Europejski Trybunał Praw Człowieka
eu-LISA	Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości
EuroPriSe	Europejski Certyfikat Ochrony Prywatności
FRA	Agencja Praw Podstawowych Unii Europejskiej
GPS	Globalny system pozycjonowania
IOD	Inspektor Ochrony Danych
ISP	Dostawca usług internetowych
JSB	Wspólny organ nadzorczy

Karta praw podstawowych	Karta praw podstawowych Unii Europejskiej
Konwencja nr 108	Konwencja (Rady Europy) o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych Protokół zmieniający (CETS nr 223) konwencję nr 108 („zaktualizowaną konwencję nr 108") został przyjęty przez Komitet Ministrów Rady Europy podczas 128 sesji w Elsinore, w Danii (17–18 maja 2018 r.). Odniesienia do „zaktualizowanej konwencji nr 108" odnoszą się do konwencji zmienionej protokołem CETS nr 223.
MPPOIP	Międzynarodowy pakt praw obywatelskich i politycznych
NGO	Organizacja pozarządowa
N-SIS	Krajowy system informacyjny Schengen
OECD	Organizacja Współpracy Gospodarczej i Rozwoju
ONZ	Organizacja Narodów Zjednoczonych
PDPC	Powszechna deklaracja praw człowieka
PIN	Osobisty numer identyfikacyjny
PNR	Dane dotyczące przelotu pasażera
RE	Rada Europy
RODO	Ogólne rozporządzenie o ochronie danych
SCG	Grupa ds. koordynowania nadzoru
SEPA	Jednolity obszar płatności w euro
SIS	System Informacyjny Schengen
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
TFUE	Traktat o funkcjonowaniu Unii Europejskiej
TIK	Technologia informacyjno-komunikacyjna
TSUE	Trybunał Sprawiedliwości Unii Europejskiej (przed grudniem 2009 r. Europejski Trybunał Sprawiedliwości, ETS)
TUE	Traktat o Unii Europejskiej
UE	Unia Europejska
VIS	Wizowy System Informacyjny
WE	Wspólnota Europejska

Jak korzystać z niniejszego podręcznika?

Niniejszy podręcznik przedstawia w zarysie normy prawne dotyczące ochrony danych określone przez Unię Europejską (UE) i Radę Europy (RE). Ma on stanowić pomoc dla prawników praktyków, którzy nie specjalizują się w dziedzinie ochrony danych, w tym adwokatów, sędziów i innych prawników praktyków, jak też dla osób pracujących dla innych podmiotów, takich jak organizacje pozarządowe (NGO), które mogą w swojej działalności zetknąć się z zagadnieniami prawnymi związanymi z ochroną danych.

Podręcznik stanowi podstawowe kompendium wiedzy zarówno o odpowiednich przepisach prawa UE, jak i o zapisach europejskiej konwencji praw człowieka (EKPC) oraz postanowień Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencji nr 108) i innych aktów prawnych RE.

Każdy rozdział zaczyna się od tabeli, w której zawarto obowiązujące przepisy prawne, istotne w kontekście tematyki danego rozdziału. W tabelach przedstawiono zarówno prawo RE, jak i prawo UE, w tym wybrane istotne orzecznictwo Europejskiego Trybunału Praw Człowieka (ETPC) oraz Trybunału Sprawiedliwości Unii Europejskiej (TSUE). Następnie kolejno omówiono odpowiednie przepisy wspomnianych dwóch europejskich porządków odnoszące się do kolejnych poruszanych tematów. Pozwala to czytelnikowi dostrzec, gdzie oba te systemy prawne są zbieżne, a gdzie się różnią. Powinno to także pomóc czytelnikom w odnalezieniu najważniejszych informacji dotyczących ich sytuacji, zwłaszcza jeżeli podlegają wyłącznie przepisom prawnym RE. W niektórych rozdziałach kolejność tematów w tabelach może nieznacznie różnić się od tej w ramach samego rozdziału, jeżeli uznano to za wskazane w celu zwięzłego przedstawienia jego treści. Podręcznik zawiera także krótkie omówienie ram ONZ.

Prawnicy praktycy w państwach niebędących członkami UE, które są państwami członkowskimi Rady Europy, a tym samym stronami EKPC i konwencji nr 108, mogą uzyskać dostęp do informacji na temat swoich krajów, przechodząc bezpośrednio do sekcji dotyczących RE. Prawnicy praktycy z państw niebędących członkami UE muszą także mieć na uwadze fakt, że z chwilą przyjęcia unijnego ogólnego rozporządzenia o ochronie danych unijne przepisy dotyczące ochrony danych mają zastosowanie do organizacji i innych podmiotów, które nie mają jednostki organizacyjnej w UE, jeżeli przetwarzają dane osobowe i oferują w Unii produkty i usługi osobom, których dane dotyczą lub monitorują zachowanie tych osób.

Prawnicy praktycy z państw członkowskich UE będą musieli zapoznać się z obiema sekcjami, jako że w państwach tych obowiązują oba porządki prawne. Należy zauważyć, że reformy i uaktualnienie przepisów dotyczących ochrony danych w Europie, przeprowadzone zarówno w ramach Rady Europy (zaktualizowana konwencja nr 108 zmieniona protokołem CETS nr 223), jak i UE (przyjęcie ogólnego rozporządzenia o ochronie danych i dyrektywy (UE) 2016/680), przeprowadzane były równolegle. Organy regulacyjne w obu systemach prawnych dołożyły wszelkich starań, by zapewnić spójność i zgodność pomiędzy tymi ramami prawnymi. Reformy przyniosły skutek w postaci większej harmonizacji pomiędzy prawem ochrony danych RE i UE. Ci, którzy potrzebują więcej informacji na dany temat, mogą w sekcji podręcznika „Dodatkowe źródła" znaleźć wykaz bardziej specjalistycznych materiałów. Informacje dotyczące przepisów konwencji nr 108 i protokołu dodatkowego do niej z 2001 r., które mają zastosowanie do czasu wejścia w życie protokołu zmieniającego, czytelnicy znajdą w wersji podręcznika z 2014 r.

Przepisy prawne RE przedstawiono, posługując się krótkimi odniesieniami do wybranych spraw ETPC. Wybrano je spośród licznych wyroków i decyzji ETPC dotyczących ochrony danych.

Stosowne przepisy UE obejmują przyjęte akty ustawodawcze, odpowiednie postanowienia traktatów oraz Karty praw podstawowych Unii Europejskiej zgodnie z wykładnią zawartą w orzecznictwie TSUE. Ponadto w podręczniku przedstawiono opinie i wytyczne przyjęte przez Grupę Roboczą Art. 29, organ doradczy, któremu na mocy dyrektywy o ochronie danych powierzono pełnienie roli doradczej względem państw członkowskich UE, a którą od dnia 25 maja 2018 r. zastąpi Europejska Rada Ochrony Danych (EROD). Opinie Europejskiego Inspektora Ochrony Danych dostarczają także istotnych informacji w przedmiocie wykładni prawa UE, wobec czego zostały uwzględnione w niniejszym podręczniku.

Sprawy opisane lub cytowane w niniejszym podręczniku zawierają przykłady ważnych orzeczeń zarówno ETPC, jak i TSUE. Wskazówki zamieszczone na końcu podręcznika mają pomóc czytelnikom w wyszukiwaniu orzecznictwa w Internecie. Przedstawione orzecznictwo TSUE odnosi się do poprzedniej dyrektywy w sprawie ochrony danych. Jednakże wykładnia TSUE nadal znajduje zastosowanie do odpowiednich praw i obowiązków ustanowionych na mocy ogólnego rozporządzenia o ochronie danych.

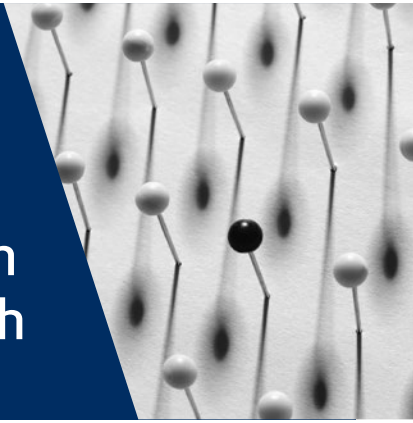
Ponadto w ramkach z niebieskim tłem podano praktyczne przykłady z hipotetycznymi scenariuszami. Ich celem jest dokładniejsze zilustrowanie zastosowania

europejskich przepisów o ochronie danych w praktyce, zwłaszcza w przypadkach gdy nie istnieje konkretne orzecznictwo ETPC lub TSUE na dany temat. W innych ramkach – z szarym tłem – zawarto przykłady pochodzące ze źródeł innych niż orzecznictwo ETPC i TSUE, takich jak przepisy prawa i opinie wydane przez Grupę Roboczą Art. 29.

Na początku podręcznika zamieszczono krótki opis roli dwóch systemów prawnych, których podstawę stanowią EKPC i prawo UE (rozdział 1). W rozdziałach 2–10 omówiono następujące zagadnienia:

- terminologię związaną z ochroną danych;
- najważniejsze zasady europejskiego prawa o ochronie danych;
- przepisy europejskiego prawa o ochronie danych;
- niezależny nadzór;
- prawa osób, których dane dotyczą, oraz ich egzekwowanie;
- transgraniczne przekazywanie i przepływy danych osobowych;
- ochronę danych w kontekście działań policji i wymiaru sprawiedliwości w sprawach karnych;
- inne europejskie przepisy o ochronie danych;
- współczesne wyzwania w dziedzinie ochrony danych osobowych.

1 Kontekst i ogólne informacje o europejskim prawie o ochronie danych



UE	Omówione zagadnienia	RE
Prawo do ochrony danych		
Artykuł 16 Traktatu o funkcjonowaniu Unii Europejskiej Artykuł 8 Karty praw podstawowych Unii Europejskiej (Karta praw podstawowych) (prawo do ochrony danych osobowych) Dyrektywa 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dyrektywa o ochronie danych), Dz.U. L 281 z 23.11.1995, (obowiązuje do maja 2018 r.) Decyzja ramowa Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych, Dz.U. L 350 z 30.12.2008, (obowiązuje do maja 2018 r.) Rozporządzenie (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), Dz.U. L 119 z 4.5.2016		Artykuł 8 EKPC (prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji) Zaktualizowana konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zaktualizowana konwencja nr 108)

UE	Omówione zagadnienia	RE
Dyrektywa (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (ochrona danych dla policji i organów sądowych), Dz.U. L 119 z 4.5.2016 Dyrektywa 2002/58/WE w sprawie przetwarzania danych osobowych oraz ochrony prywatności w sektorze łączności elektronicznej (dyrektywa dotycząca prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002 Rozporządzenie (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (rozporządzenie o ochronie danych przez instytucje UE), Dz.U. L 8 z 12.1.2001		
Ograniczenia prawa do ochrony danych osobowych		
Artykuł 52 ust. 1 Karty praw podstawowych Artykuł 23 ogólnego rozporządzenia o ochronie danych TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 2010		Artykuł 8 ust. 2 EKPC Artykuł 11 zaktualizowanej konwencji nr 108 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 2008
Wyważenie praw		
TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 2010	**Ogólne**	
TSUE, C-73/07, *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy* [WI], 2008 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 2014	**Wolność wypowiedzi**	ETPC, *Axel Springer AG przeciwko Niemcom* [WI], nr 39954/08, 2012 ETPC, *Mosley przeciwko Zjednoczonemu Królestwu*, nr 48009/08, 2011 ETPC, *Bohlen przeciwko Niemcom*, nr 53495/09, 2015

UE	Omówione zagadnienia	RE
TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.* [WI], 2010 TSUE, C-615/13 P, *ClientEarth, PAN Europe przeciwko EFSA*, 2015	Dostęp do dokumentów	ETPC, *Magyar Helsinki Bizottság przeciwko* Węgrom [WI], nr 18030/11, 2016
Artykuł 90 ogólnego rozporządzenia o ochronie danych	Tajemnica zawodowa	ETPC, *Pruteanu przeciwko Rumunii*, nr 30181/05, 2015
Artykuł 91 ogólnego rozporządzenia o ochronie danych	Wolność religii lub przekonań	
	Wolność sztuki i nauki	ETPC, *Vereinigung bildender Künstler przeciwko Austrii*, nr 68354/01, 2007
TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 2008	Ochrona własności	
TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 2014 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 2017	Prawa gospodarcze	

1.1. Prawo do ochrony danych osobowych

Najważniejsze kwestie

- Na mocy art. 8 EKPC prawo do ochrony w kontekście przetwarzania danych osobowych stanowi część prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji.
- Konwencja nr 108 RE jest pierwszym, i jak dotąd jedynym, prawnie wiążącym aktem międzynarodowym odnoszącym się do ochrony danych. Konwencję poddano procesowi aktualizacji, który zakończył się przyjęciem protokołu zmieniającego CETS nr 223.
- Zgodnie z prawem UE ochronę danych osobowych uznaje się za odrębne prawo podstawowe. Uznano je w art. 16 Traktatu o funkcjonowaniu Unii Europejskiej oraz w art. 8 Karty praw podstawowych Unii Europejskiej.

- Na mocy prawa UE ochrona danych została po raz pierwszy uregulowana w 1995 r. dyrektywą o ochronie danych.
- W związku z szybkim postępem technologicznym w 2016 r. UE przyjęła nowe przepisy służące dostosowaniu przepisów o ochronie danych do ery cyfrowej. Ogólne rozporządzenie o ochronie danych weszło w życie w maju 2018 r. i uchyliło dyrektywę o ochronie danych.
- Wraz z ogólnym rozporządzeniem o ochronie danych UE przyjęła przepisy dotyczące przetwarzania danych osobowych przez organy państwowe do celów egzekwowania prawa. W dyrektywie (UE) 2016/680 ustanowiono przepisy i zasady dotyczące ochrony danych osobowych, które regulują przetwarzanie danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar.

1.1.1. Prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych: krótkie wprowadzenie

Prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych, choć ściśle powiązane, stanowią odrębne prawa. Prawo do prywatności – określane w prawie europejskim jako prawo do poszanowania życia prywatnego – wyłoniło się w międzynarodowym prawie dotyczącym praw człowieka w Powszechnej deklaracji praw człowieka (PDPC) przyjętej w 1948 r. jako jedno z podstawowych chronionych praw człowieka. Wkrótce po przyjęciu PDPC Europa również potwierdziła to prawo – w europejskiej konwencji praw człowieka (EKPC), traktacie, który jest prawnie wiążący dla umawiających się stron i który sporządzono w 1950 r. Europejska konwencja praw człowieka stanowi, że każdy ma prawo do poszanowania swojego życia prywatnego i rodzinnego, swojego mieszkania i swojej korespondencji. Zakazuje się ingerencji władzy publicznej w to prawo, z wyjątkiem przypadków przewidzianych przez ustawę, służących realizacji ważnych i prawnie uzasadnionych interesów publicznych i koniecznych w demokratycznym społeczeństwie.

Powszechną deklarację praw człowieka i EKPC przyjęto na długo przed rozwojem komputerów i Internetu oraz rozwojem społeczeństwa informacyjnego. Zmiany te przyniosły znaczne korzyści jednostkom i społeczeństwu, poprawiając jakość życia, efektywność i produktywność. Jednocześnie stwarzają one nowe zagrożenia dla prawa do poszanowania życia prywatnego. W odpowiedzi na potrzebę szczegółowych zasad regulujących gromadzenie i wykorzystywanie danych osobowych

pojawiła się nowa koncepcja prywatności, znana w niektórych jurysdykcjach jako „prywatność informacji", a w innych jako „prawo do decydowania o wykorzystywaniu własnych danych"[1]. Koncepcja ta doprowadziła do opracowania specjalnych regulacji prawnych, które zapewniają ochronę danych osobowych.

Ochrona danych w Europie rozpoczęła się w latach 70. ubiegłego wieku wraz z przyjęciem – przez niektóre państwa – przepisów służących kontrolowaniu przetwarzania danych osobowych przez władze publiczne i duże przedsiębiorstwa[2]. Instrumenty ochrony danych zostały następnie ustanowione na szczeblu europejskim[3] i z biegiem lat ochrona danych przekształciła się w odrębną wartość, której nie obejmuje prawo do poszanowania życia prywatnego. W porządku prawnym UE ochrona danych jest uznawana za prawo podstawowe, odrębne od podstawowego prawa do poszanowania życia prywatnego. Rozdzielenie to rodzi pytanie o związek i różnice między tymi dwoma prawami.

Prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych są ze sobą ściśle powiązane. Oba dążą do ochrony podobnych wartości, tj. autonomii i godności ludzkiej jednostek, przyznając im sferę osobistą, w której mogą swobodnie rozwijać swoje osobowości, myśleć i kształtować swoje opinie. Stanowią one zatem zasadniczy warunek wstępny korzystania z innych podstawowych wolności, takich jak wolność wypowiedzi, wolność pokojowego gromadzenia się i stowarzyszania się oraz wolność religii.

Oba prawa różnią się sformułowaniem i zakresem. Prawo do poszanowania życia prywatnego polega na ogólnym zakazie ingerencji, z zastrzeżeniem pewnych kryteriów interesu publicznego, które w niektórych przypadkach mogą uzasadniać ingerencję. Ochrona danych osobowych jest postrzegana jako nowoczesne i aktywne

1 Niemiecki Federalny Trybunał Konstytucyjny potwierdził prawo do decydowania o wykorzystywaniu własnych danych w wyroku z 1983 r. w sprawie *Volkszählungsurteil*, BVerfGE Bd. 65, S. 1ff. Sąd ten uznał, że prawo do decydowania o wykorzystywaniu własnych danych wynika z podstawowego prawa do poszanowania osobowości, chronionego przez konstytucję niemiecką. Europejski Trybunał Praw Człowieka uznał w wyroku z 2017 r., że art. 8 europejskiej konwencji praw człowieka „zapewnia więc prawo do formy informacyjnego samostanowienia". Zob. ETPC, *Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii* [WI], nr 931/13, 27 czerwca 2017 r., pkt 137.

2 Niemiecki kraj związkowy Hesja przyjął w 1970 r. pierwszą ustawę o ochronie danych, która obowiązywała tylko w tym kraju związkowym. W 1973 r. Szwecja przyjęła pierwszą na świecie krajową ustawę o ochronie danych. Do końca lat 80. ubiegłego wieku kilka państw europejskich (Francja, Niemcy, Niderlandy i Zjednoczone Królestwo) również przyjęło przepisy dotyczące ochrony danych.

3 Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencję nr 108) przyjęto w 1981 r. W 1995 r. UE przyjęła swój pierwszy kompleksowy instrument ochrony danych: dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

prawo[4], wprowadzające system kontroli i równowagi w celu ochrony osób fizycznych podczas przetwarzania ich danych osobowych. Przetwarzanie musi być zgodne z podstawowymi elementami ochrony danych osobowych, a mianowicie z niezależnym nadzorem i poszanowaniem praw osoby, której dane dotyczą[5].

W art. 8 Karty praw podstawowych Unii Europejskiej (Karta praw podstawowych) nie tylko potwierdzono prawo do ochrony danych osobowych, lecz także określono podstawowe wartości związane z tym prawem. Stanowi on, że dane osobowe muszą być przetwarzane rzetelnie, w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą. Osoby fizyczne muszą mieć prawo dostępu do zebranych danych, które ich dotyczą, i prawo do dokonania ich sprostowania, a przestrzeganie tego prawa podlega kontroli niezależnego organu.

Prawo do ochrony danych osobowych ma zastosowanie w każdym przypadku przetwarzania danych osobowych; jest ono zatem szersze niż prawo do poszanowania życia prywatnego. Każda operacja przetwarzania danych osobowych podlega odpowiedniej ochronie. Ochrona danych dotyczy wszystkich rodzajów danych osobowych i przetwarzania danych, niezależnie od ich związku z prywatnością i wpływu na nią. Przetwarzanie danych osobowych może również naruszać prawo do życia prywatnego, co ilustrują poniższe przykłady. Dla powołania przepisów o ochronie danych nie jest jednak konieczne wykazanie, że doszło do naruszenia przepisów dotyczących [poszanowania] życia prywatnego.

Prawo do prywatności dotyczy sytuacji, w których naruszono interes prywatny lub „życie prywatne" jednostki. Jak wykazano w niniejszym podręczniku, pojęcie „życia prywatnego" zostało szeroko zinterpretowane w orzecznictwie jako obejmujące sytuacje intymne, informacje szczególnie chronione lub poufne, informacje, które mogłyby zaszkodzić postrzeganiu jednostki przez opinię publiczną, a nawet aspekty życia zawodowego i zachowania publicznego. Jednakże ocena, czy doszło do ingerencji w „życie prywatne", zależy od kontekstu i okoliczności faktycznych danej sprawy.

4 Rzecznik generalny E. Sharpston opisała tę kwestię jako obejmującą dwa odrębne prawa: „klasyczne" prawo do ochrony prywatności i bardziej „nowoczesne" prawo, czyli prawo do ochrony danych. Zob. TSUE, sprawy połączone C-92/09 i C-93/02, *Volker und Markus Schecke GbR przeciwko Land Hessen, opinia rzecznika generalnego E. Sharpston*, 17 czerwca 2010 r., pkt 71.

5 Hustinx, P., EDPS Speeches & Articles, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, lipiec 2013 r.

Natomiast każda operacja związana z przetwarzaniem danych osobowych może wchodzić w zakres przepisów o ochronie danych i skutkować prawem do ochrony danych osobowych. Na przykład w przypadku gdy pracodawca rejestruje informacje dotyczące nazwisk i wynagrodzeń wypłacanych pracownikom, samo rejestrowanie tych informacji nie może być postrzegane jako ingerencja w życie prywatne. Można by natomiast zarzucić tego rodzaju ingerencję, gdyby, na przykład, pracodawca przekazał dane osobowe pracowników osobom trzecim. Pracodawcy muszą w każdym przypadku przestrzegać zasad ochrony danych, ponieważ rejestrowanie informacji pracowników stanowi przetwarzanie danych.

Przykład: W sprawie *Digital Rights Ireland*[6] do TSUE zwrócono się o rozstrzygnięcie w przedmiocie ważności dyrektywy 2006/24/WE w świetle podstawowych praw do ochrony danych osobowych i poszanowania życia prywatnego, potwierdzonych w Karcie praw podstawowych Unii Europejskiej. Dyrektywa nałożyła na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązek zatrzymywania danych telekomunikacyjnych obywateli przez okres do dwóch lat, aby zapewnić dostępność przedmiotowych danych w celu dochodzenia, wykrywania i ścigania poważnych przestępstw. Ten akt prawny dotyczył jedynie metadanych, danych o lokalizacji i danych niezbędnych do identyfikacji abonenta lub użytkownika. Nie odnosił się on do treści komunikatów elektronicznych.

TSUE uznał, że dyrektywa stanowi ingerencję w prawo podstawowe do ochrony danych osobowych, „gdyż przewiduje możliwość przetwarzania danych osobowych”[7]. Ponadto TSUE stwierdził, że dyrektywa narusza prawo do poszanowania życia prywatnego[8]. Całokształt danych osobowych zatrzymywanych zgodnie z dyrektywą „może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy,

6 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

7 Tamże, pkt 36.

8 Tamże, pkt 32–35.

podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają”[9]. Ingerencja w te dwa prawa była szeroka i wyjątkowo poważna.

Trybunał stwierdził nieważność dyrektywy 2006/24/WE, uznając, że chociaż jej celem było osiągnięcie prawnie uzasadnionego celu, to ingerencja w prawo do ochrony danych osobowych i życia prywatnego była poważna i nie ograniczała się do tego, co absolutnie konieczne.

1.1.2. Międzynarodowe ramy prawne: Organizacja Narodów Zjednoczonych

W ramach Organizacji Narodów Zjednoczonych ochrona danych osobowych nie jest uznawana za prawo podstawowe, chociaż prawo do prywatności jest od dawna utrwalonym prawem podstawowym w międzynarodowym porządku prawnym. Prawo jednostki do ochrony swojej sfery prywatnej przed ingerencją innych osób lub podmiotów, w szczególności państwa, zostało po raz pierwszy określone w międzynarodowym instrumencie prawnym w art. 12 PDPC dotyczącym poszanowania życia prywatnego i rodzinnego[10]. Powszechna deklaracja praw człowieka, choć jest niewiążącą deklaracją, ma znaczący status jako fundamentalny instrument międzynarodowego prawa dotyczącego praw człowieka i wpłynęła na rozwój innych aktów prawnych dotyczących praw człowieka w Europie. Międzynarodowy pakt praw obywatelskich i politycznych (MPPOiP) wszedł w życie w 1976 r. Stanowi on, że nikt nie może być narażony na samowolną lub bezprawną ingerencję w jego życie prywatne, rodzinne, dom czy korespondencję, ani też na bezprawne zamachy na jego cześć i dobre imię. Międzynarodowy pakt praw obywatelskich i politycznych jest traktatem międzynarodowym, który zobowiązuje 169 stron do poszanowania i zapewnienia wykonywania praw obywatelskich jednostek, w tym prawa do prywatności.

Od 2013 r. Organizacja Narodów Zjednoczonych przyjęła dwie rezolucje w sprawie ochrony prywatności nt. „prawa do prywatności w erze cyfrowej”[11] w odpowiedzi

9 Tamże, pkt 27.

10 Organizacja Narodów Zjednoczonych (ONZ), Powszechna deklaracja praw człowieka (PDPC), 10 grudnia 1948 r.

11 Zob. ONZ, Zgromadzenie Ogólne, Resolution on the right to privacy in the digital age, A/RES/68/167, Nowy Jork, 18 grudnia 2013 r.; oraz ONZ, Zgromadzenie Ogólne, Revised draft resolution on the right to privacy in the digital age, A/C.3/69/L.26/Rev.1, Nowy Jork, 19 listopada 2014 r.

na rozwój nowych technologii i doniesienia dotyczące praktyk masowej inwigilacji stosowanych w niektórych państwach (doniesienia Snowdena). W rezolucjach tych potępiono masową inwigilację i podkreślono wpływ, jaki może ona mieć na podstawowe prawa do prywatności i wolności wypowiedzi oraz na funkcjonowanie dynamicznego i demokratycznego społeczeństwa. Choć nie były one prawnie wiążące, wywołały ważną międzynarodową debatę polityczną na wysokim szczeblu na temat prywatności, nowych technologii i inwigilacji. Doprowadziły one również do powołania specjalnego sprawozdawcy ds. prawa do prywatności, uprawnionego do promowania i ochrony tego prawa. Do szczegółowych zadań sprawozdawcy należy gromadzenie informacji na temat krajowych praktyk i doświadczeń związanych z prywatnością oraz wyzwań wynikających z nowych technologii, wymiana i promowanie najlepszych praktyk, a także identyfikacja potencjalnych przeszkód.

Podczas gdy wcześniejsze rezolucje koncentrowały się na negatywnych skutkach masowej inwigilacji i odpowiedzialności państw za ograniczanie uprawnień organów wywiadowczych, nowsze rezolucje odzwierciedlają kluczowe zmiany w debacie na temat prywatności w Organizacji Narodów Zjednoczonych[12]. Rezolucje przyjęte w 2016 i 2017 r. potwierdzają potrzebę ograniczenia uprawnień agencji wywiadowczych i potępiają masową inwigilację. Stanowią one jednak również wyraźnie, że „rosnące możliwości przedsiębiorstw w zakresie gromadzenia, przetwarzania i wykorzystywania danych osobowych mogą stanowić zagrożenie dla korzystania z prawa do prywatności w erze cyfrowej". Dlatego też, oprócz odpowiedzialności władz państwowych, w rezolucjach wskazuje się na odpowiedzialność sektora prywatnego za przestrzeganie praw człowieka i wzywa się przedsiębiorstwa do informowania użytkowników o gromadzeniu, wykorzystywaniu, udostępnianiu i zatrzymywaniu danych osobowych oraz do ustanowienia przejrzystych polityk przetwarzania danych.

1.1.3. Europejska konwencja praw człowieka

Radę Europy utworzono po II wojnie światowej jako organizację służącą wspólnemu krzewieniu przez państwa europejskie praworządności, demokracji, praw człowieka i rozwoju społecznego. W tym celu przyjęła ona w 1950 r. EKPC , która weszła w życie w 1953 r.

12 Zgromadzenie Ogólne ONZ, Revised draft resolution on the right to privacy in the digital age, A/C.3/71/L.39/Rev.1, Nowy Jork, 16 listopada 2016 r.; ONZ, Rada Praw Człowieka, The right to privacy in the digital age, A/HRC/34/L.7/Rev.1, Nowy Jork, 23 marca 2017 r.

Na państwach członkowskich spoczywa międzynarodowe zobowiązanie do przestrzegania EKPC. Wszystkie państwa członkowskie RE włączyły już EKPC do swojego porządku prawnego lub stosują ją w swoim prawie krajowym, a więc mają obowiązek przestrzegać jej postanowień. Wykonując swoje działania lub korzystając z uprawnień, umawiające się strony muszą przestrzegać praw określonych w konwencji. Obowiązek ten obejmuje działania podejmowane na rzecz bezpieczeństwa narodowego. W przełomowych wyrokach Europejskiego Trybunału Praw Człowieka (ETPC) uwzględniono działania państwa we wrażliwych obszarach prawa i praktyki w zakresie bezpieczeństwa narodowego[13]. Trybunał nie zawahał się potwierdzić, że działania inwigilacyjne stanowią ingerencję w poszanowanie życia prywatnego[14].

Aby zapewnić przestrzeganie przez umawiające się strony zobowiązań wynikających z EKPC, w Strasburgu (Francja) ustanowiono w 1959 r. Europejski Trybunał Praw Człowieka (ETPC). Europejski Trybunał Praw Człowieka zapewnia przestrzeganie przez państwa zobowiązań na mocy konwencji, rozpatrując skargi wnoszone przez osoby, grupy osób, organizacje pozarządowe lub osoby prawne zarzucające naruszenia konwencji. Europejski Trybunał Praw Człowieka może również rozpatrywać sprawy między państwami wniesione przez jedno lub więcej państw członkowskich Rady Europy przeciwko innemu państwu członkowskiemu.

W 2018 r. Rada Europy składała się z 47 państw członkowskich, z których 28 było zarazem państwami członkowskimi UE. Skarżący przed ETPC nie musi być obywatelem jednego z państw członkowskich, chociaż domniemane naruszenia muszą mieć miejsce w ramach jurysdykcji jednej z umawiających się stron.

Prawo do ochrony danych osobowych stanowi część praw chronionych na mocy art. 8 EKPC, w którym gwarantuje się prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji oraz określa warunki, pod jakimi dopuszczalne są ograniczenia tego prawa[15].

W swoim orzecznictwie ETPC zbadał wiele przypadków, w których pojawiało się zagadnienie ochrony danych, w szczególności dotyczących przechwytywania

13 Zob. na przykład: ETPC, *Klass i in. przeciwko Niemcom*, nr 5029/71, 6 września 1978 r.; ETPC, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, 4 maja 2000 r. oraz ETPC, *Szabó i Vissy przeciwko Węgrom*, nr 37138/14, 12 stycznia 2016 r.

14 Tamże.

15 Rada Europy, Europejska konwencja praw człowieka, CETS nr 005, 1950.

łączności[16], różnych form inwigilacji zarówno w sektorze prywatnym, jak i publicznym[17] oraz ochrony przed przechowywaniem danych osobowych przez władze publiczne[18]. Poszanowanie życia prywatnego nie jest prawem bezwzględnym, ponieważ korzystanie z prawa do prywatności mogłoby zagrażać innym prawom, takim jak wolność wypowiedzi i dostęp do informacji i odwrotnie. W związku z tym Trybunał dąży do znalezienia równowagi pomiędzy różnymi przedmiotowymi prawami. Trybunał wyjaśnił, że art. 8 EKPC nie tylko zobowiązuje państwa do powstrzymania się od wszelkich działań, które mogłyby naruszać to prawo zapisane w konwencji, ale nakłada na nie też w pewnych okolicznościach pozytywne obowiązki aktywnego zapewnienia skutecznego poszanowania życia prywatnego i rodzinnego[19]. Wiele spośród tych przypadków zostanie szczegółowo omówionych w stosownych rozdziałach.

1.1.4. Konwencja Rady Europy nr 108

Pojawienie się technologii informacyjnych w latach 60. XX w. poskutkowało rosnącą potrzebą opracowania bardziej szczegółowych zasad zabezpieczenia osób fizycznych przez ochronę ich danych osobowych. Do połowy lat 70. XX w. Komitet Ministrów Rady Europy przyjął rozmaite rezolucje w sprawie ochrony danych osobowych, w których powoływano się na art. 8 EKPC[20]. W 1981 r. otwarto do podpisu Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108)[21]. Konwencja nr 108 była i pozostaje jedynym prawnie wiążącym międzynarodowym aktem dotyczącym ochrony danych.

Konwencja nr 108 ma zastosowanie do wszelkich operacji przetwarzania danych prowadzonych zarówno przez sektor prywatny, jak i publiczny, w tym do

16 Zob. na przykład: ETPC, *Malone przeciwko Zjednoczonemu Królestwu*, nr 8691/79, 2 sierpnia 1984 r.; ETPC, *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 3 kwietnia 2007 r. lub ETPC, *Mustafa Sezgin Tanrıkulu przeciwko Turcji*, nr 27473/06, 18 lipca 2017 r.

17 Zob. na przykład: ETPC, *Klass i in. przeciwko Niemcom*, nr 5029/71, 6 września 1978 r.; ETPC, *Uzun przeciwko Niemcom*, nr 35623/05, 2 września 2010 r.

18 Zob. na przykład: ETPC, *Roman Zakharov przeciwko Rosji*, nr 47143/06, 4 grudnia 2015 r.; ETPC, *Szabó i Vissy przeciwko Węgrom*, nr 37138/14, 12 stycznia 2016 r.

19 Zob. na przykład: ETPC, *I przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.; ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2 grudnia 2008 r.

20 Rada Europy, Komitet Ministrów (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector, 26 września 1973 r.; Rada Europy, Komitet Ministrów (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector, 20 września 1974 r.

21 Rada Europy, Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, CETS nr 108, 1981.

przetwarzania danych przez organy sądowe i organy odpowiedzialne za egzekwowanie prawa. Zapewnia ona osobom fizycznym ochronę przed nadużyciami, które mogą towarzyszyć przetwarzaniu danych osobowych, a jej drugim celem jest uregulowanie transgranicznego przepływu danych osobowych. Zasady ustanowione w konwencji w odniesieniu do przetwarzania danych osobowych dotyczą w szczególności rzetelnego i zgodnego z prawem gromadzenia oraz automatycznego przetwarzania danych dla określonych i usprawiedliwionych celów. Oznacza to, że dane te nie mogą być wykorzystywane w sposób niezgodny z tymi celami ani przechowywane przez okres dłuższy, niż jest to wymagane. Dotyczą one także jakości danych – w szczególności stwierdza się, że muszą one być odpowiednie, stosowne, niewykraczające poza potrzeby wynikające z celów, dla których są gromadzone (proporcjonalność), a także prawidłowe.

Oprócz zapewnienia gwarancji w zakresie przetwarzania danych osobowych konwencja zakazuje także, przy braku odpowiednich prawnych gwarancji ochrony, przetwarzania danych szczególnie chronionych, na przykład dotyczących rasy, poglądów politycznych, stanu zdrowia, przekonań religijnych, życia seksualnego bądź karalności danej osoby.

W konwencji zapisano również prawo osób fizycznych do wiedzy o tym, że są przechowywane dotyczące ich informacje, oraz do ich sprostowania w razie potrzeby. Ograniczenie praw określonych w konwencji jest możliwe tylko wtedy, gdy zagrożone są nadrzędne interesy, takie jak bezpieczeństwo lub obronność państwa. W konwencji przewidziano swobodny przepływ danych osobowych między umawiającymi się stronami i nałożono pewne ograniczenia w zakresie przepływu tych danych do krajów, których regulacje prawne nie zapewniają równoważnej ochrony.

Należy zauważyć, że konwencja nr 108 jest wiążąca dla państw, które ją ratyfikowały. Nie podlega ona nadzorowi sądowemu ETPC, lecz jest uwzględniana w orzecznictwie ETPC w kontekście art. 8 EKPC. Na przestrzeni lat Trybunał orzekał, że ochrona danych osobowych stanowi ważny element prawa do poszanowania życia prywatnego (art. 8) i przy ustalaniu, czy doszło do ingerencji w to prawo podstawowe, kierował się zasadami konwencji nr 108[22].

W celu dalszego rozwoju ogólnych zasad i przepisów określonych w konwencji nr 108 Komitet Ministrów Rady Europy przyjął szereg zaleceń, które nie są prawnie wiążące. Zalecenia te wpłynęły na rozwój prawa o ochronie danych w Europie.

22 Zob. na przykład: ETPC, *Z przeciwko Finlandii*, nr 22009/93, 25 lutego 1997 r.

Na przykład przez lata jedynym instrumentem w Europie zapewniającym wytyczne w zakresie wykorzystania danych osobowych w sektorze policyjnym było zalecenie w sprawie policji[23]. Zasady zawarte w zaleceniu, takie jak sposoby zatrzymywania zbiorów danych oraz potrzeba wdrożenia jasnych zasad dotyczących osób, którym umożliwiono dostęp do tych zbiorów, zostały dopracowane i znalazły odzwierciedlenie w późniejszym prawodawstwie UE[24]. Nowsze zalecenia mają na celu sprostanie wyzwaniom ery cyfrowej – na przykład w odniesieniu do przetwarzania danych w kontekście zatrudnienia (zob. rozdział 9).

Konwencję nr 108 ratyfikowały wszystkie państwa członkowskie UE. W 1999 r. zaproponowano zmiany do konwencji nr 108, aby umożliwić UE stanie się jej stroną[25]. W 2001 r. przyjęto protokół dodatkowy do konwencji nr 108, w którym znalazły się przepisy dotyczące transgranicznego przepływu danych do państw niebędących jej stronami (tak zwanych państw trzecich) oraz obowiązkowego ustanowienia krajowych organów nadzorczych ds. ochrony danych[26].

Do konwencji nr 108 mogą przystępować państwa niebędące członkami RE. Możliwość stosowania konwencji jako powszechnego standardu i jej otwarty charakter mogą uczynić ją podstawą promowania ochrony danych na poziomie globalnym. Jak dotąd 51 państw jest stronami konwencji nr 108. Obejmują one wszystkie państwa członkowskie Rady Europy (47 państw), Urugwaj, pierwszy kraj pozaeuropejski, który przystąpił w sierpniu 2013 r., oraz Mauritius, Senegal i Tunezję, które przystąpiły w 2016 i 2017 r.

Konwencję poddano ostatnio procesowi aktualizacji. Konsultacje społeczne przeprowadzone w 2011 r. potwierdziły dwa główne cele tego procesu: wzmocnienia ochrony prywatności w środowisku cyfrowym i usprawnienia mechanizmu związanego z działaniami następczymi w ramach konwencji. Proces uaktualniania

23 Rada Europy, Komitet Ministrów (1987), Recommendation Rec(87)15 to Member States regulating the use of personal data in the police sector, Strasburg, 17 września 1987 r.

24 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995.

25 Rada Europy, Zmiany Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) przyjęte przez Komitet Ministrów w Strasburgu w dniu 15 czerwca 1999 r.

26 Rada Europy, Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzorczych i transgranicznych przepływów danych, CETS nr 181, 2001. Wraz z aktualizacją konwencji nr 108 protokół ten nie ma już zastosowania, ponieważ jego postanowienia zostały zaktualizowane i uwzględnione w zaktualizowanej konwencji nr 108.

koncentrował się na tych celach i zakończył się 18 kwietnia 2018 r. przyjęciem protokołu zmieniającego konwencję nr 108 (protokół CETS nr 223). Prace prowadzono równolegle z innymi reformami międzynarodowych instrumentów ochrony danych oraz równolegle z reformą unijnych zasad ochrony danych, rozpoczętą w 2012 r. Organy regulacyjne na szczeblu Rady Europy i na szczeblu UE dołożyły wszelkich starań, aby zapewnić spójność i zgodność między tymi dwoma ramami prawnymi. Uaktualnienie zachowuje ogólny i elastyczny charakter konwencji i wzmacnia jej potencjał jako uniwersalnego instrumentu prawa o ochronie danych. Potwierdza i stabilizuje ważne zasady i zapewnia nowe prawa osobom fizycznym, zwiększając jednocześnie odpowiedzialność podmiotów przetwarzających dane osobowe i zapewniając większą rozliczalność. Na przykład osoby fizyczne, których dane osobowe są przetwarzane, mają prawo do uzyskania informacji o przyczynie takiego przetwarzania danych oraz prawo do sprzeciwienia się takiemu przetwarzaniu. Aby przeciwdziałać coraz częstszemu wykorzystywaniu profilowania w świecie internetowym, konwencja ustanawia również prawo jednostki do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu danych bez uwzględniania jej własnych poglądów. Skuteczne egzekwowanie przepisów o ochronie danych przez niezależne organy nadzorcze umawiających się stron uważa się za kluczowe dla praktycznego wdrożenia konwencji. W tym celu zaktualizowana konwencja podkreśla potrzebę przyznania organom nadzorczym skutecznych uprawnień i funkcji oraz korzystania z prawdziwej niezależności przy wypełnianiu swojej misji.

1.1.5. Europejskie przepisy o ochronie danych

Prawo UE składa się z prawa pierwotnego i prawa wtórnego UE. Traktaty, czyli Traktat o Unii Europejskiej (TUE) i Traktat o funkcjonowaniu Unii Europejskiej (TFUE), zostały ratyfikowane przez wszystkie państwa członkowskie UE i są także określane mianem „prawa pierwotnego UE". Rozporządzenia, dyrektywy i decyzje UE są przyjmowane przez instytucje UE upoważnione do tego na mocy traktatów i często bywają określane mianem „prawa wtórnego UE".

Ochrona danych w prawie pierwotnym UE

Traktaty założycielskie Wspólnot Europejskich nie zawierały żadnych odniesień do praw człowieka lub ich ochrony, z uwagi na to, że początkowo przewidywano Europejską Wspólnotę Gospodarczą jako organizację regionalną skupiającą się na integracji gospodarczej i ustanowieniu wspólnego rynku. Naczelną zasadą leżącą u podstaw tworzenia i rozwoju Wspólnot Europejskich – i równie ważną obecnie – jest zasada przyznania. Zgodnie z tą zasadą UE działa jedynie w granicach kompetencji

przyznanych jej przez państwa członkowskie, co znajduje odzwierciedlenie w traktatach UE. W przeciwieństwie do Rady Europy, traktaty UE nie zawierają żadnych wyraźnych kompetencji w sprawach dotyczących praw podstawowych.

Ponieważ jednak do Trybunału Sprawiedliwości UE wpłynęły sprawy dotyczące domniemanych przypadków łamania praw człowieka w obszarach objętych prawem UE, TSUE przedstawił ważną wykładnię traktatów. Aby przyznać ochronę osobom fizycznym, Trybunał włączył prawa podstawowe do ogólnych zasad prawa europejskiego. Według TSUE wspomniane ogólne zasady odzwierciedlają zakres ochrony praw człowieka zapisanej w konstytucjach krajowych i traktatach dotyczących praw człowieka, w szczególności EKPC. W opinii TSUE takie włączenie zapewni zgodność prawa UE z tymi zasadami.

Uznając, że jej polityka może mieć wpływ na prawa człowieka, oraz aby „zbliżyć" obywateli do UE, Unia ogłosiła w 2000 r. Kartę praw podstawowych Unii Europejskiej. Karta obejmuje cały zakres praw obywatelskich, politycznych, gospodarczych i społecznych obywateli europejskich, stanowiąc syntezę tradycji konstytucyjnych oraz zobowiązań międzynarodowych wspólnych państwom członkowskim. Prawa określone w karcie zawarto w sześciu tytułach: godność, wolności, równość, solidarność, prawa obywatelskie i wymiar sprawiedliwości.

Chociaż pierwotnie była ona jedynie dokumentem o charakterze politycznym, karta praw podstawowych stała się wiążąca prawnie[27] jako prawo pierwotne UE (zob. art. 6 ust. 1 TUE), gdy wszedł w życie Traktat z Lizbony w dniu 1 grudnia 2009 r.[28]. Postanowienia karty są skierowane do instytucji i organów UE i zobowiązują je do poszanowania praw w nich wymienionych podczas pełnienia swoich obowiązków. Postanowienia karty są również wiążące dla państw członkowskich przy wdrażaniu przez nie prawa UE.

W karcie zagwarantowano nie tylko poszanowanie życia prywatnego i rodzinnego (art. 7), lecz także ustanowiono prawo do ochrony danych osobowych (art. 8). Karta wyraźnie podnosi poziom tej ochrony do rangi prawa podstawowego w prawie UE. Instytucje UE i państwa członkowskie muszą przestrzegać tego prawa oraz zagwarantować jego stosowanie; odnosi się to również do wdrażania prawa unijnego przez państwa członkowskie (art. 51 karty). Jako że sformułowano go kilka lat po

27 UE (2012), Karta praw podstawowych Unii Europejskiej, Dz.U. C 326 z 26.10.2012.

28 Zob. skonsolidowane wersje Wspólnoty Europejskie (2012), Traktat o Unii Europejskiej, Dz.U. C 326 z 26.10.2012; oraz Wspólnoty Europejskie (2012), TFUE, Dz.U. C 326 z 26.10.2012.

dyrektywie o ochronie danych, należy uznać, iż art. 8 Karty praw podstawowych zawiera w sobie wcześniejsze unijne prawo o ochronie danych. W związku z tym w karcie nie tylko wyraźnie wskazano prawo do ochrony danych w art. 8 ust. 1, lecz także zawarto odniesienie do podstawowych zasad ochrony danych w art. 8 ust. 2. Wreszcie w art. 8 ust. 3 zagwarantowano kontrolę wprowadzania w życie tych zasad przez niezależny organ.

Przyjęcie traktatu z Lizbony jest momentem przełomowym w rozwoju prawa o ochronie danych, nie tylko poprzez nadanie karcie statusu wiążącego dokumentu prawnego na poziomie prawa pierwotnego, ale również poprzez zapewnienie prawa do ochrony danych osobowych. Prawo to jest wyraźnie przewidziane w art. 16 TFUE w części traktatu poświęconej ogólnym zasadom UE. Artykuł 16 tworzy również nową podstawę prawną, przyznając UE kompetencję do stanowienia prawa w kwestiach związanych z ochroną danych. Jest to ważna zmiana, ponieważ unijne przepisy o ochronie danych – w szczególności dyrektywa o ochronie danych – opierały się początkowo na podstawie prawnej dotyczącej rynku wewnętrznego oraz na potrzebie zbliżenia przepisów krajowych, tak aby nie utrudniać swobodnego przepływu danych w UE. Artykuł 16 TFUE stanowi obecnie niezależną podstawę prawną dla nowoczesnego, kompleksowego podejścia do ochrony danych, które obejmuje wszystkie kwestie wchodzące w zakres kompetencji UE, w tym współpracę policyjną i sądową w sprawach karnych. W art. 16 TFUE potwierdza się również, że przestrzeganie zasady ochrony danych przyjętych zgodnie z tym artykułem musi podlegać kontroli niezależnych organów nadzorczych. Artykuł 16 posłużył jako podstawa prawna do przyjęcia w 2016 r. kompleksowej reformy zasad ochrony danych, tj. ogólnego rozporządzenia o ochronie danych oraz dyrektywy o ochronie danych dla policji i organów wymiaru sprawiedliwości w sprawach karnych (zob. poniżej).

Ogólne rozporządzenie o ochronie danych

Od 1995 r. do maja 2018 r. głównym aktem prawnym UE dotyczącym ochrony danych była dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (dyrektywa o ochronie danych)[29]. Dyrektywę przyjęto w 1995 r., w czasie gdy kilka państw członkowskich

29 Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, Dz.U. L 281 z 23.11.1995.

przyjęło już krajowe przepisy o ochronie danych[30], a jej przyjęcie wynikało z potrzeby harmonizacji tych przepisów w celu zapewnienia wysokiego poziomu ochrony i swobodnego przepływu danych osobowych między różnymi państwami członkowskimi. Swobodny przepływ towarów, kapitału, usług i osób w obrębie rynku wewnętrznego wymagał swobodnego przepływu danych, który nie byłby możliwy, gdyby państwa członkowskie nie mogły powołać się na jednolity, wysoki poziom ochrony danych.

Dyrektywa o ochronie danych odzwierciedlała zasady ochrony danych zawarte już w przepisach krajowych i w konwencji nr 108, a jednocześnie często je rozszerzała. W dyrektywie o ochronie danych wykorzystano jednak możliwość rozszerzenia zakresu ochrony przewidzianą w art. 11 konwencji nr 108. W szczególności ważnym wkładem w skuteczne funkcjonowanie europejskiego prawa o ochronie danych okazało się wprowadzenie niezależnego nadzoru jako instrumentu poprawy zgodności z przepisami dotyczącymi ochrony danych. W związku z tym tę zasadę włączono w 2001 r. do prawa RE na mocy protokołu dodatkowego do konwencji nr 108. Ilustruje to bliską interakcję i pozytywny wzajemny wpływ obu instrumentów na przestrzeni lat.

Dyrektywa o ochronie danych ustanowiła szczegółowy i kompleksowy system ochrony danych w UE. Jednakże zgodnie z systemem prawnym UE dyrektywy nie mają bezpośredniego zastosowania i podlegają transpozycji do krajowych porządków prawnych państw członkowskich. Oczywiście państwa członkowskie mają pewien margines uznania w transponowaniu przepisów dyrektywy. Mimo że dyrektywa miała w założeniu zapewnić pełną harmonizację[31] (i pełny poziom ochrony), w praktyce była transponowana w różny sposób w poszczególnych państwach członkowskich. Doprowadziło to do ustanowienia różnych przepisów o ochronie danych w całej UE, przy czym definicje i przepisy interpretowane są w ustawodawstwie krajowym w różny sposób. Poziomy egzekwowania i surowość sankcji także różniły się w poszczególnych państwach członkowskich. Ponadto od czasu opracowania dyrektywy w połowie lat dziewięćdziesiątych ubiegłego wieku nastąpiły istotne zmiany w technologii informacyjnej. Rozpatrywane w ujęciu całościowym,

30 W 1970 r. niemiecki kraj związkowy Hesja przyjął pierwszą na świecie ustawę o ochronie danych, która miała zastosowanie jedynie do tego kraju związkowego. Szwecja przyjęła *Datalagen* w 1973 r., Niemcy przyjęły *Bundesdatenschutzgesetz* w 1976 r., a Francja przyjęła *Loi relatif à l'informatique, aux fichiers et aux libertés* w 1977 r. W Zjednoczonym Królestwie w 1984 r. przyjęto *Data Protection Act*. Wreszcie w 1989 r. Niderlandy przyjęły *Wet Persoonregistraties.*

31 TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r., pkt 29.

powody te stały się przyczynkiem do reformy prawodawstwa UE w zakresie ochrony danych.

Reforma ta doprowadziła do przyjęcia ogólnego rozporządzenia o ochronie danych w kwietniu 2016 r., po latach intensywnych dyskusji. Debaty na temat potrzeby uaktualnienia unijnych przepisów o ochronie danych rozpoczęły się w 2009 r., kiedy to Komisja zainicjowała konsultacje społeczne na temat przyszłych ram prawnych dotyczących podstawowego prawa do ochrony danych osobowych. Wniosek dotyczący rozporządzenia został opublikowany przez Komisję w styczniu 2012 r., rozpoczynając długi proces legislacyjny negocjacji między Parlamentem Europejskim a Radą UE. Po przyjęciu ogólne rozporządzenie o ochronie danych przewidywało dwuletni okres przejściowy. Rozporządzenie obowiązuje w pełni od 25 maja 2018 r., kiedy to uchylono dyrektywę o ochronie danych.

Przyjęcie ogólnego rozporządzenia o ochronie danych w 2016 r. skutkowało uaktualnieniem prawodawstwa UE w zakresie ochrony danych, czyniąc je odpowiednim do ochrony praw podstawowych w kontekście wyzwań gospodarczych i społecznych ery cyfrowej. Ogólne rozporządzenie o ochronie danych zachowuje i rozwija podstawowe zasady i prawa osoby, której dane dotyczą, określone w dyrektywie o ochronie danych. Ponadto wprowadzono w nim nowe obowiązki wymagające od organizacji wdrożenia ochrony danych już w fazie projektowania i domyślnie, wyznaczenia w pewnych okolicznościach inspektora ochrony danych, przestrzegania nowego prawa do przenoszenia danych oraz przestrzegania zasady rozliczalności. Zgodnie z prawem UE rozporządzenia stosuje się bezpośrednio; nie ma potrzeby ich wdrażania na szczeblu krajowym. Ogólne rozporządzenie o ochronie danych przewiduje zatem jednolity zbiór przepisów o ochronie danych w całej UE. Dzięki temu ustanowiono spójne przepisy o ochronie danych w całej UE, tworząc środowisko pewności prawa, z którego mogą korzystać przedsiębiorcy i osoby fizyczne jako „osoby, których dane dotyczą".

Mimo że ogólne rozporządzenie o ochronie danych jest bezpośrednio stosowane, oczekuje się jednak, że państwa członkowskie zaktualizują swoje istniejące krajowe przepisy o ochronie danych, aby w pełni dostosować je do rozporządzenia, jednocześnie odzwierciedlając margines uznania w odniesieniu do przepisów szczegółowych w motywie 10. Znaczną część podręcznika poświęcono głównym regułom i zasadom ustanowionym w rozporządzeniu oraz silnym prawom, jakie przyznaje ono osobom fizycznym, i przedstawiono je w kolejnych rozdziałach. Rozporządzenie zawiera kompleksowe przepisy dotyczące zakresu terytorialnego. Ma ono zastosowanie do przedsiębiorstw mających siedzibę w UE, a także do administratorów

i podmiotów przetwarzających niemających siedziby w UE, którzy oferują towary lub usługi osobom, których dane dotyczą, w UE lub monitorują ich zachowanie. Ponieważ kilka zamorskich przedsiębiorstw z branży technologicznej ma kluczowy udział w rynku europejskim oraz miliony klientów w UE, poddanie tych organizacji unijnym przepisom o ochronie danych jest istotne dla zapewnienia ochrony osób fizycznych oraz równych szans.

Ochrona danych w kontekście ścigania przestępstw – dyrektywa (UE) 2016/680

Uchylona dyrektywa o ochronie danych zapewniła kompleksowy system ochrony danych. System ten został dodatkowo wzmocniony poprzez przyjęcie ogólnego rozporządzenia o ochronie danych. Zakres stosowania uchylonej dyrektywy o ochronie danych, choć kompleksowy, ograniczał się do działań wchodzących w zakres rynku wewnętrznego oraz do działań organów publicznych innych niż organy ścigania. W związku z tym konieczne było przyjęcie specjalnych instrumentów w celu osiągnięcia niezbędnej jasności i równowagi między ochroną danych a innymi uzasadnionymi interesami oraz sprostania wyzwaniom, które są szczególnie istotne w danych sektorach. Dotyczy to zasad regulujących przetwarzanie danych osobowych przez organy ścigania.

Pierwszym instrumentem prawnym UE regulującym tę kwestię była decyzja ramowa Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych. Przepisy decyzji miały zastosowanie wyłącznie do danych policyjnych i sądowych wymienianych między państwami członkowskimi. Krajowe przetwarzanie danych osobowych przez organy ścigania zostało wyłączone z zakresu jego stosowania.

Naprawienie tej sytuacji nastąpiło wraz z przyjęciem dyrektywy (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych[32], zwanej dalej dyrektywą o ochronie danych dla policji i organów wymiaru sprawiedliwości

32 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych, Dz.U. L 119 z 4.5.2016.

w sprawach karnych. Dyrektywa ta, przyjęta równolegle z ogólnym rozporządzeniem o ochronie danych, uchyliła decyzję ramową 2008/977/WSiSW i ustanowiła kompleksowy system ochrony danych osobowych w kontekście ścigania przestępstw, uwzględniając jednocześnie specyfikę przetwarzania danych związanych z bezpieczeństwem publicznym. Podczas gdy ogólne rozporządzenie o ochronie danych określa ogólne zasady służące ochronie osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz zagwarantowaniu swobodnego przepływu takich danych w UE, dyrektywa ustanawia szczegółowe zasady ochrony danych w dziedzinie współpracy wymiarów sprawiedliwości w sprawach karnych i współpracy policyjnej. W przypadku gdy właściwy organ przetwarza dane osobowe do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, zastosowanie będzie miała dyrektywa (UE) 2016/680. W przypadku gdy właściwe organy przetwarzają dane osobowe do celów innych niż wyżej wymienione, zastosowanie będzie miał ogólny system ustanowiony na gruncie ogólnego rozporządzenia o ochronie danych. W przeciwieństwie do jej poprzednika (decyzji ramowej Rady 2008/977/WSiSW) zakres stosowania dyrektywy (UE) 2016/680 obejmuje krajowe przetwarzanie danych osobowych przez organy ścigania i nie ogranicza się do wymiany takich danych między państwami członkowskimi. Ponadto dyrektywa ma na celu osiągnięcie równowagi między prawami jednostek a prawnie uzasadnionymi celami przetwarzania danych związanego z bezpieczeństwem.

W tym celu dyrektywa potwierdza prawo do ochrony danych osobowych oraz podstawowe zasady, które powinny obejmować przetwarzanie danych, z zastrzeżeniem ścisłej zgodności z przepisami i zasadami określonymi w ogólnym rozporządzeniu o ochronie danych. Prawa osób fizycznych i obowiązki nałożone na administratorów danych – na przykład w odniesieniu do bezpieczeństwa danych, ochrony danych już w fazie projektowania i domyślnej ochrony danych oraz zawiadomień o naruszeniu ochrony danych – przypominają prawa i obowiązki określone w ogólnym rozporządzeniu o ochronie danych. W dyrektywie uwzględniono również pojawiające się poważne wyzwania technologiczne, które mogą mieć szczególnie uciążliwy wpływ na jednostki, takie jak stosowanie technik profilowania przez organy ścigania, i podjęto próbę sprostania im. Zasadniczo decyzje oparte wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, muszą być zakazane[33]. Ponadto nie mogą one opierać się na danych szczególnie chronionych.

33 Dyrektywa o ochronie danych dla policji i organów wymiaru sprawiedliwości w sprawach karnych, art. 11 ust. 1.

Zasady te podlegają pewnym wyjątkom przewidzianym w dyrektywie. Ponadto przetwarzanie takie nie może prowadzić do dyskryminacji żadnej osoby[34].

Dyrektywa zawiera również przepisy mające na celu zapewnienie rozliczalności administratorów danych. Muszą oni wyznaczyć inspektora ochrony danych, który będzie monitorował przestrzeganie przepisów o ochronie danych, informował podmiot i pracowników przetwarzających dane i doradzał im w zakresie przetwarzania danych, a także współpracował z organem nadzorczym. Przetwarzanie danych osobowych w sektorze policji i wymiaru sprawiedliwości w sprawach karnych podlega obecnie nadzorowi niezależnych organów nadzorczych. Zarówno ogólny system prawny ochrony danych, jak i specjalny system ochrony danych dla organów ścigania i spraw karnych muszą być w równym stopniu zgodne z wymogami Karty praw podstawowych UE.

Specjalny system przetwarzania danych w kontekście współpracy policyjnej i sądowej ustanowiony dyrektywą o ochronie danych dla policji i organów wymiaru sprawiedliwości w sprawach karnych opisano szczegółowo w rozdziale 8.

Dyrektywa o prywatności i łączności elektronicznej

Ustanowienie specjalnych zasad ochrony danych uznano również za konieczne w sektorze łączności elektronicznej. Wraz z rozwojem Internetu, telefonii stacjonarnej i komórkowej ważne było zapewnienie poszanowania prawa użytkowników do prywatności i poufności. Dyrektywa 2002/58/WE[35] dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) ustanawia przepisy dotyczące bezpieczeństwa danych osobowych w tych sieciach, zawiadamiania o naruszeniach ochrony danych osobowych oraz poufności komunikacji.

W odniesieniu do bezpieczeństwa operatorzy usług łączności elektronicznej muszą między innymi zapewnić, aby dostęp do danych osobowych był ograniczony wyłącznie do osób uprawnionych, oraz podjąć środki zapobiegające zniszczeniu, utracie lub przypadkowemu uszkodzeniu danych osobowych[36]. W przypadku gdy istnieje szczególne ryzyko naruszenia bezpieczeństwa publicznej sieci łączności,

34 Tamże, art. 11 ust. 2 i 3.

35 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.U. L 201 z 31.7.2002 (dyrektywa o prywatności i łączności elektronicznej).

36 Dyrektywa o prywatności i łączności elektronicznej, art. 4 ust. 1.

operatorzy zobowiązani są informować abonentów o tym ryzyku[37]. Jeżeli pomimo wdrożonych środków bezpieczeństwa dojdzie do naruszenia bezpieczeństwa, operatorzy muszą zawiadomić o naruszeniu ochrony danych osobowych właściwy organ krajowy, któremu powierzono wdrożenie i egzekwowanie przepisów dyrektywy. Czasami operatorzy są również zobowiązani do zawiadamiania osób fizycznych o naruszeniach ochrony danych osobowych, a mianowicie w przypadkach, gdy takie naruszenie może mieć negatywny wpływ na ich dane osobowe lub prywatność[38]. Poufność komunikatu wymaga, aby zasadniczo zakazane było słuchanie, nagrywanie, przechowywanie lub innego rodzaju nadzór nad komunikatem lub metadanymi albo ich przejęcie. Dyrektywa zakazuje również niezamówionych komunikatów (często zwanych „spamem"), chyba że użytkownicy wyrazili na to zgodę, i zawiera przepisy dotyczące przechowywania plików cookies na komputerach i urządzeniach. Te podstawowe negatywne zobowiązania wyraźnie wskazują, że poufność komunikatów jest w znacznym stopniu powiązana z ochroną prawa do poszanowania życia prywatnego zapisanego w art. 7 Karty praw podstawowych oraz prawa do ochrony danych osobowych zapisanego w art. 8 karty.

W styczniu 2017 r. Komisja opublikowała wniosek dotyczący rozporządzenia w sprawie poszanowania życia prywatnego i ochrony danych osobowych w łączności elektronicznej, które ma zastąpić dyrektywę o prywatności i łączności elektronicznej. Celem reformy jest dostosowanie przepisów regulujących łączność elektroniczną do nowego systemu ochrony danych ustanowionego na mocy ogólnego rozporządzenia o ochronie danych. Nowe rozporządzenie będzie bezpośrednio stosowane w całej UE; wszystkie osoby będą korzystać z tego samego poziomu ochrony ich łączności elektronicznej, natomiast operatorzy telekomunikacyjni i przedsiębiorstwa skorzystają na jasności, pewności prawnej i istnieniu jednolitego zbioru przepisów w całej UE. Proponowane przepisy dotyczące poufności łączności elektronicznej będą miały również zastosowanie do nowych podmiotów świadczących usługi łączności elektronicznej, które nie są objęte dyrektywą o prywatności i łączności elektronicznej. Ta ostatnia obejmowała jedynie tradycyjnych dostawców usług telekomunikacyjnych. W związku z powszechnym korzystaniem z usług takich jak Skype, WhatsApp, Facebook Messenger i Viber w celu wysyłania wiadomości lub wykonywania połączeń, te usługi OTT będą teraz objęte zakresem rozporządzenia i będą musiały spełniać jego wymogi w zakresie ochrony danych, prywatności i bezpieczeństwa. W chwili publikacji niniejszego podręcznika nadal trwał proces legislacyjny dotyczący zasad prywatności i łączności elektronicznej.

37 Tamże, art. 4 ust. 2.

38 Tamże, art. 4 ust. 3.

Rozporządzenie (WE) nr 45/2001

Ponieważ dyrektywa o ochronie danych mogła mieć zastosowanie jedynie do państw członkowskich UE, potrzebny był dodatkowy instrument prawny w celu ustanowienia ochrony danych do celów przetwarzania danych osobowych przez instytucje i organy UE. Rozporządzenie (WE) nr 45/2001 o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (rozporządzenie o ochronie danych przez instytucje UE) spełnia tę funkcję[39].

Rozporządzenie (WE) nr 45/2001 ściśle przestrzega zasad ogólnego unijnego systemu ochrony danych i stosuje te zasady do przetwarzania danych przez instytucje i organy UE w ramach wykonywania przez nie swoich funkcji. Ponadto ustanawia ono niezależny organ nadzorczy, Europejskiego Inspektora Ochrony Danych (EIOD), odpowiedzialny za monitorowanie stosowania jego przepisów. Europejski Inspektor Ochrony Danych posiada uprawnienia nadzorcze i obowiązek monitorowania przetwarzania danych osobowych w instytucjach i organach UE oraz rozpatrywania i badania skarg dotyczących domniemanych naruszeń przepisów o ochronie danych. Doradza on również instytucjom i organom UE we wszystkich kwestiach dotyczących ochrony danych osobowych, począwszy od wniosków dotyczących nowych aktów prawnych, a skończywszy na sporządzaniu przepisów wewnętrznych dotyczących przetwarzania danych.

W styczniu 2017 r. Komisja Europejska przedstawiła wniosek dotyczący nowego rozporządzenia w sprawie przetwarzania danych przez instytucje UE, które uchyli obecne rozporządzenie. Podobnie jak w przypadku reformy dyrektywy o prywatności i łączności elektronicznej reforma rozporządzenia (WE) nr 45/2001 uaktualni i dostosuje jego przepisy do nowego systemu ochrony danych ustanowionego na mocy ogólnego rozporządzenia o ochronie danych.

Rola TSUE

Trybunał Sprawiedliwości Unii Europejskiej jest właściwy do orzekania, czy państwo członkowskie wypełniło swoje zobowiązania wynikające z unijnego prawa o ochronie danych, a także do interpretowania przepisów UE w sposób zapewniający ich skuteczne i jednolite stosowanie we wszystkich państwach członkowskich.

39 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

Od czasu przyjęcia dyrektywy o ochronie danych w 1995 r. zgromadzono obszerny zbiór orzecznictwa, w którym wyjaśniono zakres i znaczenie zasad ochrony danych oraz podstawowego prawa do ochrony danych osobowych zapisanego w art. 8 Karty praw podstawowych. Mimo że dyrektywę uchylono i obecnie obowiązuje nowy instrument prawny – ogólne rozporządzenie o ochronie danych – dotychczasowe orzecznictwo pozostaje aktualne i istotne dla interpretacji i stosowania unijnych zasad ochrony danych w zakresie, w jakim główne zasady i koncepcje dyrektywy o ochronie danych zostały utrzymane w RODO.

1.2. Ograniczenia prawa do ochrony danych osobowych

Najważniejsze kwestie

- Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; może być ograniczone, jeżeli jest to konieczne ze względu na cel leżący w interesie ogólnym lub w celu ochrony praw i wolności innych osób.
- Warunki ograniczania praw do poszanowania życia prywatnego i ochrony danych osobowych są wymienione w art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności oraz w art. 52 ust. 1 Karty praw podstawowych. Zostały one opracowane i zinterpretowane w oparciu o orzecznictwo ETPC i TSUE.
- Zgodnie z prawem o ochronie danych RE przetwarzanie danych osobowych stanowi zgodną z prawem ingerencję w prawo do poszanowania życia prywatnego i może być prowadzone tylko wtedy, gdy:
  - następuje zgodnie z prawem;
  - służy uzasadnionemu celowi;
  - respektuje istotę podstawowych praw i wolności;
  - jest niezbędne i proporcjonalne w demokratycznym społeczeństwie dla realizacji uzasadnionego celu.
- W porządku prawnym UE nakłada się podobne warunki na ograniczenia w korzystaniu z praw podstawowych chronionych kartą. Wszelkie ograniczenia w korzystaniu z praw podstawowych, w tym z prawa do ochrony danych osobowych, są dopuszczalne wyłącznie wtedy, gdy:
  - następują zgodnie z prawem;

- szanują istotę tego prawa;
- są konieczne, z zastrzeżeniem zasady proporcjonalności;
- odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw innych osób.

Podstawowe prawo do ochrony danych osobowych zgodnie z art. 8 karty nie jest prawem bezwzględnym, lecz „należy je postrzegać w kontekście jego funkcji społecznej”[40]. W art. 52 ust. 1 karty uznaje się zatem, że ograniczenia w korzystaniu z praw takich jak te określone w jej art. 7 i 8 są możliwe, o ile są przewidziane ustawą, respektują istotę tych praw i wolności oraz, z zastrzeżeniem zasady proporcjonalności, są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez UE lub potrzebie ochrony praw i wolności innych osób[41]. Podobnie w systemie EKPC ochrona danych jest zagwarantowana w art. 8, a korzystanie z tego prawa może być ograniczone, jeżeli jest to konieczne do osiągnięcia zgodnego z prawem celu. Niniejsza sekcja odnosi się do warunków ingerencji na mocy EKPC zgodnie z wykładnią zawartą w orzecznictwie ETPC, jak również do warunków wprowadzania ograniczeń zgodnych z prawem na mocy art. 52 karty.

1.2.1. Wymagania dotyczące usprawiedliwionej ingerencji na mocy EKPC

Przetwarzanie danych osobowych może stanowić ingerencję w prawo do poszanowania życia prywatnego osoby, której dane dotyczą, zagwarantowane na mocy art. 8 EKPC[42]. Jak wyjaśniono powyżej (zob. sekcja 1.1.1 i sekcja 1.1.4), w przeciwieństwie do porządku prawnego UE, EKPC nie uznaje ochrony danych osobowych za odrębne prawo podstawowe. Ochrona danych osobowych stanowi raczej część praw chronionych na mocy prawa do poszanowania życia prywatnego. W związku z tym żadna operacja związana z przetwarzaniem danych osobowych nie może być objęta zakresem art. 8 europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności. Aby zastosować art. 8, należy najpierw ustalić, czy naruszone zostały interesy prywatne lub życie prywatne danej osoby. W swoim orzecznictwie ETPC pojęcie „życia prywatnego” traktuje szeroko, jako koncepcję obejmującą

40 Zob. na przykład TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r., pkt 48.

41 Tamże, pkt 50.

42 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 8 grudnia 2008 r., pkt 67.

nawet aspekty życia zawodowego i zachowania publicznego. Trybunał orzekł również, że ochrona danych osobowych stanowi ważny element prawa do poszanowania życia prywatnego. Jednakże, pomimo szerokiej wykładni życia prywatnego, nie wszystkie rodzaje przetwarzania same w sobie zagrażałyby prawom chronionym na mocy art. 8.

W przypadku gdy ETPC uzna, że dana operacja przetwarzania danych narusza prawo osób fizycznych do poszanowania życia prywatnego, Trybunał zbada, czy ingerencja jest uzasadniona. Prawo do poszanowania życia prywatnego nie jest prawem bezwzględnym, ale musi być wyważone i pogodzone z innymi uzasadnionymi interesami i prawami, czy to innych osób (interes prywatny), czy też społeczeństwa jako całości (interes publiczny).

Łączne warunki spełnienia przesłanek uzasadnionej ingerencji są następujące:

Zgodność z prawem

Zgodnie z orzecznictwem ETPC ingerencja jest zgodna z prawem, jeżeli jej podstawą jest przepis prawa krajowego, które ma pewne cechy. Prawo musi być „dostępne dla zainteresowanych osób, a jego skutki muszą być przewidywalne"[43]. Przepis jest przewidywalny, „jeżeli został sformułowany wystarczająco precyzyjnie, aby umożliwić każdej osobie – w razie potrzeby po zasięgnięciu odpowiedniej porady – dostosowanie swojego postępowania"[44]. Ponadto „[s]topień precyzji wymagany od »prawa« w tym kontekście jest zależny od konkretnego zagadnienia"[45].

Przykłady: W sprawie *Rotaru przeciwko Rumunii*[46] skarżący zarzuca naruszenie prawa do poszanowania życia prywatnego poprzez przechowywanie i wykorzystywanie przez rumuńskie służby wywiadowcze akt zawierających

43 ETPC, *Amann przeciwko Szwajcarii* [WI], nr 27798/95, 16 lutego 2000 r., pkt 50; zob. także ETPC, *Kopp przeciwko Szwajcarii*, nr 23224/94, 25 marca 1998 r., pkt 55 oraz ETPC, *Iordachi i in. przeciwko Mołdawii*, nr 25198/02, 10 lutego 2009 r., pkt 50.

44 ETPC, *Amann przeciwko Szwajcarii* [WI], nr 27798/95, 16 lutego 2000 r., pkt 56; zob. także ETPC, *Malone przeciwko Zjednoczonemu Królestwu*, nr 8691/79, 2 sierpnia 1984 r., pkt 66; ETPC, *Silver i in. przeciwko Zjednoczonemu Królestwu*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 marca 1983 r., pkt 88.

45 ETPC, *The Sunday Times przeciwko Zjednoczonemu Królestwu*, nr 6538/74, 26 kwietnia 1979 r., pkt 49; zob. także ETPC, *Silver i in. przeciwko Zjednoczonemu Królestwu*, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75, 25 marca 1983 r., pkt 88.

46 ETPC, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, 4 maja 2000 r., pkt 57; zob. także ETPC, *Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii*, nr 62540/00, 28 czerwca 2007 r.; ETPC, *Shimovolos przeciwko Rosji*, nr 30194/09, 21 czerwca 2011 r.; oraz ETPC, *Vetter przeciwko Francji*, nr 59842/00, 31 maja 2005 r.

jego dane osobowe. Europejski Trybunał Praw Człowieka orzekł, że chociaż prawo rumuńskie zezwalało na gromadzenie, rejestrację i archiwizację w tajnych aktach informacji mających wpływ na bezpieczeństwo narodowe, nie ustanowiono w nim ograniczeń w wykonywaniu tych uprawnień, które pozostawiono do uznania władz. W prawie krajowym nie określono na przykład rodzaju informacji, które mogą być przetwarzane, kategorii osób, które można objąć nadzorem, okoliczności, w których można podejmować takie środki, ani procedur, jakich należy przestrzegać. Trybunał stwierdził, że prawo krajowe nie jest zgodne z wymogiem przewidywalności na mocy art. 8 EKPC i doszło do naruszenia tego artykułu.

W sprawie *Taylor-Sabori przeciwko Zjednoczonemu Królestwu*[47] skarżący był przedmiotem nadzoru ze strony policji. Dzięki „sklonowaniu" pagera skarżącego policja była w stanie przechwytywać wysyłane do niego wiadomości. Skarżącego następnie aresztowano i oskarżono o zmowę przestępczą w celu rozpowszechniania substancji kontrolowanej. Oskarżenie przeciwko niemu opierało się w części na notatkach sporządzonych przez policję na podstawie wiadomości przesyłanych na pager. W chwili gdy odbywał się proces skarżącego, w prawie brytyjskim nie było jednak przepisu regulującego przechwytywanie komunikatów przekazywanych za pośrednictwem prywatnego systemu telekomunikacyjnego. Ingerencja w prawa skarżącego nie nastąpiła więc „zgodnie z prawem". Europejski Trybunał Praw Człowieka stwierdził, że doszło do naruszenia art. 8 EKPC.

Sprawa *Vukota-Bojić przeciwko Szwajcarii*[48] dotyczyła tajnego nadzoru nad osobą ubiegającą się o ubezpieczenie społeczne przez prywatnych detektywów na zlecenie jej towarzystwa ubezpieczeniowego. Europejski Trybunał Praw Człowieka stwierdził, że chociaż środek nadzoru będący przedmiotem skargi został zarządzony przez prywatny zakład ubezpieczeń, to jednak państwo przyznało temu zakładowi prawo do wypłacania świadczeń wynikających z obowiązkowego ubezpieczenia medycznego oraz do pobierania składek ubezpieczeniowych. Państwo nie mogło zwolnić się z odpowiedzialności wynikającej z konwencji poprzez delegowanie swoich zobowiązań na podmioty prywatne lub osoby fizyczne. Prawo krajowe musiało zapewnić wystarczające zabezpieczenia przed nadużyciami, aby ingerencja w prawa wynikające z art. 8 EKPC była „zgodna z prawem". W przedmiotowej sprawie ETPC stwierdził, że nastąpiło naruszenie art. 8

47 ETPC, *Taylor-Sabori przeciwko Zjednoczonemu Królestwu*, nr 47114/99, 22 października 2002 r.

48 ETPC, *Vukota-Bojić przeciwko Szwajcarii*, nr 61838/10, 18 października 2016 r., pkt 77.

EKPC, ponieważ prawo krajowe nie wskazywało wystarczająco jasno zakresu i sposobu wykonywania uprawnień dyskrecjonalnych przyznanych zakładom ubezpieczeń działającym w charakterze organów publicznych w sporach ubezpieczeniowych w celu prowadzenia tajnego nadzoru nad osobą ubezpieczoną. W szczególności nie zawierał on wystarczających zabezpieczeń przed nadużyciami.

Służenie uzasadnionemu celowi

Uzasadnionym celem może być jeden z wymienionych rodzajów interesu publicznego bądź ochrona praw i wolności innych osób. Uzasadnionymi celami, które mogłyby stanowić podstawę ingerencji, są, zgodnie z art. 8 ust. 2 EKPC, interesy bezpieczeństwa narodowego, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju, zapobieganie zakłóceniom porządku lub przestępstwom, ochrona zdrowia lub moralności oraz ochrona praw i wolności innych osób.

Przykład: W sprawie *Peck przeciwko Zjednoczonemu Królestwu*[49] skarżący usiłował popełnić na ulicy samobójstwo, podcinając sobie nadgarstki; nie wiedział przy tym, że jest filmowany przez kamerę telewizji przemysłowej. Po tym jak funkcjonariusze monitorujący system kamer uratowali mu życie, organ policyjny przekazał nagranie mediom, które opublikowały je, nie maskując twarzy skarżącego. Europejski Trybunał Praw Człowieka stwierdził, że nie występowały żadne istotne i wystarczające powody, które uzasadniałyby bezpośrednią publikację materiału przez władze bez uzyskania zgody skarżącego lub zamaskowania jego tożsamości. Trybunał orzekł zatem, że doszło do naruszenia art. 8 EKPC.

Niezbędne w demokratycznym społeczeństwie

Europejski Trybunał Praw Człowieka stwierdził, że „pojęcie konieczności implikuje, że ingerencja odpowiada pilnej potrzebie społecznej, a w szczególności, że jest ona proporcjonalna do zamierzonego zgodnego z prawem celu"[50]. Oceniając, czy dany środek jest niezbędny do zaspokojenia pilnej potrzeby społecznej, ETPC bada jego adekwatność i przydatność w odniesieniu do zamierzonego celu. W tym celu może on wziąć pod uwagę, czy ingerencja ta ma na celu rozwiązanie problemu, który,

49 ETPC, *Peck przeciwko Zjednoczonemu Królestwu*, nr 44647/98, 28 stycznia 2003 r., pkt 85.

50 ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r., pkt 58.

jeżeli nie zostanie rozwiązany, może mieć szkodliwy wpływ na społeczeństwo, czy istnieją dowody na to, że ingerencja ta może złagodzić taki szkodliwy wpływ, oraz jakie są szersze społeczne poglądy na dany problem[51]. Na przykład gromadzenie i przechowywanie przez służby bezpieczeństwa danych osobowych poszczególnych osób, co do których stwierdzono, że są powiązane z ruchami terrorystycznymi, naruszałoby prawo osób fizycznych do poszanowania życia prywatnego, które jednak zaspokaja poważną i naglącą potrzebę społeczną: bezpieczeństwo narodowe i walkę z terroryzmem. Aby spełnić kryterium konieczności, ingerencja musiałaby także pozostawać w relacji proporcjonalności. W orzecznictwie ETPC proporcjonalność jest rozpatrywana w ramach pojęcia konieczności. Proporcjonalność wymaga, aby ingerencja w prawa chronione na mocy EKPC nie wykraczała poza to, co jest konieczne do osiągnięcia zamierzonego zgodnego z prawem celu. Istotnymi czynnikami, które należy wziąć pod uwagę przy badaniu kryterium proporcjonalności, jest zakres ingerencji, w szczególności liczba osób, których ona dotyczy, oraz zabezpieczenia lub zastrzeżenia wprowadzone w celu ograniczenia jej zakresu lub szkodliwego wpływu na prawa osób fizycznych[52].

Przykład: W sprawie *Khelili przeciwko Szwajcarii*[53] policja znalazła podczas kontroli przy skarżącej wizytówki o następującej treści: „Miła, ładna kobieta po trzydziestce pragnie poznać pana, aby pójść wspólnie na drinka lub umówić się z nim od czasu do czasu. Nr tel. […]". Skarżąca zarzuciła, że po tym odkryciu policja określiła ją w bazie danych mianem „prostytutki", którą w rzeczywistości – jak utrzymywała – nie jest. Skarżąca żądała usunięcia słowa „prostytutka" z policyjnej bazy danych. Europejski Trybunał Praw Człowieka uznał, że co do zasady zatrzymanie danych osobowych osoby fizycznej w związku z tym, że może ona popełnić kolejne przestępstwo, może w pewnych okolicznościach być proporcjonalne. Jednak w przypadku skarżącej zarzut niezgodnego z prawem uprawiania prostytucji wydawał się zbyt niejasny i ogólny oraz nie był poparty konkretnymi faktami, gdyż skarżąca nie została nigdy skazana za niezgodne z prawem uprawianie prostytucji, a zatem nie można uznać, aby zarzut ten odpowiadał „pilnej potrzebie społecznej" w rozumieniu art. 8 EKPC. Uznając, że na władzach spoczywa obowiązek udowodnienia prawidłowości danych przechowywanych na temat skarżącej, oraz ze względu na powagę ingerencji

51 Grupa Robocza Art. 29 (2014), *Opinion on the application of the necessity and proportionality concepts and data protection within the law enforcement sector*, WP 211, Bruksela, 27 lutego 2014 r., s. 7–8.

52 Tamże, s. 9–11.

53 ETPC, *Khelili przeciwko Szwajcarii*, nr 16188/07, 18 października 2011 r.

w prawa skarżącej, Trybunał orzekł, iż wieloletnia obecność wzmianki „prostytutka" w aktach policyjnych nie była podyktowana koniecznością w demokratycznym społeczeństwie. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu*[54] obaj skarżący zostali aresztowani i oskarżeni o popełnienie przestępstwa. Policja pobrała odciski palców i próbki DNA zgodnie z Police and Criminal Evidence Act [ustawą o policji i dowodach w postępowaniach karnych]. Skarżący nigdy nie zostali skazani za przestępstwa: jeden z nich został uniewinniony w sądzie, a postępowanie karne przeciwko drugiemu skarżącemu zostało umorzone. Ich odciski palców, profile DNA i próbki komórek były niemniej przechowywane przez policję w bazie danych, a przepisy krajowe zezwalały na ich przechowywanie bez stosownego terminu. Podczas gdy rząd Zjednoczonego Królestwa argumentował, że zatrzymanie danych pomogło w identyfikacji przyszłych sprawców przestępstw, a tym samym przyczyniło się do osiągnięcia zgodnego z prawem celu, jakim jest zapobieganie i wykrywanie przestępstw, ETPC uznał, że ingerencja w prawo skarżących do poszanowania życia prywatnego jest nieuzasadniona. Trybunał przypomniał, że podstawowe zasady ochrony danych wymagają, by zatrzymywanie danych osobowych było proporcjonalne do celu, w jakim są one gromadzone, oraz że okresy zatrzymywania danych muszą być ograniczone. Trybunał przyznał, że rozszerzenie bazy danych o profile DNA nie tylko osób skazanych, ale także wszystkich osób podejrzanych, ale nie skazanych, mogło przyczynić się do wykrywania i zapobiegania przestępczości w Zjednoczonym Królestwie. Jednakże nastąpiło „zderzenie z generalnym i bezkrytycznie stosowanym uprawnieniem do zatrzymywania danych"[55].

Biorąc pod uwagę bogactwo informacji genetycznych i zdrowotnych zawartych w próbkach komórek, ingerencja w prawo skarżących do życia prywatnego była szczególnie inwazyjna. Odciski palców i próbki można by pobierać od osób aresztowanych i przechowywać przez czas nieokreślony w policyjnej bazie danych, niezależnie od charakteru i wagi przestępstwa, a nawet w przypadku drobnych przestępstw, za które nie grozi kara pozbawienia wolności. Ponadto możliwości usunięcia swoich danych z bazy danych przez osoby uniewinnione były ograniczone. Na koniec ETPC zwrócił

54 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.

55 Tamże, pkt 119.

szczególną uwagę na fakt, że w momencie aresztowania jeden ze skarżących miał jedenaście lat. Zatrzymywanie danych osobowych nieletniego, który nie jest skazany, może być szczególnie szkodliwe ze względu na jego bezbronność oraz znaczenie jego rozwoju i integracji ze społeczeństwem[56]. Trybunał jednogłośnie orzekł, że zatrzymanie stanowi nieproporcjonalną ingerencję w prawo do życia prywatnego, której nie można uznać za konieczną w demokratycznym społeczeństwie.

Przykład: W sprawie *Leander przeciwko Szwecji*[57] ETPC orzekł, że tajne procedury sprawdzania wobec osób ubiegających się o zatrudnienie na stanowiskach ważnych dla bezpieczeństwa narodowego nie są same w sobie sprzeczne z wymogiem konieczności w demokratycznym społeczeństwie. Ze względu na specjalne zabezpieczenia przewidziane w prawie krajowym w celu ochrony interesów osób, których dane dotyczą – na przykład kontrolę sprawowaną przez parlament i kanclerza sprawiedliwości – ETPC stwierdził, że szwedzki system kontroli personelu spełniał wymagania art. 8 ust. 2 EKPC. Uwzględniając szeroki margines swobodnego uznania, którym dysponowało pozwane państwo, miało ono prawo uznać, że w przypadku skarżącego interes bezpieczeństwa narodowego przeważa nad interesem indywidualnym. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

1.2.2. Warunki nałożenia ograniczeń zgodnie z prawem na mocy Karty praw podstawowych UE

Karta praw podstawowych różni się od EKPC pod względem struktury i użytych sformułowań. W karcie nie wspomina się o ingerencji w zagwarantowane prawa, zawiera ona natomiast przepis dotyczący ograniczenia lub ograniczeń w korzystaniu z uznanych w niej praw i wolności.

Zgodnie z art. 52 ust. 1 karty ograniczenia w korzystaniu z praw i wolności uznanych w karcie, a więc też w korzystaniu z prawa do ochrony danych osobowych, takie jak przetwarzanie danych osobowych, są dopuszczalne wyłącznie wtedy, gdy:

- przewidziano je ustawą;

56 Tamże, pkt 124.

57 ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r., pkt 59 i 67.

- szanują one istotę prawa do ochrony danych;
- są konieczne, z zastrzeżeniem zasady proporcjonalności[58];
- odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Ponieważ ochrona danych osobowych jest odrębnym i samodzielnym prawem podstawowym w porządku prawnym UE, chronionym na mocy art. 8 karty, wszelkie przetwarzanie danych osobowych samo w sobie stanowi ingerencję w to prawo. Nie ma znaczenia, czy dane osobowe, o których mowa, odnoszą się do życia prywatnego osoby fizycznej, czy są szczególnie chronione, czy też osoby, których dane dotyczą, doznały jakichkolwiek niedogodności. Aby ingerencja była zgodna z prawem, musi spełniać wszystkie warunki wymienione w art. 52 ust. 1 karty.

Przewidziane ustawą

Ograniczenia prawa do ochrony danych osobowych muszą być przewidziane ustawą. Wymóg ten oznacza, że ograniczenia muszą opierać się na podstawie prawnej, która jest odpowiednio dostępna, przewidywalna i sformułowana z wystarczającą precyzją, aby umożliwić jednostkom zrozumienie swoich obowiązków i dostosowanie swojego postępowania. Podstawa prawna musi również jasno określać zakres i sposób wykonywania uprawnień przez właściwe organy w celu ochrony osób fizycznych przed arbitralną ingerencją. Wykładnia ta przypomina wymóg „zgodnej z prawem ingerencji" zgodnie z orzecznictwem ETPC[59] i argumentowano, że wyrażeniu „przewidziane ustawą" trzeba przypisać zakres podobny do zakresu tego pojęcia w kontekście EKPC[60]. Orzecznictwo ETPC, a w szczególności rozwijane przez lata pojęcie „jakości prawa", jest istotnym zagadnieniem, które TSUE powinien wziąć pod uwagę dokonując wykładni zakresu stosowania art. 52 ust. 1 Karty praw podstawowych[61].

58 Jeśli chodzi o ocenę konieczności środków ograniczających prawo podstawowe do ochrony danych osobowych, zob. EIOD (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r.

59 EIOD (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r., s. 4; zob. także TSUE, *Opinia 1/15 Trybunału* [WI], 26 lipca 2017 r.

60 TSUE, sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in., opinia rzecznika generalnego H. Saugmandsgaarda Øe*, przedstawiona w dniu 19 lipca 2016 r., pkt 140.

61 TSUE, C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, *opinia rzecznika generalnego P. Cruza Villalóna*, przedstawiona w dniu 14 kwietnia 2011 r., pkt 100.

Poszanowanie istoty prawa

W porządku prawnym UE wszelkie ograniczenia praw podstawowych chronionych na mocy Karty praw podstawowych muszą szanować istotę tych praw. Oznacza to, że nie można usprawiedliwiać ograniczeń, które są tak rozległe i inwazyjne, że pozbawiają podstawowe prawo jego podstawowej treści. Jeżeli istota prawa zostaje naruszona, ograniczenie należy uznać za niezgodne z prawem, bez konieczności dalszej oceny, czy służy ono celowi leżącemu w interesie ogólnym i czy spełnia kryteria konieczności i proporcjonalności.

Przykład: Sprawa *Schrems*[62] dotyczyła ochrony osób fizycznych w związku z przekazywaniem ich danych osobowych państwom trzecim – w tym przypadku Stanom Zjednoczonym. Schrems, obywatel Austrii, który przez kilka lat był użytkownikiem Facebooka, złożył skargę do irlandzkiego organu nadzorczego ds. ochrony danych, aby zaprotestować przeciwko przekazywaniu jego danych osobowych z irlandzkiej spółki zależnej Facebooka do spółki Facebook Inc. oraz serwerów znajdujących się w USA, na których były przetwarzane. Twierdził on, że w świetle doniesień Edwarda Snowdena, amerykańskiego informatora, z 2013 r., dotyczących działalności w zakresie nadzoru amerykańskich służb nadzoru, prawo i praktyka USA nie zapewniają wystarczającej ochrony danych osobowych przekazywanych na terytorium USA. Snowden ujawnił, że Agencja Bezpieczeństwa Narodowego wykorzystywała bezpośrednio serwery firm, takich jak Facebook, i miała dostęp do treści rozmów i prywatnych wiadomości.

Przekazywanie danych do Stanów Zjednoczonych opierało się na przyjętej w 2000 r. decyzji Komisji w sprawie adekwatności, zezwalającej na przekazywanie danych amerykańskim przedsiębiorstwom, które zadeklarowały, że będą chronić dane osobowe przekazywane z UE i będą przestrzegać tzw. zasad „bezpiecznej przystani". W następstwie skierowania sprawy do TSUE Trybunał zbadał kwestię ważności decyzji Komisji w świetle Karty praw podstawowych. Przypomniał, że ochrona praw podstawowych w UE wymaga, by odstępstwa od tych praw i ich ograniczenia ograniczały się do tego, co absolutnie konieczne. Trybunał uznał, że uregulowania pozwalające organom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych należy uznać za „naruszenie

62 TSUE, sprawa C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

zasadniczej istoty prawa podstawowego do poszanowania życia prywatnego, wynikającego z art. 7 karty". Prawo to zostałoby pozbawione znaczenia, gdyby organy publiczne mogły uzyskać dowolny i powszechny dostęp do wiadomości elektronicznych bez obiektywnego uzasadnienia opartego na względach bezpieczeństwa narodowego lub zapobiegania przestępczości związanych w szczególny sposób z zainteresowanymi jednostkami i bez otoczenia tych praktyk odpowiednimi gwarancjami przeciwko nadużyciom uprawnień.

Ponadto TSUE zauważył, że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych" jest niezgodne z podstawowym prawem do skutecznej ochrony sądowej (art. 47 karty). W związku z tym decyzja w sprawie „bezpiecznej przystani" nie zapewniła w Stanach Zjednoczonych poziomu ochrony praw podstawowych zasadniczo równoważnego poziomowi gwarantowanemu w UE na mocy dyrektywy interpretowanej w świetle karty. W konsekwencji TSUE stwierdził nieważność tej decyzji[63].

Przykład: W sprawie *Digital Rights Ireland*[64] TSUE zbadał zgodność dyrektywy 2006/24/WE (dyrektywy w sprawie zatrzymywania danych) z art. 7 i 8 karty. Dyrektywa nałożyła na dostawców usług telekomunikacyjnych obowiązek zatrzymywania danych o ruchu i lokalizacji przez okres co najmniej sześciu miesięcy do 24 miesięcy oraz umożliwienia właściwym organom krajowym dostępu do tych danych w celu zapobiegania i wykrywania poważnych przestępstw oraz prowadzenia czynności dochodzeniowo-śledczych. Dyrektywa nie zezwalała na zatrzymywanie treści komunikatów elektronicznych. Trybunał zauważył, że dane, które zgodnie z dyrektywą dostawcy usług mieli obowiązek zatrzymywać, obejmowały dane niezbędne do ustalenia źródła i celu połączenia, daty, godziny i czasu trwania połączenia, numerów nadawcy i odbiorcy połączenia oraz adresów IP. „Całokształt [tych] danych może dostarczyć bardzo precyzyjnych wskazówek dotyczących życia

63 Decyzja TSUE o unieważnieniu decyzji Komisji 520/2000/WE opierała się również na innych podstawach, które zostaną omówione w innych częściach niniejszego podręcznika. W szczególności TSUE uznał, że decyzja w sposób niezgodny z prawem ogranicza uprawnienia krajowych organów nadzorczych ds. ochrony danych. Ponadto w ramach systemu „bezpiecznej przystani" nie przewidziano dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych. W ten sposób naruszona została również istota podstawowego prawa do skutecznej ochrony sądowej, zapisana w art. 47 karty.

64 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

prywatnego osób, których dane są zatrzymywane, takich jak ich codzienne nawyki, miejsca stałego lub czasowego pobytu, codziennie lub okazyjnie pokonywane trasy, podejmowane czynności, relacje społeczne i środowiska społeczne, w których osoby te się obracają".

Zatrzymywanie danych osobowych na mocy dyrektywy stanowi zatem szczególnie poważną ingerencję w prawa do prywatności i ochrony danych osobowych. Trybunał orzekł jednak, że ingerencja ta nie miała negatywnego wpływu na istotę tych praw. Jeżeli chodzi o prawo do prywatności, jego istota nie została naruszona, ponieważ dyrektywa nie pozwalała na zapoznawanie się z samą treścią komunikatów elektronicznych. Podobnie nie naruszono istoty prawa do ochrony danych osobowych, ponieważ dyrektywa zobowiązywała dostawców usług łączności elektronicznej do przestrzegania określonych zasad ochrony danych i bezpieczeństwa danych oraz do wdrożenia w tym celu odpowiednich środków technicznych i organizacyjnych.

Konieczność i proporcjonalność

Artykuł 52 ust. 1 karty stanowi, że z zastrzeżeniem zasady proporcjonalności, ograniczenia w korzystaniu z podstawowych praw i wolności uznanych w karcie mogą być wprowadzane wyłącznie wtedy, gdy są konieczne.

Ograniczenie może być **konieczne**, jeżeli istnieje potrzeba przyjęcia środków służących realizacji zamierzonego celu leżącego w interesie publicznym, ale konieczność, zgodnie z wykładnią TSUE, oznacza również, że przyjęte środki muszą być mniej inwazyjne w porównaniu z innymi możliwościami osiągnięcia tego samego celu. W przypadku ograniczeń prawa do poszanowania życia prywatnego i ochrony danych osobowych TSUE stosuje rygorystyczne kryterium konieczności, wymagając, aby „odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne". Jeżeli ograniczenie zostanie uznane za absolutnie konieczne, należy również ocenić, czy jest ono proporcjonalne.

Proporcjonalność oznacza, że korzyści wynikające z ograniczenia powinny przeważyć nad niedogodnościami, jakie powoduje ono w korzystaniu z praw podstawowych[65]. W celu ograniczenia niedogodności i zagrożeń dla korzystania z prawa do prywatności i ochrony danych istotne jest, aby ograniczenia zawierały odpowiednie gwarancje.

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

Przykład: W sprawie *Volker und Markus Schecke*[66] TSUE stwierdził, że nakazując publikację danych osobowych wszystkich osób fizycznych będących beneficjentami pomocy z określonych funduszy rolnych bez wprowadzenia rozróżnienia według odpowiednich kryteriów, takich jak okresy, w których otrzymali tę pomoc, jej częstość czy też rodzaj i wysokość, Rada i Komisja przekroczyły granice, które wyznacza poszanowanie zasady proporcjonalności.

TSUE uznał zatem za konieczne stwierdzenie nieważności niektórych przepisów rozporządzenia Rady (WE) nr 1290/2005 i stwierdzenie nieważności rozporządzenia (WE) nr 259/2008 w całości[67].

Przykład: W sprawie *Digital Rights Ireland*[68] TSUE orzekł, że ingerencja w prawo do prywatności spowodowana dyrektywą w sprawie zatrzymywania danych nie stanowi zagrożenia dla istoty tego prawa, ponieważ zakazuje ona zatrzymywania treści zawartych w komunikatach elektronicznych. Trybunał wysnuł jednak wniosek, zgodnie z którym dyrektywa jest niezgodna z art. 7 i 8 karty, i stwierdził jej nieważność. Ponieważ dane o ruchu i lokalizacji, zagregowane i potraktowane jako całość, mogłyby być analizowane i przedstawiać szczegółowy obraz życia prywatnego osób fizycznych, stanowiło to poważną ingerencję w te prawa. Trybunał wziął pod uwagę, że dyrektywa wymaga zachowania wszystkich metadanych dotyczących telefonii stacjonarnej, telefonii komórkowej, dostępu do Internetu, elektronicznej poczty internetowej i telefonii internetowej, i że ma ona zastosowanie do wszystkich środków komunikacji elektronicznej, z których korzystanie jest bardzo rozpowszechnione w codziennym życiu obywateli. W praktyce stanowiło to ingerencję, która dotknęła całą ludność Europy. Biorąc pod uwagę zakres i wagę tej ingerencji, zatrzymywanie danych dotyczących ruchu i lokalizacji może, zdaniem TSUE, być uzasadnione

66 TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r., pkt 89 i 86.

67 Rozporządzenie Rady (WE) nr 1290/2005 z dnia 21 czerwca 2005 r. w sprawie finansowania wspólnej polityki rolnej, Dz.U. L 209 z 11.8.2005; rozporządzenie Komisji (WE) nr 259/2008 z dnia 18 marca 2008 r. ustanawiające szczegółowe zasady stosowania rozporządzenia Rady (WE) nr 1290/2005 w zakresie publikowania informacji na temat beneficjentów środków pochodzących z Europejskiego Funduszu Rolniczego Gwarancji (EFRG) i Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich (EFRROW), Dz.U. L 76 z 19.3.2008.

68 TSUE, sprawy połączone C-293/12 i C-594/12,*Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r., pkt 39.

jedynie w celu zwalczania poważnych przestępstw. Ponadto dyrektywa nie określiła żadnych obiektywnych kryteriów, które gwarantowałyby, że dostęp właściwych organów krajowych do zatrzymanych danych jest ograniczony do tego, co absolutnie konieczne. Ponadto nie zawierała ona merytorycznych i proceduralnych warunków regulujących dostęp organów krajowych do zatrzymanych danych i korzystanie z nich, które nie były uzależnione od uprzedniej kontroli ze strony sądu lub innego niezależnego organu.

Do podobnych wniosków TSUE doszedł w wyroku w sprawach połączonych *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.*[69]. Sprawy te miały za przedmiot zatrzymywanie danych dotyczących ruchu i lokalizacji „wszystkich abonentów i zarejestrowanych użytkowników i [dotyczących] wszystkich środków łączności elektronicznej i wszystkich metadanych" bez „zróżnicowania, ograniczenia ani wyjątku zależnego od zamierzonego celu"[70]. W owej sprawie fakt ewentualnego związku danej osoby, bezpośredniego lub pośredniego, z poważnymi przestępstwami lub ewentualnego znaczenia jej komunikatów dla bezpieczeństwa publicznego, nie stanowił warunku pozwalającego na zatrzymywanie jej danych. W świetle braku wymaganego związku między zatrzymanymi danymi a zagrożeniem dla bezpieczeństwa publicznego lub ograniczeń czasowych czy geograficznych TSUE stwierdził, że uregulowanie krajowe wykraczało poza granice tego, co jest absolutnie konieczne w celu zwalczania poważnej przestępczości[71].

Podobne podejście, jeśli chodzi o konieczność, przyjął Europejski Inspektor Ochrony Danych w swoim *Necessity Toolkit*[72]. Podręcznik ten ma pomóc w ocenie zgodności proponowanych środków z prawem UE w zakresie ochrony danych. Został on opracowany w celu lepszego wyposażenia decydentów politycznych i prawodawców UE odpowiedzialnych za przygotowanie lub kontrolę środków obejmujących przetwarzanie danych osobowych i ograniczających prawo do ochrony danych osobowych oraz inne prawa i wolności określone w Karcie praw podstawowych.

69 TSUE, sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.* [WI], 21 grudnia 2016 r., pkt 105–106.

70 Tamże, pkt 105.

71 Tamże, pkt 107.

72 EIOD (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r.

Cele interesu ogólnego

Aby ograniczenia w korzystaniu z praw uznanych w Karcie były uzasadnione, muszą one również rzeczywiście odpowiadać celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób. Jeśli chodzi o potrzebę ochrony praw i wolności innych osób, prawo do ochrony danych osobowych często wchodzi w interakcję z innymi prawami podstawowymi. W sekcji 1.3 przedstawiono szczegółową analizę takiego współoddziaływania. Jeśli chodzi o cele interesu ogólnego, obejmują one ogólne cele UE potwierdzone w art. 3 Traktatu o Unii Europejskiej (TUE), takie jak wspieranie pokoju i dobrobytu jej narodów, sprawiedliwości i ochrony socjalnej oraz ustanowienie przestrzeni wolności, bezpieczeństwa i sprawiedliwości, w której zapewniony jest swobodny przepływ osób, w powiązaniu z właściwymi środkami zapobiegania przestępczości i jej zwalczania, jak również inne cele i interesy chronione szczególnymi postanowieniami traktatów[73]. Ogólne rozporządzenie o ochronie danych doprecyzowuje w tym względzie art. 52 ust. 1 karty: W art. 23 ust. 1 rozporządzenia wymieniono szereg celów interesu ogólnego uznanych za uzasadnione w kontekście ograniczenia praw osób fizycznych, pod warunkiem że ograniczenie to jest zgodne z istotą prawa do ochrony danych osobowych, a także konieczne i proporcjonalne. Wśród celów interesu publicznego wymieniono bezpieczeństwo i obronę narodową, zapobieganie przestępczości, ochronę ważnych interesów gospodarczych i finansowych UE lub państw członkowskich, zdrowie publiczne i zabezpieczenie społeczne.

Ważne jest, aby zdefiniować i dostatecznie szczegółowo wyjaśnić cel leżący w interesie ogólnym, realizowany wskutek wprowadzenia ograniczenia, ponieważ konieczność ograniczenia zostanie oceniona w tym kontekście. Jasny, szczegółowy opis celu ograniczenia oraz proponowanych środków jest niezbędny, aby umożliwić ocenę, czy spełnia ono kryterium konieczności[74]. Osiągnięty cel oraz konieczność i proporcjonalność ograniczenia są ściśle ze sobą powiązane.

Przykład: Sprawa *Schwarz przeciwko Stadt Bochum*[75] dotyczyła ograniczeń prawa do poszanowania życia prywatnego i prawa do ochrony danych osobowych wynikających z pobrania i przechowywania odcisków palców w związku z wydawaniem paszportów przez organy państwa

73 Wyjaśnienia dotyczące Karty praw podstawowych (2007/C 303/02), Dz.U. C 303 z 14.12.2007, s. 17–35.

74 EIOD (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r., s. 4.

75 TSUE, C-291/12, *Michael Schwarz przeciwko Stadt Bochum*, 17 października 2013 r.

członkowskiego[76]. Skarżący zwrócił się do Stadt Bochum o wydanie mu paszportu, nie zgadzając się jednak na to, by zostały od niego pobrane odciski palców; Stadt Bochum następnie oddalił jego wniosek o paszport. W dalszej kolejności skarżący wniósł do sądu niemieckiego skargę, w której domagał się wydania mu paszportu bez pobierania od niego odcisków palców. Sąd niemiecki zwrócił się do TSUE z pytaniem, czy art. 1 ust. 2 rozporządzenia (WE) nr 2252/2004 w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez państwa członkowskie należy uznać za ważny.

Trybunał wskazał, że odciski palców **stanowią dane osobowe**, ponieważ obiektywnie zawierają one unikatowe informacje o osobach fizycznych i pozwalają na ich dokładne zidentyfikowanie, natomiast pobranie odcisków palców i ich przechowywanie stanowi przetwarzanie. Przetwarzanie tego ostatniego typu, które reguluje art. 1 ust. 2 rozporządzenia (WE) nr 2252/2004, stanowi naruszenie praw do poszanowania życia prywatnego oraz do ochrony danych osobowych[77]. Artykuł 52 ust. 1 karty dopuszcza jednak wprowadzenie ograniczeń w wykonywaniu tych praw, o ile przewidziane są one ustawą, szanują istotę tych praw i, przy poszanowaniu zasady proporcjonalności, są konieczne i rzeczywiście odpowiednie w stosunku do celów interesu ogólnego uznanych przez Unię lub potrzeby ochrony praw i wolności innych osób.

W przedmiotowej sprawie TSUE w pierwszej kolejności wskazał, że ograniczenie wynikające z pobrania i przechowywania odcisków palców w związku z wydawaniem paszportów powinno być uważane za **przewidziane ustawą**, skoro operacje te są przewidziane w art. 1 ust. 2 rozporządzenia (WE) nr 2252/2004. Po drugie, przepis ten ma na celu zapobieganie fałszowaniu paszportów i uniemożliwienie bezprawnego z nich korzystania. Wobec tego art. 1 ust. 2 ma zapobiegać, między innymi, nielegalnemu wjazdowi na terytorium UE, a więc zmierza do realizacji celu interesu ogólnego uznanego przez Unię. Po trzecie, z dowodów, którymi dysponuje Trybunał, nie wynika – i nie było to zresztą podnoszone – by wprowadzone ograniczenia w wykonywaniu tych praw nie przestrzegały istoty tych praw. Po czwarte, przechowywanie odcisków palców na nośniku pamięci o wysokim stopniu zabezpieczenia wiąże się z technicznym

76 Tamże, pkt 33–36.

77 Tamże, pkt 27–30.

wyrafinowaniem. Przechowywanie to może zmniejszyć ryzyko fałszowania paszportów oraz ułatwiać zadanie organom właściwym do przeprowadzania na granicach UE kontroli ich autentyczności. Okoliczność, iż metoda ta nie jest całkowicie niezawodna, nie ma decydującego znaczenia. Mimo iż metoda ta nie wyklucza w pełni przypadków wpuszczenia osób nieuprawnionych, wystarczające jest, że w sposób znaczący zmniejsza ryzyko takich przypadków. W świetle powyższych rozważań TSUE orzekł, że pobieranie i przechowywanie odcisków palców, o czym mowa w art. 1 ust. 2 rozporządzenia nr 2252/2004, to operacje właściwe dla osiągnięcia celów rozporządzenia, a tym samym również celu polegającego na uniemożliwieniu nielegalnego wjazdu osób na terytorium Unii[78].

W dalszej kolejności TSUE ocenił, czy przetwarzanie jest **konieczne**, zauważając, że sporna czynność wiązała się z pobieraniem odcisków jedynie dwóch palców, które są zresztą zazwyczaj wystawione na widok innych osób, a zatem nie chodzi o czynność mającą charakter intymny. Nie wiąże się też ona ze szczególnym dyskomfortem fizycznym lub psychicznym dla zainteresowanego, podobnie jak wykonanie fotografii twarzy. Należy również zauważyć, że jedyna realna alternatywa dla pobrania odcisków palców przytoczona w trakcie postępowania przed TSUE polega na sporządzeniu obrazu tęczówki oka. Nic jednak w aktach TSUE nie wskazuje na to, by ta ostatnia procedura słabiej naruszała prawa uznane w art. 7 i 8 karty niż pobranie odcisków palców. Ponadto jeżeli chodzi o skuteczność tych dwóch metod, to bezsporne jest, że poziom dojrzałości technologicznej metody związanej z rozpoznawaniem tęczówki oka nie osiąga poziomu dojrzałości metody dotyczącej odcisków palców, jest obecnie procedurą znacznie bardziej kosztowną, a tym samym mniej dostosowaną do upowszechnionego korzystania. W związku z powyższym nie podano do wiadomości TSUE, by istniały środki mogące w wystarczająco skuteczny sposób przyczynić się do celu związanego z ochroną paszportów przed bezprawnym użyciem i jednocześnie naruszające prawa uznane w art. 7 i 8 karty w stopniu mniejszym niż metoda związana z odciskami palców[79].

Trybunał zauważył, że art. 4 ust. 3 rozporządzenia (WE) nr 2252/2004 wyraźnie stwierdza, iż odciski palców mogą być wykorzystywane wyłącznie w celu sprawdzenia autentyczności dokumentu i tożsamości jego posiadacza,

78 Tamże, pkt 35–45.

79 TSUE, C-291/12, *Michael Schwarz przeciwko Stadt Bochum*, 17 października 2013 r., pkt 46–53.

natomiast art. 1 ust. 2 rozporządzenia nie przewiduje przechowywania odcisków palców, z wyjątkiem samego paszportu, który należy wyłącznie do jego posiadacza. Wobec tego rozporządzenie nie dawało podstawy prawnej do ewentualnej centralizacji danych zgromadzonych na jego podstawie lub do ich wykorzystywania w celach innych niż cel polegający na uniemożliwieniu nielegalnego wjazdu osób na terytorium Unii[80]. W świetle powyższych rozważań Trybunał wskazał, że analiza pytania prejudycjalnego nie wykazała okoliczności, które mogłyby wpłynąć na ważność art. 1 ust. 2 rozporządzenia nr 2252/2004.

Związek między Kartą a EKPC

Pomimo różnych sformułowań, warunki dla zgodnych z prawem ograniczeń w korzystaniu z praw zawartych w art. 52 ust. 1 karty przypominają artykuł 8 ust. 2 EKPC dotyczący prawa do poszanowania życia prywatnego. W swoim orzecznictwie TSUE i ETPC często odwołują się wzajemnie do swoich orzeczeń w ramach stałego dialogu między tymi sądami w celu dążenia do harmonijnej wykładni przepisów o ochronie danych. Artykuł 52 ust. 3 karty stanowi, że „w zakresie, w jakim niniejsza Karta zawiera prawa, które odpowiadają prawom zagwarantowanym w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności, ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję". Jednakże art. 8 karty nie odpowiada bezpośrednio artykułowi EKPC[81]. Artykuł 52 ust. 3 karty dotyczy treści i zakresu praw chronionych przez każdy porządek prawny, a nie warunków ich ograniczenia. W świetle szerszego kontekstu dialogu i współpracy między tymi dwoma sądami TSUE może jednak uwzględnić w swoich analizach kryteria zgodnego z prawem ograniczenia na mocy art. 8 EKPC, zgodnie z wykładnią ETPC. Możliwy jest również scenariusz odwrotny, w którym ETPC może odnieść się do warunków zgodnego z prawem ograniczenia na mocy karty. W każdym razie należy również wziąć pod uwagę, że w EKPC nie ma idealnego odpowiednika art. 8 karty, który odnosi się do ochrony danych osobowych, a zwłaszcza do praw osoby, której dane dotyczą, uzasadnionych podstaw przetwarzania danych i nadzoru niezależnego organu. Niektóre elementy art. 8 karty mogą być oparte na orzecznictwie ETPC opracowanym na mocy art. 8 EKPC i odnoszącym się do konwencji nr 108[82]. Powiązanie to zapewnia istnienie wzajemnej inspiracji między TSUE a ETPC w sprawach związanych z ochroną danych.

80 Tamże, pkt 56–61.

81 EIOD (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r., s. 6.

82 Wyjaśnienia dotyczące europejskiej Karty praw podstawowych (2007/C 303/02), art. 8.

1.3. Interakcja z innymi prawami i prawnie uzasadnionymi interesami

Najważniejsze kwestie

- Prawo do ochrony danych często wchodzi w interakcję z innymi prawami, takimi jak wolność wypowiedzi oraz prawo do otrzymywania i przekazywania informacji.
- Interakcja ta jest często ambiwalentna: chociaż istnieją sytuacje, w których prawo do ochrony danych osobowych jest sprzeczne z określonym prawem, istnieją również sytuacje, w których prawo do ochrony danych osobowych skutecznie zapewnia poszanowanie tego samego konkretnego prawa. Dotyczy to na przykład wolności wypowiedzi, biorąc pod uwagę, że tajemnica zawodowa stanowi element prawa do poszanowania życia prywatnego.
- Potrzeba ochrony praw i wolności innych osób jest jednym z kryteriów oceny zgodnego z prawem ograniczenia w korzystaniu z prawa do ochrony danych osobowych.
- W przypadku gdy w grę wchodzą różne prawa, sądy muszą dokonać ich wyważenia w celu ich pogodzenia.
- Ogólne rozporządzenie o ochronie danych wymaga od państw członkowskich pogodzenia prawa do ochrony danych osobowych z wolnością wypowiedzi i informacji.
- Państwa członkowskie mogą również przyjąć szczegółowe przepisy prawa krajowego, aby pogodzić prawo do ochrony danych osobowych z publicznym dostępem do dokumentów urzędowych i obowiązkiem zachowania tajemnicy służbowej.

Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; warunki prawnego ograniczenia tego prawa zostały szczegółowo opisane powyżej. Jednym z kryteriów prawnych ograniczeń praw, uznawanych zarówno przez RE, jak i prawo UE, jest to, że ingerencja w ochronę danych jest konieczna dla ochrony praw i wolności innych osób. W przypadkach, w których ochrona danych oddziałuje na inne prawa, zarówno ETPC, jak i TSUE wielokrotnie stwierdzały, że przy stosowaniu i wykładni art. 8 EKPC i art. 8 karty konieczne jest zapewnienie równowagi między ochroną danych a innymi prawami[83]. Kilka ważnych przykładów ilustruje, w jaki sposób osiąga się tę równowagę.

83 ETPC, *Von Hannover przeciwko Niemcom* (nr 2) [WI], nr 40660/08 i 60641/08, 7 lutego 2012 r.; TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r., pkt 48; TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 29 stycznia 2008 r., pkt 68.

Oprócz równoważenia działań prowadzonych przez te sądy, państwa mogą, w razie potrzeby, przyjąć ustawodawstwo w celu pogodzenia prawa do ochrony danych osobowych z innymi prawami. Z tego powodu ogólne rozporządzenie o ochronie danych przewiduje szereg obszarów odstępstwa krajowego.

W odniesieniu do wolności wypowiedzi RODO wymaga, by państwa członkowskie przyjmowały przepisy pozwalające pogodzić „prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji, w tym do przetwarzania dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej”[84]. Państwa członkowskie mogą również przyjąć przepisy prawne w celu pogodzenia ochrony danych z publicznym dostępem do dokumentów urzędowych i obowiązkiem zachowania tajemnicy zawodowej chronionym jako forma prawa do poszanowania życia prywatnego[85].

1.3.1. Wolność wypowiedzi

Jednym z praw, które często wchodzą w interakcję z prawem do ochrony danych, jest prawo do wolności wypowiedzi.

Wolność wypowiedzi jest chroniona na mocy art. 11 karty praw podstawowych („Wolność wypowiedzi i informacji”). Prawo to obejmuje „wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei bez ingerencji władz publicznych i bez względu na granice państwowe”. Wolność informacji, zarówno zgodnie z art. 11 karty, jak i art. 10 EKPC, chroni prawo nie tylko do przekazywania informacji, ale również do ich *otrzymywania*.

Ograniczenia wolności wypowiedzi muszą być zgodne z kryteriami przewidzianymi w art. 52 ust. 1 karty, opisanymi powyżej. Ponadto art. 11 odpowiada art. 10 EKPC. Zgodnie z art. 52 ust. 3 karty, w zakresie, w jakim zawiera ona prawa, które odpowiadają prawom zagwarantowanym w EKPC, „znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję”. Ograniczenia, które mogą być zgodnie z prawem nałożone na prawo zagwarantowane w art. 11 karty, nie mogą zatem wykraczać poza ograniczenia przewidziane w art. 10 ust. 2 EKPC, to znaczy muszą być przewidziane ustawą i konieczne w demokratycznym społeczeństwie „z uwagi na ochronę [...] dobrego imienia i praw innych osób”. Prawa te obejmują

84 Ogólne rozporządzenie o ochronie danych, art. 85.

85 Tamże, art. 86 i 90.

w szczególności prawo do poszanowania życia prywatnego i prawo do ochrony danych osobowych.

Związek pomiędzy ochroną danych osobowych a wolnością wypowiedzi reguluje art. 85 ogólnego rozporządzenia o ochronie danych, zatytułowany „Przetwarzanie a wolność wypowiedzi i informacji". Zgodnie z tym artykułem państwa członkowskie przyjmują przepisy pozwalające pogodzić prawo do ochrony danych osobowych na mocy niniejszego rozporządzenia z wolnością wypowiedzi i informacji. W szczególności wyjątki i odstępstwa od konkretnych rozdziałów ogólnego rozporządzenia o ochronie danych określa się dla przetwarzania do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej, jeżeli są one niezbędne, by pogodzić prawo do ochrony danych osobowych z wolnością wypowiedzi i informacji.

Przykład: W sprawie *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy*[86] zwrócono o określenie związku między ochroną danych a wolnością prasy[87]. Trybunał badał sprawę rozpowszechniania, za pośrednictwem usługi sms, danych podatkowych około 1,2 mln osób fizycznych uzyskanych zgodnie z prawem od fińskich organów podatkowych. Fiński organ nadzorczy ds. ochrony danych wydał decyzję wzywającą spółkę do zaprzestania rozpowszechniania tych danych. Spółka zaskarżyła tę decyzję do sądu krajowego, który zwrócił się do TSUE o wyjaśnienia w przedmiocie wykładni dyrektywy o ochronie danych. W szczególności TSUE miał sprawdzić, czy przetwarzanie danych osobowych, które udostępniły organy podatkowe, w celu umożliwienia użytkownikom telefonów komórkowych uzyskiwania danych podatkowych odnoszących się do innych osób fizycznych należy uznać za działalność prowadzoną wyłącznie w celach dziennikarskich. Stwierdziwszy, że działania spółki stanowiły „przetwarzanie danych osobowych" w rozumieniu art. 3 ust. 1 dyrektywy o ochronie danych, Trybunał przystąpił do wykładni art. 9 dyrektywy (dotyczącego przetwarzania danych osobowych i wolności wypowiedzi).

86 TSUE, C-73/07, *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy* [WI], 16 grudnia 2008 r., pkt 56, 61 i 62.

87 Sprawa dotyczyła wykładni art. 9 dyrektywy o ochronie danych – obecnie zastąpionego art. 85 ogólnego rozporządzenia o ochronie danych – który brzmiał: „Państwa członkowskie wprowadzają możliwość wyłączenia lub odstąpienia od przepisów niniejszego rozdziału, rozdziału IV i VI w przypadku przetwarzania danych osobowych wyłącznie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego jedynie wówczas, gdy jest to konieczne dla pogodzenia prawa do zachowania prywatności z przepisami dotyczącymi wolności wypowiedzi".

Trybunał w pierwszej kolejności podkreślił znaczenie prawa do wolności wypowiedzi w każdym społeczeństwie demokratycznym i uznał, że pojęcia związane z tą wolnością, w tym pojęcie dziennikarstwa, należy interpretować szeroko. Następnie zauważył, że w celu wyważenia wskazanych dwóch praw podstawowych odstępstwa od prawa do ochrony danych i ograniczenia tego prawa powinny ograniczać się do tego, co absolutnie konieczne. W tych okolicznościach TSUE uznał, że działania takie, jak prowadzone przez zainteresowane spółki, dotyczące danych pochodzących z dokumentów jawnych w świetle przepisów krajowych, mogą zostać zaklasyfikowane w ramach „działalności dziennikarskiej", jeśli ich celem jest publiczne rozpowszechnienie informacji, opinii lub myśli za pomocą jakiegokolwiek środka przekazu. Trybunał orzekł też, że taka działalność nie jest zastrzeżona dla przedsiębiorstw medialnych i może być związana z celem zarobkowym. Trybunał pozostawił jednak sądowi krajowemu ustalenie, czy tak było w tym konkretnym przypadku.

Ta sama sprawa została również zbadana przez ETPC po tym, jak sąd krajowy orzekł na podstawie wskazówek TSUE, że nakaz zaprzestania publikacji wszystkich informacji podatkowych przez organ nadzorczy stanowi uzasadnioną ingerencję w swobodę wypowiedzi spółki. Europejski Trybunał Praw Człowieka podtrzymał to podejście[88]. Trybunał stwierdził, że nawet jeśli nastąpiło naruszenie prawa przedsiębiorstw do udzielania informacji, ingerencja ta była zgodna z prawem, miała prawnie uzasadniony cel i była konieczna w demokratycznym społeczeństwie.

Trybunał przypomniał o kryteriach orzecznictwa, którymi powinny kierować się organy krajowe oraz sam Europejski Trybunał Praw Człowieka przy równoważeniu wolności wypowiedzi z prawem do poszanowania życia prywatnego. Tam, gdzie w grę wchodzi przemówienie polityczne lub debata na temat interesu publicznego, istnieje niewielkie pole do ograniczania prawa do otrzymywania i przekazywania informacji, gdyż ogół ma prawo do bycia poinformowanym i „jest to prawo istotne w społeczeństwie demokratycznym"[89]. Artykułów mających na celu wyłącznie zaspokojenie ciekawości określonego kręgu czytelników dotyczącej szczegółów życia prywatnego danej osoby, niezależnie od tego jak dobrze znanej, nie można

88 ETPC, *Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii* [WI], nr 931/13, 27 czerwca 2017 r.

89 Tamże, pkt 169.

jednak uznać za udział w debacie w interesie publicznym. Odstępstwo odnoszące się do celów dziennikarskich ma na celu umożliwienie dziennikarzom dostępu, zbierania i przetwarzania danych w celu zapewnienia im możliwości wykonywania swojej działalności dziennikarskiej. Wobec tego stwierdzono jednak istnienie interesu publicznego w zapewnieniu dostępu oraz zezwoleniu zainteresowanym spółkom na zbieranie dużych ilości stosownych danych podatkowych. Z kolei Trybunał wskazał, że nie oznaczało to istnienia interesu publicznego w masowym rozpowszechnianiu takich surowych danych w niezmienionej formie bez żadnego analitycznego opracowania. Te dane podatkowe mogły umożliwić dociekliwym członkom społeczeństwa skategoryzowanie konkretnych osób niebędących osobami publicznymi według ich statusu ekonomicznego, co mogło zostać uznane za manifestację pragnienia ogółu informacji na temat życia prywatnego innych osób. Nie można było uznać tego za udział w debacie w interesie publicznym.

Przykład: W sprawie *Google Spain*[90] TSUE zbadał, czy Google było zobowiązane do usunięcia z listy wyników wyszukiwania nieaktualnych informacji o trudnościach finansowych skarżącego. Jeżeli wyszukiwanie przeprowadzono w wyszukiwarce Google z wykorzystaniem nazwiska skarżącego, wyniki wyszukiwania zawierały linki do artykułów w starych gazetach, w których wymieniono jego związek z postępowaniem upadłościowym. Skarżący uznał to za naruszenie jego prawa do poszanowania życia prywatnego i ochrony danych osobowych, ponieważ postępowanie zostało zakończone wiele lat temu, przez co odniesienia te stały się nieistotne.

Trybunał wyjaśnił przede wszystkim, że wyszukiwarki internetowe i wyniki wyszukiwania dostarczające danych osobowych mogą określać szczegółowy profil osoby fizycznej. W świetle coraz bardziej zdigitalizowanego społeczeństwa wymóg prawidłowości danych osobowych oraz ich publikowania w taki sposób, by nie wykraczały poza to, co jest konieczne, czym jest dostarczenie informacji społeczeństwu, ma zasadnicze znaczenie dla zapewnienia wysokiego poziomu ochrony danych osobowych osób fizycznych. „Administrator danych w związku z tym przetwarzaniem winien w ramach spoczywającej na nim odpowiedzialności, przysługujących mu uprawnień i posiadanych możliwości zapewnić, iż działalność ta spełnia [określone w prawie Unii] wymogi", tak aby przewidziane w nim gwarancje były

90 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 81–83.

w pełni skuteczne. Oznacza to, że prawo do usunięcia danych osobowych, gdy przetwarzanie nie jest już konieczne lub nieaktualne, obejmuje również wyszukiwarki, które uznano za administratorów danych, a nie tylko podmioty przetwarzające dane (zob. sekcja 2.3.1).

Po zbadaniu, czy Google było zobowiązane do usunięcia linków dotyczących skarżącego TSUE stwierdził, że pod pewnymi warunkami osoby fizyczne mają prawo do uzyskania usunięcia swoich danych osobowych z wyników wyszukiwania w wyszukiwarce internetowej. Prawo to można powołać w sytuacji, gdy informacje dotyczące osoby fizycznej są nieprawidłowe, niewłaściwe, nieistotne czy też nadmierne w stosunku do celów, w jakich są one przetwarzane. TSUE przyznał, że prawo to nie jest bezwzględne; należy je zrównoważyć z innymi prawami, w szczególności interesem i prawem ogółu społeczeństwa do dostępu do informacji. Każdy wniosek o usunięcie danych wymaga indywidualnej oceny każdego przypadku w celu znalezienia równowagi między podstawowymi prawami do ochrony danych osobowych i życia prywatnego osoby, której dane dotyczą, z jednej strony, a uzasadnionymi interesami wszystkich użytkowników Internetu z drugiej strony. Trybunał przedstawił wytyczne dotyczące czynników, które należy wziąć pod uwagę przy próbie równoważenia praw. Szczególnie ważnym czynnikiem jest charakter przedmiotowych informacji. Jeżeli informacje mają charakter szczególnie chroniony w związku z ochroną życia prywatnego danej osoby i jeżeli nie ma interesu publicznego w ich udostępnianiu, ochrona danych i prywatności byłaby nadrzędna w stosunku do prawa ogółu społeczeństwa do dostępu do informacji. Z kolei jeżeli wydaje się, że osoba, której dane dotyczą, jest osobą publiczną lub że informacje te mają taki charakter, że uzasadniają udzielenie ogółowi społeczeństwa dostępu do takich informacji, wówczas uzasadnione jest naruszenie podstawowego prawa do ochrony danych i prywatności.

W następstwie tego wyroku Grupa Robocza Art. 29 przyjęła wytyczne w sprawie wykonania orzeczenia TSUE. Wytyczne zawierają wykaz wspólnych kryteriów, które mają być stosowane przez organy nadzorcze przy rozpatrywaniu skarg dotyczących wniosków osób fizycznych o usunięcie danych, a także mają stanowić dla nich wskazówki przy równoważeniu wykonywania praw[91].

91 Grupa Robocza Art. 29 (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, Bruksela, 26 listopada 2014 r.

W odniesieniu do równoważenia prawa do ochrony danych z prawem do wolności wypowiedzi ETPC wydał kilka przełomowych orzeczeń.

Przykład: W sprawie *Axel Springer AG przeciwko Niemcom*[92] ETPC uznał, że nałożony na skarżącą spółkę sądowy zakaz publikacji artykułu na temat aresztowania i skazania znanego aktora naruszał art. 10 EKPC. ETPC ponownie wymienił ustanowione w swoim orzecznictwie kryteria, które należy uwzględnić przy wyważeniu prawa do wolności wypowiedzi z prawem do poszanowania życia prywatnego:

- czy zdarzenie, którego dotyczył opublikowany artykuł, stanowiło przedmiot ogólnego zainteresowania;
- czy zainteresowana osoba była osobą publiczną;
- w jaki sposób uzyskano informacje i czy były one rzetelne.

Europejski Trybunał Praw Człowieka orzekł, że aresztowanie i skazanie aktora było publicznym faktem związanym z wymiarem sprawiedliwości, a zatem była to kwestia stanowiąca przedmiot publicznego zainteresowania; oraz że aktor był na tyle dobrze znany, aby uznać go za osobę publiczną; ponadto informacje przekazała prokuratura i ich prawidłowość nie była kwestionowana przez strony. W związku z tym ETPC orzekł, że nałożone na spółkę ograniczenia dotyczące publikacji nie były proporcjonalne do uzasadnionego celu ochrony życia prywatnego skarżącego. Trybunał stwierdził, że doszło do naruszenia art. 10 EKPC.

Przykład: Sprawa *Couderc i Hachette Filipacchi Associés przeciwko Francji*[93] dotyczyła publikacji przez francuski tygodnik wywiadu z panią Coste, która twierdziła, że książę Albert z Monako jest ojcem jej syna. W wywiadzie opisano również związek p. Coste z księciem oraz sposób, w jaki zareagował on na narodziny dziecka, wraz ze zdjęciami księcia z dzieckiem. Książę Albert wytoczył przeciwko wydawnictwu powództwo o naruszenie jego prawa do ochrony życia prywatnego. Sądy francuskie orzekły, że publikacja artykułu

92 ETPC, *Axel Springer przeciwko Niemcom* [WI], nr 39954/08, 7 lutego 2012 r., pkt 90 i 91.

93 ETPC, *Couderc i Hachette Filipacchi Associés przeciwko Francji* [WI], nr 40454/07, 10 listopada 2015 r.

wyrządziła mu nieodwracalną szkodę i zasądziły od wydawcy odszkodowanie na rzecz księcia Alberta, jak również nakazały opublikowanie szczegółów wyroku na okładce czasopisma.

Wydawcy czasopisma wnieśli skargę do ETPC, twierdząc, że wyrok sądów francuskich stanowił nieuzasadnioną ingerencję w ich prawo do wolności wypowiedzi. Europejski Trybunał Praw Człowieka musiał wyważyć prawo księcia Alberta do poszanowania życia prywatnego z prawem wydawcy do wolności wypowiedzi oraz prawem ogółu społeczeństwa do posiadania informacji. Istotne względy to także prawo p. Coste do podzielenia się swoją historią z opinią publiczną oraz interes dziecka polegający na oficjalnym ustanowieniu relacji ojciec–dziecko.

Trybunał uznał, że publikacja wywiadu stanowi ingerencję w prywatne życie księcia, a następnie zbadał, czy ingerencja ta była konieczna. Trybunał uznał, że publikacja dotyczyła osoby publicznej i interesu publicznego, ponieważ obywatele Monako mieli interes w tym, aby wiedzieć o istnieniu dziecka księcia, ponieważ przyszłość dziedzicznej monarchii jest „nierozerwalnie związana z istnieniem potomstwa", a tym samym leży w sferze zainteresowania społeczeństwa[94]. Trybunał zauważył również, że artykuł ten umożliwił p. Coste i jej dziecku skorzystanie z przysługującego im prawa do wolności wypowiedzi. Sądy krajowe nie uwzględniły należycie zasad i kryteriów wypracowanych w orzecznictwie ETPC w celu wyważenia prawa do poszanowania życia prywatnego i prawa do wolności wypowiedzi. Trybunał stwierdził, że Francja naruszyła art. 10 EKPC dotyczący wolności wypowiedzi.

W orzecznictwie ETPC jednym z kluczowych kryteriów wyważenia tych praw jest to, czy dana wypowiedź przyczynia się do debaty w ogólnym interesie publicznym.

Przykład: W sprawie *Mosley przeciwko Zjednoczonemu Królestwu*[95] krajowy tygodnik opublikował intymne zdjęcia skarżącego, osoby znanej, który następnie skutecznie wytoczył powództwo cywilne przeciwko wydawcy i uzyskał zadośćuczynienie. Pomimo zasądzonej rekompensaty finansowej skarżący skarżył się, że nadal był ofiarą naruszenia jego prawa do prywatności, ponieważ odmówiono mu możliwości wystąpienia o wydanie

94 Tamże, pkt 104–116.

95 ETPC, *Mosley przeciwko Zjednoczonemu Królestwu*, nr 48009/08, 10 maja 2011 r., pkt 129 i 130.

nakazu sądowego przed publikacją tych zdjęć ze względu na brak prawnego wymogu uprzedniego zgłoszenia przez gazetę zamiaru publikacji materiałów mogących naruszyć prawo do prywatności.

Trybunał zauważył, że chociaż rozpowszechnianie tych materiałów służyło ogólnie celom rozrywkowym, a nie edukacyjnym, niewątpliwie korzystało ono z ochrony art. 10 EKPC, która może jednak ustępować wymogom art. 8 EKPC w przypadku, gdy informacje mają charakter prywatny i intymny oraz nie ma interesu publicznego w ich upowszechnianiu. Należało wszakże zachować szczególną ostrożność, badając ograniczenia, które mogłyby działać jako forma cenzury prewencyjnej. Jeżeli chodzi o skutek odstraszający, do którego mógłby prowadzić wymóg uprzedniego zgłoszenia, wątpliwości co do jego skuteczności oraz szeroki margines uznania w tej dziedzinie, ETPC stwierdził, że istnienie prawnie wiążącego wymogu uprzedniego zgłoszenia nie jest wymagane na mocy art. 8. Trybunał stwierdził zatem, że nie doszło do naruszenia art. 8.

Przykład: W sprawie *Bohlen przeciwko Niemcom*[96] skarżący, znany piosenkarz i producent artystyczny, wydał książkę autobiograficzną, a następnie został zmuszony do usunięcia niektórych fragmentów tekstu w następstwie orzeczeń sądowych. Historia ta została szeroko opisana w mediach krajowych, a firma tytoniowa rozpoczęła żartobliwą kampanię reklamową odnoszącą się do tego wydarzenia, używając imienia skarżącego bez jego zgody. Skarżący bezskutecznie domagał się odszkodowania od firmy reklamowej z tytułu naruszenia jego praw wynikających z art. 8 EKPC. Europejski Trybunał Praw Człowieka powtórzył kryteria, którymi kieruje się przy wyważaniu prawa do poszanowania życia prywatnego i prawa do wolności wypowiedzi, i stwierdził, że nie doszło do naruszenia art. 8. Skarżący był osobą publiczną, a reklama nie odnosiła się do szczegółów jego życia prywatnego, lecz do wydarzenia publicznego, które zostało już przedstawione przez media i stanowiło część debaty publicznej. Ponadto reklama miała charakter humorystyczny i nie zawierała niczego poniżającego lub negatywnego w stosunku do skarżącego.

96 ETPC, *Bohlen przeciwko Niemcom*, nr 53495/09, 19 lutego 2015 r., pkt 45–60.

Przykład: W sprawie *Biriuk przeciwko Litwie*[97] skarżąca podniosła przed ETPC, że Litwa uchybiła ciążącemu na niej obowiązkowi zapewnienia poszanowania jej prawa do życia prywatnego, ponieważ mimo że jedna z głównych gazet poważnie naruszyła jej prywatność, sądy krajowe rozpatrujące sprawę przyznały jej śmieszną kwotę odszkodowania. Zasądzając zadośćuczynienie, sądy krajowe zastosowały przepisy prawa krajowego dotyczące informowania opinii publicznej, które nakładają niski pułap zadośćuczynienia za krzywdę spowodowaną bezprawnym publicznym udostępnieniem przez media informacji o życiu prywatnym danej osoby. Sprawa dotyczyła największej na Litwie gazety codziennej, która na pierwszej stronie opublikowała artykuł informujący, że skarżąca jest nosicielką wirusa HIV. Artykuł ten krytykuje również zachowanie skarżącej i kwestionuje jej standardy moralne.

Europejski Trybunał Praw Człowieka przypomniał, że ochrona danych osobowych, w szczególności danych medycznych, ma, na mocy EKPC, fundamentalne znaczenie dla prawa do poszanowania życia prywatnego. Poufność danych dotyczących zdrowia jest szczególnie ważna, ponieważ ujawnienie danych medycznych (w tym przypadku statusu serologicznego skarżącej) może mieć dramatyczny wpływ na życie prywatne i rodzinne danej osoby, jej sytuację zawodową i włączenie społeczne. Sąd zwrócił szczególną uwagę na fakt, że zgodnie z raportem zamieszczonym w gazecie personel medyczny szpitala udzielił informacji o stanie zdrowia skarżącej, w sposób oczywisty naruszając ciążący na nim obowiązek zachowania tajemnicy lekarskiej. W ten sposób nie doszło do uzasadnionej ingerencji w prawo skarżącej do życia prywatnego.

Artykuł został opublikowany w prasie, a wolność wypowiedzi jest również jednym z praw podstawowych w ramach EKPC. Jednakże badając, czy istnienie interesu publicznego uzasadnia publikację tego rodzaju informacji o skarżącej, Trybunał stwierdził, że głównym celem publikacji było zwiększenie sprzedaży gazety poprzez zaspokojenie ciekawości czytelnika. Nie można uznać, że taki cel stanowi wkład w debatę w ogólnym interesie społecznym. Ponieważ chodziło o „oburzające nadużycie wolności prasy", poważne ograniczenia w zakresie naprawienia szkody oraz niewielka kwota

97 ETPC, *Biriuk przeciwko Litwie*, nr 23373/03, 25 listopada 2008 r.

zadośćuczynienia przewidziana w prawie krajowym spowodowały, że Litwa uchybiła swojemu pozytywnemu zobowiązaniu do ochrony prawa skarżącej do życia prywatnego. Trybunał orzekł, że doszło do naruszenia art. 8 EKPC.

Prawo do wolności wypowiedzi i prawo do ochrony danych osobowych nie zawsze są ze sobą sprzeczne. Istnieją przypadki, w których skuteczna ochrona danych osobowych gwarantuje wolność wypowiedzi.

Przykład: W sprawie *Tele2 Sverige* Trybunał stwierdził, że ingerencja spowodowana przez dyrektywę 2006/24 (dyrektywę w sprawie zatrzymywania danych) stanowiła „daleko posuniętą" ingerencję w prawa podstawowe ustanowione w art. 7 i 8 karty. „Ponadto [...] okoliczność, że zatrzymywanie i późniejsze wykorzystywanie danych jest dokonywane bez poinformowania o tym abonenta lub zarejestrowanego użytkownika, może wywołać u osób, których danych są zatrzymywane czy też wykorzystywane, poczucie, iż ich życie prywatne podlega stałemu nadzorowi". Trybunał Sprawiedliwości stwierdził także, że zatrzymywanie danych o ruchu i danych o lokalizacji stosowane w sposób uogólniony może mieć wpływ na korzystanie ze środków łączności elektronicznej, a „w konsekwencji – na korzystanie przez użytkowników owych środków z zagwarantowanej w art. 11 Karty praw podstawowych swobody wypowiedzi"[98]. W tym kontekście poprzez wymóg ścisłych gwarancji dotyczących zatrzymywania danych, tak aby nie odbywało się to w sposób uogólniony, przepisy w zakresie ochrony danych w efekcie przyczyniają się do urzeczywistnienia wolności wypowiedzi.

Jeśli chodzi o prawo do otrzymywania informacji, które również wpisuje się w wolność wypowiedzi, wzrasta świadomość, jak ważna dla funkcjonowania społeczeństwa demokratycznego jest przejrzystość działań rządowych. Przejrzystość jest celem leżącym w interesie ogólnym, który mógłby tym samym uzasadniać ingerencję w prawo do ochrony danych, jeżeli jest to konieczne i proporcjonalne, jak wyjaśniono w sekcji 1.2. W rezultacie w ciągu ostatnich dwudziestu lat prawo dostępu do dokumentów będących w posiadaniu organów publicznych zostało uznane za

98 TSUE, sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.* [WI], 21 grudnia 2016 r., pkt 37 i 101; TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.,pkt 28.

ważne prawo każdego obywatela UE oraz każdej osoby fizycznej lub prawnej mającej miejsce zamieszkania lub statutową siedzibę w państwie członkowskim.

W prawie RE można się odnieść do zasad zawartych w zaleceniu w sprawie dostępu do dokumentów urzędowych, które stanowiło inspirację dla autorów projektu Konwencji w sprawie dostępu do dokumentów urzędowych (konwencji nr 205)[99].

W prawie UE prawo dostępu do dokumentów jest zagwarantowane rozporządzeniem (WE) nr 1049/2001 w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (rozporządzeniem o dostępie do dokumentów)[100]. Artykuł 42 karty i art. 15 ust. 3 TFUE rozszerzyły prawo dostępu do „dokumentów instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy".

Prawo to może stać w sprzeczności z prawem do ochrony danych, jeżeli dostęp do dokumentu spowodowałby ujawnienie danych osobowych innych osób. Artykuł 86 ogólnego rozporządzenia o ochronie danych wyraźnie przewiduje, że dane osobowe zawarte w dokumentach urzędowych, które posiada organ lub podmiot publiczny mogą zostać przez ten organ lub podmiot ujawnione zgodnie z prawem Unii[101] lub prawem państwa członkowskiego dla pogodzenia publicznego dostępu do dokumentów urzędowych z prawem do ochrony danych osobowych na mocy rozporządzenia.

Wnioski o dostęp do dokumentów lub informacji będących w posiadaniu organów publicznych mogą zatem wymagać wyważenia z prawem do ochrony danych osób, których dane zawarte są w dokumentach, których dotyczy wniosek.

Przykład: W sprawie *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen*[102] TSUE miał za zadanie ocenić proporcjonalność wymaganej w prawodawstwie UE imiennej publikacji nazwisk beneficjentów

99 Rada Europy, Komitet Ministrów (2002), Recommendation Rec(81)19 and Recommendation Rec(2002)2 to member states on access to official documents, 21 lutego 2002 r.; Rada Europy, konwencja o dostępie do dokumentów urzędowych, CETS nr 205, 18 czerwca 2009 r. Konwencja nie weszła jeszcze w życie.

100 Rozporządzenie (WE) nr 1049/2001 Parlamentu Europejskiego i Rady z dnia 30 maja 2001 r. w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji, Dz.U. L 145 z 31.05.2001.

101 Artykuł 42 karty, art. 15 ust. 3 TFUE i rozporządzenie 1049/2009.

102 TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r., pkt 47–52, 58, 66–67, 75, 86 i 92.

dopłat rolnych oraz otrzymanych przez nich kwot. Publikacja miała zwiększyć przejrzystość i przyczynić się do kontroli publicznej w zakresie właściwego wykorzystania środków publicznych przez administrację. Kilku beneficjentów zakwestionowało proporcjonalność tej publikacji.

Trybunał Sprawiedliwości, zauważając, że prawo do ochrony danych nie ma charakteru absolutnego, stwierdził, że publikacja na stronie internetowej danych określających beneficjentów dwóch unijnych funduszy pomocy rolnej oraz dokładną wysokość otrzymywanych kwot stanowi ingerencję w ich życie prywatne, a w szczególności w ochronę danych osobowych.

Trybunał stwierdził, że taka ingerencja w art. 7 i 8 karty jest przewidziana ustawą i służy realizacji celu leżącego w interesie ogólnym, uznanego przez UE, a mianowicie zwiększeniu przejrzystości wykorzystania funduszy wspólnotowych. Trybunał orzekł jednak, że publikacja nazwisk osób fizycznych będących beneficjentami pomocy UE w dziedzinie rolnictwa z tych dwóch funduszy oraz dokładnych otrzymanych kwot stanowi środek nieproporcjonalny i nieuzasadniony w świetle art. 52 ust. 1 karty. Trybunał uznał znaczenie, jakie w demokratycznym społeczeństwie ma informowanie podatników o wykorzystaniu funduszy publicznych. Jednakże z uwagi na to, że „celowi przejrzystości nie można jednak przyznać automatycznego pierwszeństwa przed prawem do ochrony danych osobowych”[103], przed udostępnieniem informacji dotyczących osoby fizycznej instytucje były zobowiązane wyważyć interes Unii w zapewnieniu przejrzystości jej działań i ograniczenie w wykonywaniu praw do prywatności i ochrony danych, którego doświadczyli beneficjenci wskutek publikacji.

Trybunał Sprawiedliwości uznał, że instytucje UE nie przeprowadziły prawidłowo tej analizy, ponieważ można było przewidzieć środki, które w mniejszym stopniu naruszyłyby prawa podstawowe jednostek, a jednocześnie skutecznie przyczyniałyby się do realizacji celu w zakresie przejrzystości, jakiemu służyć ma publikacja. Na przykład zamiast ogólnej publikacji dotyczącej wszystkich beneficjentów, z podaniem ich nazwisk i dokładnych kwot otrzymanych przez każdego z nich, można by dokonać rozróżnienia według odpowiednich kryteriów, takich jak okresy, w których otrzymali tę pomoc, jej częstość czy też rodzaj i wysokość[104]. Trybunał

103 Tamże, pkt 85.

104 Tamże, pkt 89.

stwierdził zatem częściową nieważność przepisów UE dotyczących publikowania informacji dotyczących beneficjentów europejskich funduszy rolnych.

Przykład: W sprawie *Rechnungshof przeciwko Österreichischer Rundfunk i in.*[105] TSUE dokonał przeglądu zgodności niektórych przepisów austriackich z unijnym prawem o ochronie danych. Przepisy nakładały na organ państwowy obowiązek zbierania i przekazywania danych o dochodach do celów publikowania imienia i nazwiska oraz dochodów pracowników różnych podmiotów publicznych w udostępnianym ogółowi społeczeństwa sprawozdaniu rocznym. Niektóre osoby fizyczne odmówiły przekazania swoich danych ze względu na ochronę danych.

W swojej opinii TSUE powołał się na ochronę praw podstawowych jako ogólną zasadę prawa UE oraz na art. 8 EKPC, przypominając, że Karta praw podstawowych nie była w owym czasie wiążąca. Trybunał orzekł, że zbieranie danych o dochodach osób fizycznych uzyskiwanych z pracy, a w szczególności ich przekazywanie osobom trzecim, wchodzi w zakres prawa do poszanowania życia prywatnego i stanowi naruszenie tego prawa. Ingerencja mogłaby być uzasadniona, gdyby była przewidziana przez ustawę, dążyła do osiągnięcia zgodnego z prawem celu i była konieczna w demokratycznym społeczeństwie do osiągnięcia tego celu. Trybunał zauważył, że przepisy austriackie realizowały zgodny z prawem cel, jakim było utrzymanie wynagrodzeń pracowników podmiotów publicznych w rozsądnych granicach – a więc kwestia związana także z dobrobytem gospodarczym kraju. Interes Austrii w zapewnieniu jak najlepszego wykorzystania środków publicznych należy jednak wyważyć z powagą ingerencji w prawo zainteresowanych osób do poszanowania ich życia prywatnego.

Pozostawiając sądowi krajowemu ustalenie, czy publikacja danych dotyczących dochodów osób fizycznych jest konieczna i proporcjonalna do celu, jaki przyświeca tym przepisom, TSUE wezwał sąd krajowy do zbadania, czy cel ten nie mógł zostać osiągnięty w sposób równie skuteczny za pomocą

105 TSUE, sprawy połączone C-465/00, C-138/01 i C-139/01, *Rechnungshof przeciwko Österreichischer Rundfunk i in.* oraz *Christa Neukomm i Joseph Lauermann przeciwko Österreichischer Rundfunk*, 20 maja 2003 r.

mniej inwazyjnych środków. Przykładem takiego działania mogłoby być na przykład przekazanie imiennych informacji jedynie organom kontrolnym, a nie opinii publicznej.

Przy okazji kolejnych spraw okazało się, że wyważenie ochrony danych i dostępu do dokumentów wymaga szczegółowej analizy każdego przypadku z osobna. Żadne z praw nie może automatycznie zastąpić drugiego. Trybunał miał możliwość dokonania wykładni prawa dostępu do dokumentów zawierających dane osobowe w dwóch sprawach.

Przykład: W sprawie *Komisja Europejska przeciwko Bavarian Lager*[106] TSUE określił zakres ochrony danych osobowych w kontekście dostępu do dokumentów instytucji UE oraz związek między rozporządzeniami nr 1049/2001 (rozporządzeniem o dostępie do dokumentów) i nr 45/2001 (rozporządzeniem o ochronie danych przez instytucje UE). Utworzona w 1992 r. spółka Bavarian Lager importuje butelkowane niemieckie piwo do Zjednoczonego Królestwa, głównie w celu jego sprzedaży w pubach i barach. Napotkała jednak trudności, gdyż ustawodawstwo brytyjskie *de facto* faworyzowało producentów krajowych. W odpowiedzi na skargę Bavarian Lager Komisja Europejska postanowiła wszcząć postępowanie przeciwko Zjednoczonemu Królestwu w sprawie uchybienia zobowiązaniom państwa członkowskiego, co poskutkowało zmianą spornych postanowień i dostosowaniem ich do prawa UE. Bavarian Lager zwróciła się następnie do Komisji o udostępnienie jej między innymi kopii protokołu ze spotkania, w którym uczestniczyli przedstawiciele Komisji, władz brytyjskich oraz *Confédération des Brasseurs du Marché Commun* (CBMC). Komisja zgodziła się ujawnić niektóre dokumenty odnoszące się do spotkania, ale utajniła pięć nazwisk pojawiających się w protokole, gdyż dwie osoby wyraźnie sprzeciwiły się ujawnieniu ich tożsamości, a Komisja nie była w stanie skontaktować się z trzema pozostałymi. Decyzją z dnia 18 marca 2004 r. Komisja odrzuciła nowy wniosek Bavarian Lager o udostępnienie kompletnego protokołu ze spotkania, powołując się w szczególności na ochronę życia prywatnego tych osób zagwarantowaną rozporządzeniem o ochronie danych przez instytucje UE.

106 TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.* [WI], 29 czerwca 2010 r.

Nie zgadzając się z tym stanowiskiem, Bavarian Lager wniosła skargę do Sądu Pierwszej Instancji. Sąd ten stwierdził nieważność decyzji Komisji wyrokiem z dnia 8 listopada 2007 r. (sprawa T-194/04, *Bavarian Lager przeciwko Komisji)*, uznając w szczególności, że sama obecność nazwisk wspomnianych osób na liście osób biorących udział w spotkaniu w imieniu reprezentowanej instytucji nie narusza prawa do ochrony życia prywatnego i nie zagraża w jakikolwiek sposób życiu prywatnemu tych osób.

W wyniku odwołania złożonego przez Komisję TSUE uchylił wyrok Sądu Pierwszej Instancji. Trybunał uznał, że w rozporządzeniu o dostępie do dokumentów ustanowiono „szczególny i wzmocniony system ochrony osoby, której dane osobowe mogłyby zostać ewentualnie upublicznione". Według TSUE w sytuacji, gdy wniosek sporządzony w oparciu o rozporządzenie o dostępie do dokumentów ma na celu uzyskanie dostępu do dokumentów zawierających dane osobowe, przepisy rozporządzenia o ochronie danych przez instytucje UE znajdują w pełni zastosowanie. Trybunał stwierdził następnie, że Komisja słusznie odrzuciła wniosek o dostęp do kompletnego protokołu ze spotkania z października 1996 r. Przy braku zgody pięciu uczestników tego spotkania Komisja wystarczająco zastosowała się do obowiązku przejrzystości, udostępniając wersję spornego dokumentu po utajnieniu ich nazwisk.

Ponadto według TSUE „skoro Bavarian Lager nie dostarczyła żadnego wyraźnego i prawnie usankcjonowanego uzasadnienia ani żadnego przekonującego argumentu w celu wykazania konieczności przekazania tych danych osobowych, Komisja nie miała możliwości wyważenia różnych interesów zainteresowanych stron. Nie miała też możliwości sprawdzenia, czy istniał jakikolwiek powód, by zakładać, że uzasadnione interesy osób, których dane dotyczą, mogą zostać naruszone", co nakazuje rozporządzenie o ochronie danych przez instytucje UE.

Przykład: W sprawie *Client Earth, PAN Europe przeciwko EFSA*[107] TSUE zbadał, czy decyzja Europejskiego Urzędu do spraw Bezpieczeństwa Żywności (EFSA) odmawiająca skarżącym pełnego dostępu do dokumentów była konieczna w celu ochrony praw do prywatności i ochrony danych osób, których dokumenty te dotyczyły. Dokumenty dotyczyły sprawozdania

107 TSUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) przeciwko Europejskiemu Urzędowi ds. Bezpieczeństwa Żywności (EFSA), Komisji Europejskiej*, 16 lipca 2015 r.

z projektu wytycznych przygotowanego przez grupę roboczą EFSA we współpracy z biegłymi zewnętrznymi w sprawie wprowadzania do obrotu środków ochrony roślin. Początkowo EFSA przyznał częściowy dostęp skarżącym, odmawiając dostępu do niektórych wersji roboczych projektu wytycznych. Następnie umożliwił on dostęp do wersji roboczej, która zawierała indywidualne uwagi biegłych zewnętrznych. Urząd ukrył nazwiska wspomnianych biegłych, powołując się na art. 4 ust. 1 lit. b) rozporządzenia (WE) nr 45/2001 w sprawie publicznego dostępu do dokumentów instytucji Unii oraz konieczność ochrony prywatności biegłych zewnętrznych. W postępowaniu w pierwszej instancji Sąd UE utrzymał decyzję EFSA.

W wyniku odwołania TSUE uchylił wyrok sądu pierwszej instancji. Trybunał stwierdził, że przekazanie danych osobowych w tej sprawie było konieczne w celu sprawdzenia bezstronności każdego z biegłych przy wykonywaniu ich misji naukowej i zapewnienia przejrzystości procesu decyzyjnego w EFSA. Trybunał jest zdania, że EFSA nie wskazał, w jaki sposób ujawnienie nazwisk biegłych zewnętrznych, którzy przedstawili indywidualne uwagi w przedmiocie projektu wytycznych miałoby naruszyć zgodne z prawem interesy biegłych. Ogólne twierdzenie, iż ujawnienie powodowałoby ryzyko naruszenia życia prywatnego i integralności rzeczonych biegłych, nie jest wystarczające, jeżeli nie jest w żaden inny sposób poparte jakimkolwiek właściwym w danym przypadku dowodem.

Zgodnie z tymi wyrokami ingerencja w prawo do ochrony danych w kontekście dostępu do dokumentów wymaga szczególnego i uzasadnionego powodu. Prawo dostępu do dokumentów nie może automatycznie przeważyć nad prawem do ochrony danych[108].

To podejście jest zbieżne z podejściem ETPC w odniesieniu do prywatności i dostępu do dokumentów, jak wykazano w poniższym wyroku. W wyroku w sprawie *Magyar Helsinki* ETPC stwierdził, że art. 10 nie przyznaje osobie fizycznej prawa dostępu do informacji będących w posiadaniu organu publicznego ani nie zobowiązuje rządu do przekazywania takich informacji osobie fizycznej. Takie prawo lub obowiązek może jednak powstać – po pierwsze, w przypadku gdy ujawnienie informacji jest wymagane na mocy prawomocnego orzeczenia sądu; po drugie, gdy dostęp do informacji ma zasadnicze znaczenie dla korzystania przez daną osobę z jej prawa do wolności

108 Zob. jednak szczegółowe rozważania EIOD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling*, Bruksela, 24 marca 2011 r.

wypowiedzi – w szczególności wolności otrzymywania i przekazywania informacji – i gdy odmowa dostępu do informacji mogłaby stanowić ingerencję w to prawo[109]. To czy i w jakim zakresie odmowa dostępu do informacji stanowi ingerencję w wolność wypowiedzi skarżącego, należy oceniać w każdym indywidualnym przypadku i w świetle jego szczególnych okoliczności, takich jak: (i) cel wniosku o udzielenie informacji, (ii) charakter poszukiwanych informacji, (iii) rola wnioskodawcy oraz (iv) czy informacje były gotowe i dostępne.

Przykład: W sprawie *Magyar Helsinki Bizottság przeciwko Węgrom*[110] skarżąca, organizacja pozarządowa zajmująca się prawami człowieka, zwróciła się do policji z żądaniem udzielenia informacji dotyczących pracy obrońców ustanowionych z urzędu, na potrzeby opracowania w przedmiocie funkcjonowania systemu obrońców publicznych na Węgrzech. Policja odmówiła udzielenia informacji, argumentując, że stanowią one dane osobowe niepodlegające ujawnieniu. Stosując powyższe kryteria, ETPC orzekł, że doszło do ingerencji w prawo chronione na mocy art. 10. Dokładniej rzecz ujmując, skarżąca chciała skorzystać z prawa do udzielenia informacji w sprawie interesu publicznego, w tym celu dążyła do uzyskania dostępu do informacji, a informacje te były niezbędne do skorzystania z prawa skarżącej do wolności wypowiedzi. Informacje dotyczące mianowania obrońców publicznych były kwestią leżącą w interesie opinii publicznej. Nie było powodu, aby wątpić, że przedmiotowe badanie zawierało informacje, które skarżąca zobowiązała się podać do wiadomości publicznej i które opinia publiczna miała prawo otrzymać. Trybunał upewnił się zatem, że dostęp do żądanych informacji jest niezbędny do tego, aby skarżąca mogła wypełnić to zadanie. Wreszcie informacje te były gotowe i dostępne.

ETPC doszedł do wniosku, że odmowa dostępu do informacji w tej sprawie naruszyła samą istotę wolności otrzymywania informacji. Dochodząc do tego wniosku, Trybunał zbadał w szczególności cel żądanych informacji i ich wkład w ważną debatę publiczną, charakter żądanych informacji i to, czy stanowiły one kwestię istotną z punktu widzenia interesu publicznego, a także rolę, jaką skarżąca w tej sprawie odgrywała w społeczeństwie.

109 ETPC, *Magyar Helsinki Bizottság przeciwko Węgrom* [WI], nr 18030/11, 8 listopada 2016 r., pkt 148.

110 Tamże, pkt 181, 187–200.

W swoim toku rozumowania Trybunał zauważył, że badanie przeprowadzone przez organizację pozarządową dotyczyło funkcjonowania wymiaru sprawiedliwości i prawa do rzetelnego procesu sądowego, które w ramach EKPC było prawem o pierwszorzędnym znaczeniu. Ponieważ żądane informacje nie dotyczyły danych spoza domeny publicznej, prawa do prywatności osób, których dane dotyczą (publicznych obrońców z urzędu), nie zostałyby naruszone, gdyby policja udostępniła skarżącej te informacje. Informacje, o które wystąpiła skarżąca, miały charakter statystyczny i dotyczyły liczby obrońców z urzędu powołanych do reprezentowania oskarżonych w publicznych postępowaniach karnych.

W opinii Trybunału, biorąc pod uwagę, że analiza miała na celu przyczynienie się do ważnej debaty leżącej w interesie ogólnym, wszelkie ograniczenia dotyczące proponowanej publikacji przez organizację pozarządową powinny były zostać poddane jak najściślejszej kontroli. Informacje, o których mowa, były w interesie publicznym, ponieważ interes publiczny obejmuje „kwestie mogące rodzić znaczne kontrowersje, odnoszące się do ważnego problemu społecznego lub wiążące się z problemem, o którym społeczeństwo chciałoby być poinformowane”[111]. Obejmowałby on zatem z pewnością dyskusję na temat przebiegu postępowania sądowego i rzetelnego procesu, co było przedmiotem badania przeprowadzonego przez skarżącą. Równoważąc różne wchodzące w grę prawa i stosując zasadę proporcjonalności, ETPC orzekł, że miało miejsce nieuzasadnione naruszenie praw skarżącej wynikających z art. 10 EKPC.

1.3.2. Tajemnica zawodowa

Zgodnie z prawem krajowym niektóre komunikaty mogą podlegać obowiązkowi zachowania tajemnicy zawodowej. Tajemnicę zawodową można rozumieć jako szczególny obowiązek etyczny, który wiąże się z obowiązkiem prawnym nieodłącznie związanym z określonymi zawodami i funkcjami, opartymi na wierze i zaufaniu. Osoby i instytucje wypełniające te funkcje zobowiązane są do nieujawniania informacji poufnych, które otrzymały w trakcie wykonywania swoich obowiązków. Tajemnica zawodowa dotyczy w szczególności zawodu lekarza oraz wymiany informacji pomiędzy prawnikiem a klientem, przy czym w wielu jurysdykcjach uznaje się również obowiązek zachowania tajemnicy zawodowej w sektorze finansowym.

111 Tamże, pkt 156.

Tajemnica zawodowa nie jest prawem podstawowym, ale jest chroniona jako forma prawa do poszanowania życia prywatnego. Na przykład TSUE orzekał w niektórych sprawach, że „zakaz ujawniania pewnych informacji uznanych za poufne może bowiem być niezbędny do ochrony prawa podstawowego przedsiębiorstwa do ochrony życia prywatnego, któremu to prawu poświęcono art. 8 [...] EKPC oraz art. 7 karty”[112]. Do ETPC zwrócono się także o rozstrzygnięcie, czy ograniczenia tajemnicy zawodowej stanowią naruszenie art. 8 EKPC, co zostało zilustrowane w przytoczonych przykładach.

Przykład: W sprawie *Pruteanu przeciwko Rumunii*[113] skarżący działał w charakterze adwokata spółki handlowej, której uniemożliwiono dokonywanie transakcji bankowych w związku z zarzutami oszustwa. Podczas dochodzenia w tej sprawie sądy rumuńskie upoważniły organy ścigania do przechwytywania i rejestrowania przez pewien okres rozmów telefonicznych partnera spółki. Nagrania i przechwycenia obejmowały jego rozmowy z adwokatem.

Alexandru Pruteanu twierdził, że stanowiło to naruszenie jego prawa do poszanowania życia prywatnego i korespondencji. W swoim wyroku ETPC podkreślił status i znaczenie relacji adwokata z klientem. Przechwytywanie rozmów adwokata z klientem niewątpliwie naruszało tajemnicę zawodową, która była podstawą relacji między tymi dwiema osobami. W takim przypadku adwokat mógłby również złożyć skargę na ingerencję w jego prawo do poszanowania życia prywatnego i korespondencji. Trybunał orzekł, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Brito Ferrinho Bexiga Villa-Nova przeciwko Portugalii*[114] skarżąca, adwokat, odmówiła ujawnienia wyciągów z konta bankowego organom podatkowym ze względu na tajemnicę zawodową i tajemnicę bankową. Prokuratura wszczęła dochodzenie w sprawie oszustwa podatkowego i wystąpiła o zawieszenie upoważnienia do zachowania tajemnicy zawodowej. Sądy krajowe nakazały zawieszenie stosowania zasad poufności i tajemnicy bankowej, uznając, że interes publiczny powinien przeważać nad interesem prywatnym skarżącej.

112 TSUE, T-462/12 R, *Pilkington Group Ltd przeciwko Komisji Europejskiej*, Postanowienie Prezesa Sądu z dnia 11 marca 2013 r., pkt 44.

113 ETPC, *Pruteanu przeciwko Rumunii*, nr 30181/05, 3 lutego 2015 r.

114 ETPC, *Brito Ferrinho Bexiga Villa-Nova przeciwko Portugalii*, nr 69436/10, 1 grudnia 2015 r.

Gdy sprawa trafiła do ETPC, Trybunał orzekł, że dostęp do wyciągów bankowych skarżącej stanowi ingerencję w jej prawo do poszanowania tajemnicy zawodowej, które wchodzi w zakres życia prywatnego. Ingerencja miała podstawę prawną, ponieważ opierała się na kodeksie postępowania karnego i miała prawnie uzasadniony cel. Badając jednak konieczność i proporcjonalność ingerencji, ETPC zwrócił uwagę na fakt, że postępowanie o zniesienie poufności było prowadzone bez udziału lub wiedzy skarżącej. W związku z tym skarżąca nie była w stanie przedstawić swoich argumentów. Ponadto, mimo że prawo krajowe przewidywało konieczność konsultacji ze stowarzyszeniem prawników w takich postępowaniach, nie przeprowadzono konsultacji z tym stowarzyszeniem. Wreszcie skarżąca nie miała możliwości skutecznego zaskarżenia zniesienia poufności ani żadnego środka prawnego, za pomocą którego mogłaby zaskarżyć ten środek. Ze względu na brak gwarancji proceduralnych i skutecznej kontroli sądowej nad środkiem zawieszającym obowiązek zachowania poufności, ETPC stwierdził naruszenie art. 8 EKPC.

Wzajemne oddziaływanie między tajemnicą zawodową a ochroną danych ma często charakter ambiwalentny. Z jednej strony przepisy i gwarancje w zakresie ochrony danych ustanowione w prawodawstwie pomagają zapewnić tajemnicę zawodową. Na przykład przepisy nakładające na administratorów i podmioty przetwarzające obowiązek wdrożenia solidnych środków bezpieczeństwa danych mają na celu zapobieganie, między innymi, utracie poufności danych osobowych chronionych tajemnicą zawodową. Ponadto ogólne rozporządzenie UE o ochronie danych umożliwia przetwarzanie danych dotyczących zdrowia, które stanowią szczególną kategorię danych osobowych zasługujących na większą ochronę, ale uzależnia je od istnienia odpowiednich i konkretnych środków służących ochronie praw osób, których dane dotyczą, w szczególności tajemnicy zawodowej[115].

Z drugiej strony, obowiązek zachowania tajemnicy zawodowej nałożony na administratorów i podmioty przetwarzające w odniesieniu do niektórych danych osobowych może ograniczać prawa osób, których dane dotyczą, w szczególności prawo do otrzymywania informacji. Mimo że ogólne rozporządzenie o ochronie danych zawiera obszerny wykaz wraz z informacją, która, co do zasady, winna być podawana w przypadku pozyskiwania danych osobowych w sposób inny niż od osoby, której dane dotyczą, ów obowiązek ujawnienia nie znajduje zastosowania, gdy dane

115 Ogólne rozporządzenie o ochronie danych, art. 9 ust. 2 lit. h) i art. 9 ust. 3.

osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii lub w prawie państwa członkowskiego[116].

Ogólne rozporządzenie o ochronie danych (RODO) przewiduje, że państwa członkowskie mogą – w granicach rozporządzenia – przyjąć przepisy szczegółowe mające chronić obowiązek zachowania tajemnicy zawodowej lub innej równoważnej tajemnicy, o ile jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy zawodowej[117].

Ogólne rozporządzenie o ochronie danych przewiduje, że państwa członkowskie mogą przyjąć przepisy szczególne określające uprawnienia organów nadzorczych wobec administratorów lub podmiotów przetwarzających, którzy podlegają obowiązkowi zachowania tajemnicy zawodowej. Te przepisy szczegółowe dotyczą uprawnień do uzyskania dostępu do pomieszczeń administratora lub podmiotu przetwarzającego, jego sprzętu do przetwarzania danych i przechowywanych danych osobowych, w przypadku gdy takie dane osobowe otrzymano w trakcie czynności objętych obowiązkiem zachowania tajemnicy. W związku z tym organy nadzorcze, którym powierzono ochronę danych, muszą przestrzegać obowiązku zachowania tajemnicy zawodowej, który wiąże administratorów i podmioty przetwarzające. Ponadto członkowie samych organów nadzorczych podlegają również obowiązkowi zachowania tajemnicy zawodowej w trakcie pełnienia przez nich funkcji i po zakończeniu kadencji. Podczas wykonywania swoich zadań członkowie i personel organów nadzorczych mogą powziąć wiedzę na temat informacji poufnych. Artykuł 54 ust. 2 rozporządzenia wyraźnie przewiduje, że mają oni obowiązek zachowania tajemnicy zawodowej w odniesieniu do tego rodzaju informacji poufnych.

Ogólne rozporządzenie o ochronie danych wymaga, aby państwa członkowskie powiadamiały Komisję o przepisach, które przyjmują w celu pogodzenia ochrony danych i zasad ustanowionych w rozporządzeniu z obowiązkiem zachowania tajemnicy zawodowej.

1.3.3. Wolność wyznania i przekonań

Wolność wyznania i przekonań jest chroniona na mocy art. 9 EKPC (wolność myśli, sumienia i wyznania) oraz art. 10 Karty praw podstawowych UE. Dane osobowe, które ujawniają przekonania religijne lub filozoficzne, są uznawane za „dane

116 Tamże, art. 14 ust. 5 lit. d).

117 Tamże, motyw 164 i art. 90.

szczególnie chronione" zarówno na mocy prawa UE, jak i prawa RE, a ich przetwarzanie i wykorzystywanie podlega zwiększonej ochronie.

Przykład: Skarżący w sprawie *Sinak Isik przeciwko Turcji*[118] był członkiem wspólnoty religijnej alewitów, w których wierze widać wpływy sufizmu i innych przedislamskich przekonań i jest uważana przez niektórych uczonych za odrębną religię, a przez innych za część religii muzułmańskiej. Skarżący skarżył się, że wbrew jego woli w jego dokumencie tożsamości w polu wskazującym na wyznanie wskazano „islam", a nie „alewi". Sądy krajowe odrzuciły jego wniosek o zmianę wpisu w dowodzie tożsamości na „alewi" na tej podstawie, że słowo to oznaczało podgrupę islamu, a nie odrębną religię. Skarżący zarzucił następnie przed ETPC, że został zobowiązany do ujawnienia swojej wiary bez jego zgody, ponieważ obowiązkowe było wskazanie wyznania danej osoby w dokumencie tożsamości oraz że stanowiło to naruszenie jego prawa do wolności wyznania i sumienia, w szczególności biorąc pod uwagę fakt, że określenie „islam" w dokumencie tożsamości było nieprawidłowe.

Europejski Trybunał Praw Człowieka podkreślił, że wolność wyznania oznacza wolność uzewnętrzniania religii danej osoby we wspólnocie z innymi, publicznie oraz w kręgu osób wyznających tę samą wiarę, ale także indywidualnie i prywatnie. Obowiązujące wówczas ustawodawstwo krajowe zobowiązywało osoby fizyczne do posiadania przy sobie dowodu tożsamości, dokumentu, który należało okazać na żądanie władz publicznych lub przedsiębiorstw prywatnych, w którym wskazano ich wyznanie. Obowiązek ten nie uwzględniał okoliczności, że prawo do uzewnętrzniania swojej religii wiązało się także z prawem rozumianym jako odwrotność, tj. prawem do nieujawniania swoich przekonań. Mimo że rząd argumentował, iż ustawodawstwo krajowe zostało zmienione tak, aby jednostki mogły wnioskować o pozostawienie pola dotyczącego wyznania w ich dowodach tożsamości pustego, w opinii Trybunału sam fakt konieczności wnioskowania o usunięcie wyznania mógł stanowić ujawnienie informacji o ich nastawieniu do wyznania. Ponadto w sytuacji gdy dowody tożsamości zawierają pole do wskazania wyznania, pozostawienie go pustego ma szczególne konotacje, ponieważ posiadacze dowodu tożsamości bez informacji na temat wyznania

118 ETPC, *Sinan Işık przeciwko Turcji*, nr 21924/05, 2 lutego 2010 r.

wyróżniają się spośród tych, którzy mają dowód potwierdzający ich przekonania. Trybunał stwierdził, że ustawodawstwo krajowe naruszało art. 9 EKPC.

Działalność kościołów i związków lub wspólnot wyznaniowych może jednak wymagać przetwarzania danych osobowych ich członków w celu umożliwienia przekazywania i organizowania działalności w ramach zgromadzenia. W związku z tym kościoły i związki wyznaniowe często wprowadzały w życie przepisy dotyczące przetwarzania danych osobowych. Zgodnie z art. 91 ogólnego rozporządzenia o ochronie danych, jeżeli zasady te są szczegółowe, mogą one być nadal stosowane, pod warunkiem że zostaną dostosowane do przepisów rozporządzenia. Kościoły i związki wyznaniowe, które posiadają takie zasady, muszą podlegać nadzorowi niezależnego organu nadzorczego, który może być dla nich specyficzny, pod warunkiem że spełniają one wymogi ogólnego rozporządzenia o ochronie danych dotyczące takich organów[119].

Organizacje religijne mogą przetwarzać dane osobowe z kilku powodów – na przykład w celu utrzymywania kontaktu ze zgromadzeniem lub przekazywania informacji o organizowanych wydarzeniach i uroczystościach religijnych lub charytatywnych. W niektórych państwach kościoły muszą prowadzić rejestry swoich członków ze względów podatkowych, ponieważ przynależność do instytucji religijnych może mieć wpływ na podatki płacone przez osoby fizyczne. W każdym razie zgodnie z prawem europejskim dane ujawniające przekonania religijne są danymi szczególnie chronionymi, a kościoły muszą ponosić odpowiedzialność za zarządzanie danymi i ich przetwarzanie, zwłaszcza że informacje przetwarzane przez organizacje religijne często dotyczą dzieci, osób starszych lub innych, bardziej narażonych na zagrożenia członków społeczeństwa.

1.3.4. Wolność sztuki i nauki

Kolejnym prawem, które należy wyważyć z prawem do poszanowania życia prywatnego oraz ochrony danych, jest wolność sztuki i nauki, której przyznano w wyraźny sposób ochronę na mocy art. 13 Karty praw podstawowych UE. Prawo to wynika przede wszystkim z prawa do wolności myśli i wypowiedzi oraz powinno być wykonywane z poszanowaniem art. 1 karty (godność człowieka). Zdaniem ETPC wolność sztuki jest chroniona na mocy art. 10 EKPC[120]. Prawo zagwarantowane

119 Ogólne rozporządzenie o ochronie danych, art. 91 ust. 2.

120 ETPC, *Müller i in. przeciwko Węgrom*, nr 10737/84, 24 maja 1988 r.

w art. 13 karty może także podlegać ograniczeniom dopuszczalnym zgodnie z art. 52 ust. 1 karty, który można także interpretować w świetle art. 10 ust. 2 EKPC[121].

Przykład: W sprawie *Vereinigung bildender Künstler przeciwko Austrii*[122] sądy austriackie zakazały skarżącemu stowarzyszeniu dalszego wystawiania obrazu, który zawierał zdjęcia głów różnych osób publicznych, dopasowanych do ciał w pozycjach seksualnych. Austriacki parlamentarzysta, którego zdjęcie wykorzystano w obrazie, wystąpił z powództwem przeciwko skarżącemu stowarzyszeniu, wnioskując o sądowy zakaz wystawiania obrazu. Sąd krajowy wydał nakaz zgodnie z jego wnioskiem. Europejski Trybunał Praw Człowieka podkreślił, że art. 10 EKPC ma zastosowanie do przekazywania idei, które obrażają, szokują lub niepokoją państwo bądź dowolną część ludności. Osoby tworzące, wykonujące, rozpowszechniające lub wystawiające dzieła sztuki wnoszą wkład w wymianę idei i opinii, a państwo ma obowiązek nie naruszać w nadmierny sposób ich wolności wypowiedzi. Ze względu na fakt, że obraz stanowił kolaż i wykorzystywał zdjęcia wyłącznie głów przedstawionych osób, a ich ciała zostały namalowane w nierealistycznej i przesadzonej manierze, która w oczywisty sposób nie miała na celu odzwierciedlenia rzeczywistości, a nawet jej zasugerowania, ETPC stwierdził ponadto, iż „obrazu nie można interpretować jako przedstawienia szczegółów życia prywatnego [przedstawionego], dotyczy on natomiast jego roli publicznej jako polityka" oraz „w tym charakterze [przedstawiony] musi wykazywać większą tolerancję na krytykę". Wyważając różne interesy w tej sprawie, ETPC stwierdził, że nieograniczony zakaz dalszego wystawiania obrazu jest nieproporcjonalny. Trybunał orzekł zatem, że doszło do naruszenia art. 10 EKPC.

Europejskie prawo o ochronie danych także uznaje szczególną wartość nauki dla społeczeństwa. Ogólne rozporządzenie o ochronie danych i zaktualizowana konwencja nr 108 umożliwiają przechowywanie danych przez dłuższy okres, o ile dane osobowe będą przetwarzane wyłącznie do celów badań naukowych lub historycznych. Ponadto, bez względu na pierwotny cel konkretnej czynności przetwarzania, dalsze wykorzystywanie danych osobowych do badań naukowych nie

121 Wyjaśnienia dotyczące europejskiej Karty praw podstawowych, Dz.U. C 303 z 14.12.2007.

122 ETPC, *Vereinigung bildender Künstler przeciwko Austrii*, nr 68354/01, 25 stycznia 2007 r., pkt 26 i 34.

jest uznawane za cel niezgodny[123]. Jednocześnie należy wdrożyć odpowiednie gwarancje w odniesieniu do takiego przetwarzania, aby chronić prawa i wolności osób, których dane dotyczą. Prawo UE lub państwa członkowskiego może przewidywać wyjątki od praw osoby, której dane dotyczą, takie jak na przykład prawo dostępu do danych, ich poprawiania, ograniczenia przetwarzania oraz prawo do sprzeciwu w odniesieniu do przetwarzania jej danych osobowych do celów badań naukowych, historycznych lub statystycznych (zob. również sekcje 6.1 i 9.4).

1.3.5. Ochrona własności intelektualnej

Prawo do ochrony własności zapisano w art. 1 pierwszego protokołu do EKPC, a także w art. 17 ust. 1 Karty praw podstawowych UE. Ważnym aspektem prawa własności jest ochrona własności intelektualnej, o której wspomniano wprost w art. 17 ust. 2 karty. Do porządku prawnego UE należy kilka dyrektyw, których celem jest skuteczna ochrona własności intelektualnej, w szczególności praw autorskich. Własność intelektualna obejmuje nie tylko własność literacką i artystyczną, lecz także prawa patentowe, prawa do znaku towarowego i prawa pokrewne.

Jak jasno wynika z orzecznictwa TSUE, ochronę podstawowego prawa własności należy wyważyć z ochroną innych praw podstawowych, w szczególności prawa do ochrony danych[124]. Zdarzały się przypadki, w których instytucje ochrony praw autorskich żądały od dostawców dostępu do Internetu ujawnienia tożsamości użytkowników internetowych platform wymiany plików. Platformy takie często umożliwiają użytkownikom Internetu bezpłatne pobieranie utworów muzycznych, mimo że są one chronione prawem autorskim.

Przykład: Sprawa *Promusicae przeciwko Telefónica de España*[125] dotyczyła odmowy ze strony hiszpańskiego dostawcy usług dostępu do Internetu w przedmiocie ujawnienia Promusicae, niekomercyjnej organizacji producentów muzycznych oraz wydawców nagrań muzycznych i audiowizualnych, danych osobowych niektórych osób, którym podmiot ten świadczył usługi dostępu do Internetu. Promusicae wnioskowała o ujawnienie tych informacji, aby móc wszcząć postępowanie cywilne przeciwko tym

123 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. b) i zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. b).

124 TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 29 stycznia 2008 r., pkt 62–68.

125 Tamże, pkt 54 i 60.

osobom, które jej zdaniem korzystały z programu wymiany plików dającego dostęp do nagrań, do których majątkowe prawa autorskie należały do podmiotów będących członkami Promusicae.

Sąd hiszpański zwrócił się do TSUE z pytaniem, czy takie dane osobowe muszą zostać przekazane, zgodnie z prawem wspólnotowym, w ramach postępowania cywilnego w celu zapewnienia skutecznej ochrony praw autorskich. Sąd ten odwołał się przy tym do dyrektyw 2000/31/WE, 2001/29/WE i 2004/48/WE, interpretowanych również w świetle art. 17 i 47 karty. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że trzy wymienione dyrektywy, jak również dyrektywa o prywatności i łączności elektronicznej (2002/58/WE), nie wykluczają ustanowienia przez państwa członkowskie obowiązku ujawnienia danych osobowych w ramach postępowania cywilnego w celu zapewnienia skutecznej ochrony praw autorskich.

Trybunał wskazał, że sprawa dotyczy w związku z tym zagadnienia koniecznego pogodzenia wymogów związanych z ochroną poszczególnych praw podstawowych, a mianowicie z jednej strony prawa do poszanowania życia prywatnego, a z drugiej strony prawa do ochrony własności i prawa do skutecznego środka prawnego.

Trybunał stwierdził, że „przy transpozycji wyżej wskazanych dyrektyw na państwach członkowskich spoczywa obowiązek oparcia się na takiej wykładni tych dyrektyw, która pozwoli na zapewnienie odpowiedniej równowagi między poszczególnymi prawami podstawowymi chronionymi przez wspólnotowy porządek prawny. Następnie przy przyjmowaniu środków mających na celu transpozycję tych dyrektyw, władze i sądy państw członkowskich są zobowiązane nie tylko dokonywać wykładni ich prawa krajowego w sposób zgodny ze wspomnianymi dyrektywami, lecz również nie opierać się na takiej wykładni tych dyrektyw, która pozostawałaby w konflikcie z wspomnianymi prawami podstawowymi lub z innymi ogólnymi zasadami prawa wspólnotowego, takimi jak zasada proporcjonalności”[126].

126 Tamże, pkt 65 i 68; zob. także TSUE, C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV*, 16 lutego 2012 r.

Przykład: Sprawa *Bonnier Audio AB i in. przeciwko Perfect Communication Sweden AB*[127] dotyczyła wyważenia praw własności intelektualnej z ochroną danych osobowych. Skarżący – pięć wydawnictw posiadających prawa autorskie do 27 audiobooków – wnieśli do sądu szwedzkiego powództwo, zarzucając naruszenie tych praw autorskich za pomocą serwera FTP („file transfer protocol" – protokołu transferu plików umożliwiającego udostępnianie plików i przesyłanie danych przez Internet). Skarżący zwrócili się do dostawcy usług internetowych o ujawnienie nazwiska i adresu osoby korzystającej z adresu IP, z którego przesłano pliki. Dostawca usług internetowych (ePhone) zakwestionował wniosek, twierdząc, że naruszył on dyrektywę 2006/24 (dyrektywę w sprawie zatrzymywania danych – unieważnioną w 2014 r.).

Sąd szwedzki zwrócił się do TSUE z pytaniem, czy dyrektywa 2006/24 sprzeciwia się stosowaniu przepisu krajowego opartego na art. 8 dyrektywy 2004/48 (dyrektywy w sprawie egzekwowania praw własności intelektualnej), który zezwala nakazać dostawcy usług internetowych ujawnienie uprawnionemu z prawa autorskiego informacji o abonencie, któremu przyznano adres IP służący do naruszenia tego prawa. Pytanie to opierało się na założeniu, że skarżąca przedstawiła wyraźne dowody wskazujące na naruszenie konkretnego prawa autorskiego oraz że środek jest proporcjonalny.

Trybunał Sprawiedliwości wskazał, że dyrektywa 2006/24 dotyczyła wyłącznie przetwarzania i przechowywania danych generowanych przez dostawców usług łączności elektronicznej dla celów dochodzenia, wykrywania i ścigania poważnych przestępstw, jak również w celu ich przekazywania właściwym organom krajowym. W związku z tym przepis krajowy transponujący dyrektywę w sprawie egzekwowania praw własności intelektualnej nie jest objęty zakresem stosowania dyrektywy 2006/24 i w związku z tym nie jest przez nią wyłączony[128].

Co się tyczy przekazania spornego nazwiska i adresu, którego domagały się skarżące, TSUE orzekł, że tego rodzaju działanie stanowi przetwarzanie danych osobowych i podlega zastosowaniu dyrektywy 2002/58 (dyrektywy

127 TSUE, C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB przeciwko Perfect Communication Sweden AB*, 19 kwietnia 2012 r.

128 Tamże, pkt 40–41.

o e-prywatności). Trybunał zauważył ponadto, że ujawnienie tych danych było wymagane w ramach postępowania cywilnego, na rzecz uprawnionego z prawa autorskiego w celu zapewnienia skutecznej ochrony prawa autorskiego, a zatem, z uwagi na samą swoją istotę, także jest objęte zakresem dyrektywy 2004/48[129].

Trybunał stanął na stanowisku, że dyrektywy 2002/58 i 2004/48 należy interpretować w ten sposób, że nie sprzeciwiają się one przepisowi krajowemu, takiemu jak sporny przepis w postępowaniu głównym, ponieważ przepis ten zezwala sądowi krajowemu, do którego skierowano wniosek o wydanie nakazu ujawnienia danych osobowych, na wyważenie przeciwstawnych interesów, stosownie do okoliczności każdego przypadku oraz przy należytym uwzględnieniu wymogów wynikających z zasady proporcjonalności.

1.3.6. Ochrona danych a interesy gospodarcze

W erze cyfrowej lub epoce dużych zbiorów danych (Big Data) dane określa się mianem „nowej ropy naftowej" gospodarki jako pobudzające innowacyjność i kreatywność[130]. Wiele przedsiębiorstw stworzyło solidne modele biznesowe w zakresie przetwarzania danych, a takie przetwarzanie często wiąże się z przetwarzaniem danych osobowych. Niektóre przedsiębiorstwa mogą uważać, że szczegółowe przepisy dotyczące ochrony danych osobowych mogą w praktyce skutkować nadmiernie uciążliwymi obowiązkami, które mogą mieć wpływ na ich interesy gospodarcze. Pojawia się zatem pytanie, czy interesy gospodarcze administratorów i podmiotów przetwarzających lub ogółu społeczeństwa mogłyby uzasadniać ograniczenie prawa do ochrony danych.

Przykład: W sprawie *Google Spain*[131] TSUE uznał, że pod pewnymi warunkami osoby fizyczne mają prawo zwrócić się do operatorów wyszukiwarek internetowych o usunięcie wyników wyszukiwania ze swojego indeksu wyszukiwania. W swoim toku rozumowania TSUE zwrócił uwagę na fakt,

129 Tamże, pkt 52–54. Zob. także TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 29 stycznia 2008 r., pkt 58.

130 Zob. na przykład *Financial Times* (2016), „Data is the new oil... who's going to own it?", 16 listopada 2016 r.

131 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r.

że korzystanie z wyszukiwarek i wymienionych wyników wyszukiwania może spowodować ustalenie szczegółowego profilu danej osoby. Informacje te mogą dotyczyć rozległego aspektu życia prywatnego danej osoby i nie mogłyby być łatwo odnalezione lub powiązane bez wyszukiwarki. Stanowiło to zatem potencjalnie poważną ingerencję w podstawowe prawa osób, których dane dotyczą, do prywatności i ochrony danych osobowych.

Trybunał zbadał następnie, czy ingerencja mogła być uzasadniona. Co się tyczy interesu gospodarczego operatora wyszukiwarki internetowej w związku z prowadzeniem przetwarzania TSUE stwierdził, że „jasne jest, że [ingerencja] nie może być uzasadniona jedynie interesem, jaki ma w tym przetwarzaniu danych operator wyszukiwarki internetowej" oraz że „co do zasady" prawa podstawowe, które przysługują na podstawie art. 7 i 8 karty są nadrzędne wobec tego interesu gospodarczego oraz wobec interesu, jaki ten krąg odbiorców może mieć w znalezieniu rzeczonej informacji w ramach wyszukiwania prowadzonego w przedmiocie imienia i nazwiska tej osoby[132].

Jednym z kluczowych aspektów europejskiego prawa ochrony danych jest zapewnienie osobom fizycznym większej kontroli nad ich danymi osobowymi. Szczególnie w erze cyfrowej istnieje nierównowaga między władzą podmiotów gospodarczych przetwarzających i mających dostęp do ogromnych ilości danych osobowych a władzą osób fizycznych, do których należą te dane osobowe, do kontrolowania ich informacji. Trybunał Sprawiedliwości Unii Europejskiej przyjmuje indywidualne podejście do każdego przypadku, gdy chodzi o pogodzenie ochrony danych i interesów gospodarczych, takich jak interesy osób trzecich w odniesieniu do spółek akcyjnych i spółek z ograniczoną odpowiedzialnością, jak zostało to zilustrowane w wyroku w sprawie *Manni*.

Przykład: Sprawa *Manni*[133] dotyczyła włączenia danych osobowych osób fizycznych do publicznego rejestru handlowego. Pan Manni zwrócił się do izby handlowej w Lecce o usunięcie jego danych osobowych z tego rejestru, po tym jak dowiedział się, że potencjalni klienci mogliby zwrócić się do tego rejestru i zobaczyć, że był on administratorem spółki, której upadłość

132 Tamże, pkt 81 i 97.

133 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 9 marca 2017 r.

ogłoszono ponad dziesięć lat wcześniej. Informacje te wyrządziły szkodę jego potencjalnym klientom i mogłyby mieć negatywny wpływ na jego interesy handlowe.

Do TSUE zwrócono się w celu ustalenia, czy w prawie UE uznano prawo do usunięcia danych w tamtej sprawie. Dochodząc do wniosków, TSUE wyważył przepisy UE dotyczące ochrony danych oraz interes handlowy p. Manniego w usunięciu informacji o upadłości jego byłego przedsiębiorstwa z interesem publicznym w dostępie do tych informacji. Trybunał zwrócił należytą uwagę na fakt, że prawo, a w szczególności dyrektywa UE, której celem jest ułatwienie osobom trzecim dostępu do informacji o spółkach, przewiduje ich ujawnianie w rejestrze publicznym. Ujawnienie informacji było istotne dla ochrony interesów osób trzecich, które mogą chcieć prowadzić interesy z określoną spółką, ponieważ jedynymi zabezpieczeniami oferowanymi osobom trzecim przez spółki akcyjne i spółki z ograniczoną odpowiedzialnością są ich aktywa. Dlatego „podstawowe dokumenty spółki powinny być jawne, aby umożliwić osobom trzecim zapoznanie się z ich treścią oraz innymi informacjami dotyczącymi danej spółki, w szczególności z danymi osób, które są uprawnione do nabywania praw i zaciągania zobowiązań w jej imieniu”[134].

Ze względu na znaczenie słusznego celu, jaki realizuje rejestr, TSUE orzekł, że p. Manni nie był uprawniony do uzyskania usunięcia swoich danych osobowych, ponieważ konieczność ochrony interesów osób trzecich względem spółek akcyjnych i spółek z ograniczoną odpowiedzialnością oraz zapewnienia pewności prawa, uczciwości transakcji handlowych, a więc i sprawnego funkcjonowania rynku wewnętrznego była nadrzędna nad jego prawami przewidzianymi w przepisach o ochronie danych. Wynikało to w szczególności z faktu, że osoby fizyczne decydujące się na udział w obrocie za pośrednictwem spółki akcyjnej lub spółki z ograniczoną odpowiedzialnością są świadome, że są zobowiązane do ujawniania informacji dotyczących swojej tożsamości i funkcji.

Stwierdziwszy, że nie było podstaw do uzyskania usunięcia danych w tej sprawie, TSUE uznał istnienie prawa do wniesienia sprzeciwu wobec przetwarzania danych, zauważając że: „nie można wykluczyć ewentualności zaistnienia sytuacji szczególnych, w których przeważające i uzasadnione

134 Tamże, pkt 49.

względy dotyczące konkretnego przypadku osoby, której dotyczą dane, uzasadniają wyjątkowo, aby dostęp do figurujących w rejestrze danych osobowych dotyczących tej osoby został ograniczony, po upływie wystarczająco długiego okresu od daty likwidacji danej spółki, do kręgu osób trzecich mających konkretny, uzasadniony interes w uzyskaniu wglądu do tych danych”[135].

Trybunał stwierdził, że do sądów krajowych należy ustalenie w każdej sprawie, w oparciu o ocenę konkretnego przypadku, zaistnienia przeważających i uzasadnionych względów wyjątkowo uzasadniających ograniczenie dostępu osób trzecich do figurujących w rejestrze danych osobowych. Wyjaśnił on jednak, że w przypadku p. Manniego sam fakt, że ujawnienie jego danych osobowych w rejestrze rzekomo miało wpływ na jego klientelę, nie może zostać uznany za tak uzasadniony i przeważający powód. Potencjalni klienci p. Manniego mają uzasadniony interes w uzyskaniu informacji dotyczących upadłości jego poprzedniej spółki.

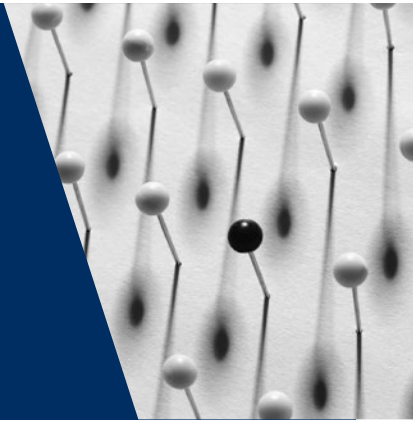
Naruszenie praw podstawowych p. Manniego i innych osób wpisanych do rejestru w zakresie poszanowania życia prywatnego i ochrony danych osobowych, zagwarantowanych w art. 7 i 8 karty, służyło interesowi ogólnemu oraz było konieczne i proporcjonalne.

W sprawie Manni TSUE orzekł zatem, że prawo do ochrony danych i prywatności nie ma pierwszeństwa względem osób trzecich w zakresie dostępu do informacji zawartych w rejestrze spółek w odniesieniu do spółek akcyjnych i spółek z ograniczoną odpowiedzialnością.

135 Tamże, pkt 60.

2

Terminologia związana z ochroną danych



UE	Omówione zagadnienia	RE
Dane osobowe		
Artykuł 4 ust. 1 ogólnego rozporządzenia o ochronie danych Artykuł 4 ust. 5 i Artykuł 5 ust. 1 lit. e) ogólnego rozporządzenia o ochronie danych Artykuł 9 ogólnego rozporządzenia o ochronie danych TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 2010 TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 2008 TSUE, C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 2011 TSUE, C-582/14, *Patrick Breyer przeciwko Bundesrepublik Deutschland*, 2016 TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 2014	Definicja prawna ochrony danych	Artykuł 2 lit. a) zaktualizowanej konwencji nr 108 ETPC, *Bernh Larsen Holding AS i in. przeciwko Norwegii*, nr 24117/08, 2013 ETPC, *Uzun przeciwko Niemcom*, nr 35623/05, 2010 ETPC, *Amann przeciwko Szwajcarii* [WI], nr 27798/95, 2000

UE	Omówione zagadnienia	RE
TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 2003	Szczególne kategorie danych osobowych (dane szczególnie chronione)	Artykuł 6 ust. 1 zaktualizowanej konwencji nr 108
TSUE, C-434/16, *Peter Nowak przeciwko Data Protection Commissioner*, 2017	Zanonimizowane i spseudo-nimizowane dane osobowe	Artykuł 5 ust. 4 lit. e) zaktualizowanej konwencji nr 108 Ust. 50 sprawozdania wyjaśniającego do zaktualizowanej konwencji nr 108
Przetwarzanie danych		
Artykuł 4 pkt 2 ogólnego rozporządzenia o ochronie danych TSUE, C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 2014 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 2017 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 2003 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 2014	Definicje	Artykuł 2 lit. b) i c) zaktualizowanej konwencji nr 108
Użytkownicy danych		
Artykuł 4 pkt 7 ogólnego rozporządzenia o ochronie danych TSUE, C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 2014 TSUE, C-1318/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 2014	Administrator	Artykuł 2 lit. d) zaktualizowanej konwencji nr 108 Artykuł 1 lit. g)* zalecenia w sprawie profilowania
Artykuł 4 pkt 8 ogólnego rozporządzenia o ochronie danych	Podmiot przetwarzający	Artykuł 2 lit. f) zaktualizowanej konwencji nr 108 Artykuł 1 lit. h) zalecenia w sprawie profilowania

UE	Omówione zagadnienia	RE
Artykuł 4 pkt 9 ogólnego rozporządzenia o ochronie danych	**Odbiorca**	Artykuł 2 lit. e) zaktualizowanej konwencji nr 108
Artykuł 4 pkt 10 ogólnego rozporządzenia o ochronie danych	**Strona trzecia**	
Zgoda		
Artykuł 4 pkt 11 i Artykuł 7 ogólnego rozporządzenia o ochronie danych TSUE, C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 2011 TSUE, C-536/15, *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*, 2017	**Definicja ważnej zgody i wymagania z nią związane**	Artykuł 5 ust. 2 zaktualizowanej konwencji nr 108 Artykuł 6 zalecenia dotyczącego danych medycznych i pewne późniejsze zalecenia ETPC, *Elberte przeciwko Łotwie*, nr 61243/08, 2015

** Rada Europy, Komitet Ministrów (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Profiling Recommendation), 23 listopada 2010 r.*

2.1. Dane osobowe

Najważniejsze kwestie

- Dane są danymi osobowymi, jeżeli odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby, czyli „osoby, której dane dotyczą".
- Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, administrator lub inna osoba musi wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej.
- Uwierzytelnienie oznacza udowodnienie, że dana osoba posiada pewną tożsamość lub jest uprawniona do wykonania pewnych czynności.
- Istnieją szczególne kategorie danych, tak zwane dane szczególnie chronione, wymienione w zaktualizowanej konwencji nr 108 i dyrektywie UE o ochronie danych, które wymagają zwiększonej ochrony i podlegają z tego powodu specjalnemu reżimowi prawnemu.
- Dane są zanonimizowane, jeżeli nie odnoszą się już do osoby zidentyfikowanej lub możliwej do zidentyfikowania.

- Pseudonimizacja jest środkiem, za pomocą którego dane osobowe nie mogą być przypisane osobie, której dane dotyczą, bez dodatkowych informacji, które są przechowywane oddzielnie. Klucz umożliwiający ponowną identyfikację osób, których dane dotyczą, musi być przechowywany oddzielnie i zabezpieczony. Dane, które zostały poddane procesowi pseudonimizacji, pozostają danymi osobowymi. W prawie UE nie istnieje pojęcie „danych spseudonimizowanych".
- Zasady i przepisy dotyczące ochrony danych nie mają zastosowania do informacji zanonimizowanych. Mają one jednak zastosowanie do danych spseudonimizowanych.

2.1.1. Podstawowe aspekty pojęcia danych osobowych

Zarówno **w prawie UE**, jak i **w prawie RE** „dane osobowe" definiuje się jako informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[136]. Obejmują one informacje o osobie, której tożsamość jest oczywista bądź przynajmniej może zostać ustalona przez uzyskanie dodatkowych informacji. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, administrator lub inna osoba musi wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej, co umożliwia odmienne traktowanie osób[137].

Jeżeli dane dotyczące takiej osoby są przetwarzane, osoba ta jest nazywana „osobą, której dane dotyczą".

Osoba, której dane dotyczą

Zgodnie z prawem UE osoby fizyczne są jedynymi beneficjentami przepisów o ochronie danych[138] i tylko osoby żyjące są chronione na mocy europejskiego prawa o ochronie danych[139]. Ogólne rozporządzenie o ochronie danych (RODO) definiuje dane osobowe jako informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.

136 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 1, zaktualizowana konwencja nr 108, art. 2 lit. a)

137 Ogólne rozporządzenie o ochronie danych, motyw 26

138 Tamże, art. 1.

139 Tamże, motyw 27. Zob. także Grupa Robocza Art. 29 (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 czerwca 2007 r., s. 22.

Prawo Rady Europy, w szczególności zaktualizowana konwencja nr 108, również odnosi się do ochrony osób fizycznych w zakresie przetwarzania ich danych osobowych. Również tam dane osobowe oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Ta osoba fizyczna, o której mowa odpowiednio w RODO i zaktualizowanej konwencji nr 108, jest znana w prawie o ochronie danych jako osoba, której dane dotyczą.

Pewną ochronę przyznaje się również osobom prawnym. Istnieje orzecznictwo dotyczące wyroków w sprawie wniosków osób prawnych dotyczących domniemanego naruszenia ich prawa do ochrony przed wykorzystywaniem ich danych na mocy art. 8 EKPC. Artykuł 8 EKPC obejmuje zarówno prawo do poszanowania życia prywatnego i rodzinnego, jak i prawo do mieszkania i korespondencji. Trybunał może zatem badać sprawy w ramach tego ostatniego aspektu, a nie w ramach życia prywatnego.

Przykład: Sprawa *Bernh Larsen Holding AS i in. przeciwko Norwegii*[140] dotyczyła skargi trzech norweskich przedsiębiorstw na decyzję organu podatkowego nakazującą im dostarczyć kontrolerom podatkowym kopię wszystkich danych przechowywanych na serwerze komputerowym wykorzystywanym wspólnie przez te trzy przedsiębiorstwa.

ETPC stwierdził, że taki obowiązek nałożony na skarżące przedsiębiorstwa stanowił ingerencję w ich prawa do poszanowania „mieszkania" oraz „korespondencji" w rozumieniu art. 8 EKPC. Trybunał stwierdził jednak, że organy podatkowe ustanowiły skuteczne i odpowiednie zabezpieczenia przed nadużyciami: skarżące przedsiębiorstwa zostały zawiadomione ze znacznym wyprzedzeniem; były obecne i mogły składać oświadczenia w trakcie inspekcji na miejscu; oraz materiały miały zostać zniszczone po zakończeniu kontroli podatkowej. W takiej sytuacji zachowano należytą równowagę między prawem do poszanowania „mieszkania" oraz „korespondencji" skarżących przedsiębiorstw i ich interesem związanym z ochroną prywatności pracujących dla nich osób z jednej strony, a interesem publicznym związanym z zapewnieniem efektywnej kontroli w celu określenia wymiaru podatku z drugiej strony. Trybunał stwierdził, że nie doszło zatem do naruszenia art. 8.

140 ETPC, *Bernh Larsen Holding AS i in. przeciwko Norwegii*, nr 24117/08, 14 marca 2013 r. Zob. jednak także ETPC, *Liberty i in. przeciwko Zjednoczonemu Królestwu*, nr 58243/00, 1 lipca 2008 r.

Zgodnie ze zaktualizowaną konwencją nr 108 ochrona danych dotyczy przede wszystkim ochrony osób fizycznych, jednak umawiające się strony mogą rozszerzyć w swoim prawie krajowym ochronę danych na osoby prawne, takie jak przedsiębiorstwa i stowarzyszenia. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji stwierdzono, że prawo krajowe może chronić uzasadnione interesy osób prawnych poprzez rozszerzenie zakresu konwencji na takie podmioty[141]. **Unijne prawo o ochronie danych** nie obejmuje przetwarzania danych, które dotyczą osób prawnych, a w szczególności nie dotyczy przedsiębiorstw prowadzących działalność jako osoby prawne, w tym nazwy oraz formy osoby prawnej i jej danych kontaktowych[142]. Dyrektywa o prywatności i łączności elektronicznej chroni jednak poufność komunikacji i uzasadnione interesy osób prawnych, w szczególności w odniesieniu do zwiększonej pojemności automatycznego przechowywania i przetwarzania danych odnoszących się do abonentów i użytkowników[143]. Podobnie projekt rozporządzenia w sprawie prywatności i łączności elektronicznej rozszerza ochronę na osoby prawne.

Przykład: W sprawie *Volker und Markus Schecke i Hartmut Eifert przeciwko Land Hessen*[144] TSUE, odnosząc się do publikacji danych osobowych dotyczących beneficjentów pomocy rolnej, stwierdził, że „osoby prawne mogą się powoływać na ochronę art. 7 i 8 karty w odniesieniu do takiej identyfikacji tylko wtedy, gdy nazwa oficjalna osoby prawnej identyfikuje jedną lub więcej osób fizycznych. [...] Poszanowanie życia prywatnego w kontekście przetwarzania danych osobowych, uznane w art. 7 i 8 karty, odnosi się do wszelkich informacji dotyczących zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej [...]"[145].

Wyważając interes UE, jakim jest zapewnienie przejrzystości w przyznawaniu pomocy z jednej strony oraz podstawowe prawa do prywatności i ochrony danych osób, które skorzystały z pomocy z drugiej strony, TSUE uznał, że ingerencja w te prawa podstawowe była nieproporcjonalna. Trybunał uznał, że cel w zakresie przejrzystości można było skutecznie osiągnąć za pomocą środków, które w mniejszym stopniu naruszają prawa zainteresowanych

141 Explanatory Report of Modernised Convention 108, pkt 30.

142 Ogólne rozporządzenie o ochronie danych, motyw 14.

143 Dyrektywa o prywatności i łączności elektronicznej, motyw 7 i art. 1 ust. 2

144 TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r., pkt 53.

145 Tamże, pkt 52–53.

osób fizycznych. Jednakże badając proporcjonalność publikowania informacji dotyczących osób prawnych, które otrzymały pomoc, TSUE doszedł do innego wniosku, orzekając, że publikacja ta nie wykraczała poza granice wyznaczone przez zasadę proporcjonalności. Trybunał orzekł, że „waga naruszenia prawa do ochrony danych osobowych jest bowiem inna w przypadku osób prawnych i w przypadku osób fizycznych”[146]. Osoby prawne podlegały szerszemu obowiązkowi publikacji danych ich dotyczących. Trybunał uznał, że obowiązek zbadania przez organy krajowe, przed publikacją omawianych danych w odniesieniu do każdej osoby prawnej będącej beneficjentem pomocy, czy jej nazwa wskazuje osoby fizyczne, nakładałby na właściwe organy krajowe nadmierne obciążenie administracyjne. Przepisy wymagające uogólnionej publikacji danych dotyczących osób prawnych zachowywały więc właściwą równowagę przy uwzględnieniu występujących w danym przypadku interesów.

Charakter danych

Danymi osobowymi mogą być wszelkiego rodzaju informacje, które odnoszą się do zidentyfikowanej lub możliwej do zidentyfikowania osoby.

Przykład: Ocena pracownika dokonana przez przełożonego i przechowywana w aktach osobowych stanowi dane osobowe dotyczące pracownika. Jest tak, nawet jeżeli w części lub w całości zawiera ona osobiste opinie przełożonego, takie jak: „pracownik nie przykłada się do pracy”, nie zaś obiektywne fakty, takie jak: „pracownik był nieobecny w pracy przez pięć tygodni w ciągu ostatnich sześciu miesięcy”.

Dane osobowe obejmują informacje na temat życia prywatnego osoby, jak również informacje o jej życiu zawodowym lub publicznym.

W sprawie *Amann*[147] ETPC zinterpretował termin „dane osobowe” jako nieograniczający się do sfery prywatnej danej osoby. Znaczenie terminu „dane osobowe” jest także istotne z punktu widzenia RODO.

146 Tamże, pkt 87.

147 Zob. ETPC, *Amann przeciwko Szwajcarii*, nr 27798/95, 16 lutego 2000 r., pkt 65.

Przykład: W sprawie *Volker und Markus Schecke i Hartmut Eifert przeciwko Land Hessen*[148] TSUE stwierdził, że „[w] tym względzie nie ma znaczenia, że publikowane dane są związane z działalnością zawodową [...]. Europejski Trybunał Praw Człowieka orzekł w tym względzie w odniesieniu do wykładni art. 8 konwencji nr 108, że termin »życie prywatne« nie może być interpretowany w sposób zawężający oraz że »nic nie uzasadnia wyłączenia działalności zawodowej [...] z zakresu życia prywatnego«".

Przykład: W sprawach połączonych *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*[149] TSUE stwierdził, że analiza prawna zawarta w projekcie decyzji Departamentu Imigracji i Naturalizacji dotyczącej wniosków o wydanie dokumentów pobytowych nie stanowi sama w sobie danych osobowych, mimo że może takie dane zawierać.

Orzecznictwo ETPC dotyczące art. 8 EKPC potwierdza, że może być trudno całkowicie oddzielić sprawy życia prywatnego od spraw zawodowych[150].

Przykład: W sprawie *Bărbulescu przeciwko Rumunii*[151] skarżący został zwolniony z pracy za niezgodne z przepisami wewnętrznymi korzystanie z Internetu pracodawcy w godzinach pracy. Jego pracodawca monitorował jego komunikaty, a protokoły, które zawierały komunikaty o charakterze czysto prywatnym, były przedstawione w trakcie postępowania przed sądem krajowym. Uznając, że art. 8 miał zastosowanie, ETPC pozostawił otwartą kwestię, czy restrykcyjne przepisy pracodawcy pozostawiają skarżącemu uzasadnione oczekiwanie prywatności, ale w każdym razie uznał, że instrukcje pracodawcy nie mogą zredukować do zera prywatnego życia społecznego w miejscu pracy. Co do istoty, umawiające się państwa musiały dysponować szerokim zakresem uznania przy ocenie konieczności ustanowienia ram prawnych regulujących warunki, w jakich pracodawca może regulować niezawodową komunikację pracowników – w formie

148 TSUE, sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r., pkt 59.

149 TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 17 lipca 2014 r., pkt 39.

150 Zob. na przykład ETPC, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, 4 maja 2000 r., pkt 43; ETPC, *Niemietz przeciwko Niemcom*, nr 13710/88, 16 grudnia 1992 r., pkt 29.

151 ETPC, *Bărbulescu przeciwko Rumunii* [WI], nr 61496/08, 5 września 2017 r., pkt 121.

elektronicznej lub innej – w miejscu pracy. Władze krajowe musiały jednak dopilnować, aby wprowadzeniu przez pracodawcę środków monitorowania korespondencji i innych komunikatów, niezależnie od zakresu i czasu trwania takich środków, towarzyszyły odpowiednie i wystarczające zabezpieczenia przed nadużyciami. Proporcjonalność i gwarancje proceduralne przeciwko arbitralności miały zasadnicze znaczenie, a ETPC zidentyfikował szereg czynników, które były istotne w danych okolicznościach. Czynniki te obejmowały na przykład zakres monitorowania pracowników przez pracodawcę oraz stopień jego ingerencji w prywatność pracownika, konsekwencje dla pracownika oraz to, czy zapewniono odpowiednie zabezpieczenia. Ponadto organy krajowe musiały zapewnić pracownikowi, którego korespondencja była monitorowana, dostęp do środków odwoławczych przed właściwym organem sądowym w celu ustalenia, przynajmniej co do istoty, sposobu przestrzegania tych kryteriów oraz zgodności z prawem zaskarżonych środków. W tej sprawie ETPC stwierdził naruszenie art. 8, ponieważ władze krajowe nie zapewniły odpowiedniej ochrony prawa skarżącego do poszanowania jego życia prywatnego i korespondencji, a w konsekwencji nie zachowały odpowiedniej równowagi między wchodzącymi w grę interesami.

Zgodnie z prawem UE, jak również **z prawem RE** informacje zawierają dane dotyczące osoby, jeżeli:

- dzięki tej informacji osoba fizyczna zostaje zidentyfikowana lub jest możliwa do zidentyfikowania; lub

- osoba fizyczna, choć nie została zidentyfikowana, może zostać wyróżniona na podstawie tych informacji w sposób umożliwiający ustalenie, kim jest osoba, której dane dotyczą, poprzez przeprowadzenie dalszych badań.

Oba rodzaje informacji są chronione w ten sam sposób na mocy europejskiego prawa o ochronie danych. Bezpośrednia lub pośrednia identyfikowalność osób wymaga ciągłej oceny, w której należy „uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny”[152]. Europejski Trybunał Praw Człowieka wielokrotnie stwierdzał, że pojęcie „danych osobowych” w ramach EKPC jest takie samo jak w konwencji nr 108, w szczególności

152 Ogólne rozporządzenie o ochronie danych, motyw 26.

w odniesieniu do warunków odnoszących się do osób zidentyfikowanych lub możliwych do zidentyfikowania[153].

Ogólne rozporządzenie o ochronie danych stanowi, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą „można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej"[154]. Identyfikacja wymaga zatem elementów, które opisują osobę w taki sposób, że można ją odróżnić od innych osób i rozpoznać jako jednostkę. Imię i nazwisko osoby jest doskonałym przykładem takich elementów opisu i może bezpośrednio identyfikować osobę. W niektórych przypadkach inne atrybuty mogą mieć podobny skutek co imię i nazwisko, czyniąc daną osobę pośrednio możliwą do zidentyfikowania. Numer telefonu, numer ubezpieczenia społecznego i numer rejestracyjny pojazdu to przykłady informacji, które mogą umożliwić zidentyfikowanie danej osoby. Możliwe jest również wykorzystanie atrybutów – takich jak pliki komputerowe, pliki cookie i narzędzia nadzoru ruchu sieciowego – w celu wyodrębnienia poszczególnych osób poprzez określenie ich zachowań i nawyków. Jak wyjaśniono w opinii Grupy Roboczej Art. 29 „[n]awet bez pytania o imię i nazwisko oraz adres osoby można ją sklasyfikować na podstawie kryteriów społeczno-ekonomicznych, psychologicznych, filozoficznych lub innych i przypisać jej pewne decyzje, ponieważ punkt kontaktowy osoby (komputer) nie wymaga już ujawniania jej tożsamości w wąskim znaczeniu tego słowa"[155]. Definicja danych osobowych zarówno w ramach RE, jak i UE jest wystarczająco szeroka, aby objąć wszystkie możliwości identyfikacji (a zatem wszystkie stopnie identyfikowalności).

Przykład: W sprawie *Promusicae przeciwko Telefónica de España*[156] TSUE stwierdził, że „bezsporne jest, że żądane przez Promusicae przekazanie nazwisk i adresów określonych użytkowników programów wymiany plików będących przedmiotem postępowania przed sądem krajowym wiąże się z udostępnieniem danych osobowych, to znaczy informacji

153 Zob. ETPC, *Amann przeciwko Szwajcarii* [WI], nr 27798/95, 16 lutego 2000 r., pkt 65.

154 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 1.

155 Grupa Robocza Art. 29, *Opinion 4/2007 on the concept of personal data*, WP 136, 20 czerwca 2007 r., s. 15.

156 TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 29 stycznia 2008 r., pkt 45.

o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej – zgodnie z definicją zawartą w art. 2 lit. a) dyrektywy 95/46 [obecnie art. 4 pkt 1 RODO]. Tego rodzaju przekazanie informacji, które, jak twierdzi Promusicae i czego nie kwestionuje Telefónica, przechowuje Telefónica, stanowi przetwarzanie danych osobowych"[157].

Przykład: Sprawa *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*[158] dotyczyła odmowy wprowadzenia przez Scarlet systemu filtrowania połączeń elektronicznych dokonywanych za pomocą programów wymiany plików celem uniemożliwienia wymiany plików naruszającej prawa autorskie chronione przez SABAM, organizację reprezentującą autorów, kompozytorów i wydawców i zarządzającą ich prawami. Trybunał orzekł, że adresy IP użytkowników „stanowią chronione dane osobowe, jako że pozwalają na precyzyjną identyfikację tych użytkowników".

Jako że wiele nazwisk się powtarza, w celu ustalenia tożsamości osoby konieczne mogą być dodatkowe identyfikatory gwarantujące, że osoby tej nie mylimy z inną. Czasami może zaistnieć konieczność połączenia atrybutów bezpośrednich i pośrednich w celu zidentyfikowania osoby, której dotyczą informacje. Często używa się daty i miejsca urodzenia. Ponadto w niektórych krajach wprowadzono indywidualne numery w celu lepszego rozróżnienia między obywatelami. Przekazywane dane podatkowe[159], dane dotyczące osoby ubiegającej się o zezwolenie na pobyt zawarte w dokumencie administracyjnym[160] oraz dokumenty dotyczące stosunków bankowych i powierniczych[161] mogą stanowić dane osobowe. W erze technologii coraz ważniejszym środkiem identyfikacji osób stają się dane biometryczne, takie jak odciski palców, zdjęcia cyfrowe czy skany tęczówki, dane o lokalizacji i cechy aktywności w Internecie.

157 Poprzednia dyrektywa 95/46, art. 2 lit. b), obecnie ogólne rozporządzenie o ochronie danych, art. 4 pkt 2.

158 TSUE, C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 listopada 2011 r., pkt 51.

159 TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 1 października 2015 r.

160 TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* i *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 17 lipca 2014 r.

161 ETPC, *M.N. i in. przeciwko San Marino*, nr 28005/12, 7 lipca 2015 r.

Aby jednak zastosowanie znalazło europejskie prawo o ochronie danych, nie jest niezbędna rzeczywista identyfikacja osoby, której dane dotyczą; wystarczy, aby dana osoba była możliwa do zidentyfikowania. Osobę uważa się za możliwą do zidentyfikowania, jeżeli informacja zawiera elementy identyfikujące, które pozwalają na bezpośrednią lub pośrednią identyfikację tej osoby[162]. Zgodnie z motywem 26 RODO punkt odniesienia stanowi to, czy jest prawdopodobne, że środki umożliwiające w racjonalny sposób identyfikację będą dostępne i zostaną zastosowane przez przewidywanych użytkowników tych informacji; obejmuje to także odbiorców będących osobami trzecimi (zob. sekcja 2.3.2).

Przykład: Organ władzy lokalnej postanawia zgromadzić dane o samochodach przekraczających dopuszczalną prędkość na lokalnych ulicach. Fotografuje on samochody, automatycznie rejestrując czas i miejsce, w celu przekazania danych właściwemu organowi, który wystawia mandaty osobom nieprzestrzegającym ograniczeń prędkości. Osoba, której dane dotyczą, składa skargę, twierdząc, że na mocy prawa o ochronie danych władze lokalne nie mają podstaw prawnych do gromadzenia takich danych. Organ władzy lokalnej twierdzi, że nie gromadzi danych osobowych. Jego zdaniem tablice rejestracyjne zawierają dane o anonimowych osobach. Organ władzy lokalnej nie jest uprawniony do dostępu do ogólnego rejestru pojazdów w celu ustalenia tożsamości właściciela pojazdu lub kierowcy.

Rozumowanie takie nie jest zgodne z motywem 26 RODO. Ze względu na to, że oczywistym celem gromadzenia danych jest identyfikacja i ukaranie osób przekraczających prędkość, można przewidzieć, iż zostanie podjęta próba ich identyfikacji. Chociaż władze lokalne nie dysponują bezpośrednio środkami identyfikacji, przekażą dane właściwemu organowi, czyli policji, która posiada takie środki. W motywie 26 wyraźnie wskazano sytuację, w której można przewidzieć, że próbę identyfikacji danej osoby mogą podjąć dalsi odbiorcy danych niebędący ich bezpośrednimi użytkownikami. W świetle motywu 26 działania organu władzy lokalnej są równoznaczne z gromadzeniem danych na temat możliwych do zidentyfikowania osób, a zatem wymagają podstawy prawnej na mocy prawa o ochronie danych.

„Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę

162 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 1.

wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny"[163].

Przykład: W sprawie *Breyer przeciwko Bundesrepublik Deutschland*[164] przedmiotem rozważań TSUE było pojęcie pośredniej identyfikowalności osób, których dane dotyczą. Sprawa dotyczyła dynamicznych adresów IP, które zmieniają się za każdym razem, gdy nawiązywane jest nowe połączenie z Internetem. Na stronach internetowych prowadzonych przez niemieckie instytucje federalne zarejestrowano i przechowano dynamiczne adresy IP w celu zapobiegania atakom cybernetycznym i wszczynania, w razie potrzeby, postępowań karnych. Jedynie dostawca usług internetowych, z którego usług korzystał p. Breyer, dysponował dodatkowymi informacjami niezbędnymi do jego identyfikacji.

TSUE uznał, że dynamiczny adres IP, który dostawca internetowych usług medialnych rejestruje, gdy dana osoba wchodzi na udostępnioną publicznie witrynę internetową, stanowi dane osobowe, w przypadku gdy tylko osoba trzecia – w tym przypadku dostawca usług internetowych – posiada dodatkowe dane niezbędne do zidentyfikowania tej osoby[165]. Trybunał stwierdził, że „nie jest wymagane, by wszystkie informacje umożliwiające identyfikację osoby, której dane dotyczą, musiały znajdować się w rękach tylko jednej osoby", aby informacje te mogły stanowić dane osobowe. Użytkownicy dynamicznego adresu IP zarejestrowanego przez dostawcę usług internetowych mogą zostać zidentyfikowani w pewnych sytuacjach, na przykład w ramach postępowania karnego w przypadku ataku cybernetycznego, z pomocą innych osób[166]. Zdaniem TSUE, w sytuacji gdy dostawca „dysponuje [...] środkami prawnymi umożliwiającymi mu zidentyfikowanie osoby, której dane dotyczą, dzięki dodatkowym informacjom, jakimi dysponuje dostawca dostępu do Internetu dla tej osoby"

163 Tamże, motyw 26.

164 TSUE, C-582/14, *Patrick Breyer przeciwko Bundesrepublik Deutschland*, 19 października 2016 r., pkt 43.

165 Poprzednia dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, art. 2 lit. a).

166 TSUE, C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 listopada 2011 r., pkt 47–48.

stanowi to „sposób, który może, racjonalnie rzecz biorąc, zostać zastosowany w celu zidentyfikowania osoby, której dane dotyczą". W związku z tym dane te uznaje się za dane osobowe.

W prawie RE identyfikowalność jest rozumiana w podobny sposób. Podobny opis zawiera sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108: pojęcie „możliwy do zidentyfikowania" odnosi się nie tylko do tożsamości cywilnej lub prawnej jako takiej, ale także do tego, co może pozwolić na „zindywidualizowanie" lub wyodrębnienie jednej osoby spośród innych i w rezultacie potencjalnie potraktowanie jej w odmienny sposób. „Indywidualizacji" tej można by dokonać na przykład poprzez odwołanie się do niej w szczególności, lub do urządzenia lub kombinacji urządzeń (komputera, telefonu komórkowego, kamery, urządzenia do gier itp.) połączonych z numerem identyfikacyjnym, pseudonimem, danymi biometrycznymi lub genetycznymi, danymi dotyczącymi lokalizacji, adresem IP lub innym identyfikatorem[167]. Osoby nie uznaje się za „możliwą do zidentyfikowania", jeżeli jej identyfikacja wymaga nieuzasadnionego nakładu czasu, wysiłku lub środków. Tak jest na przykład w przypadku, gdy identyfikacja osoby, której dane dotyczą, wymagałaby nadmiernie złożonych, długich i kosztownych operacji. Nieuzasadniony nakład czasu, wysiłku lub środków należy oceniać indywidualnie dla każdego przypadku, z uwzględnieniem takich czynników, jak cel przetwarzania danych, koszty i korzyści identyfikacji, rodzaj administratora danych i zastosowana technologia[168].

W odniesieniu do formy, w jakiej dane osobowe są przechowywane lub wykorzystywane, należy zauważyć, że nie ma to znaczenia dla stosowania prawa o ochronie danych. Komunikacja pisemna lub ustna może zawierać dane osobowe, jak również obrazy[169], w tym nagrania[170] lub dźwięk[171] z telewizji przemysłowej (CCTV). Danymi osobowymi mogą być również informacje zapisywane elektronicznie oraz w formie papierowej. Nawet próbki komórkowe tkanek ludzkich – które rejestrują DNA

167 Explanatory Report of Modernised Convention108, pkt 18.

168 Tamże, pkt 17.

169 ETPC, *Von Hannover przeciwko Niemcom*, nr 59320/00, 24 czerwca 2004 r.; ETPC, *Sciacca przeciwko Włochom*, nr 50774/99, 11 stycznia 2005 r.; TSUE, C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 11 grudnia 2014 r.

170 ETPC, *Peck przeciwko Zjednoczonemu Królestwu*, nr 44647/98, 28 stycznia 2003 r.; ETPC, *Köpke przeciwko Niemcom* (postanowienie), nr 420/07, 5 października 2010 r.; EIOD (2010), *The EDPS video-surveillance guidelines*, 17 marca 2010 r.

171 ETPC, *P.G. i J.H. przeciwko Zjednoczonemu Królestwu*, nr 44787/98, 25 września 2001 r., pkt 59–60; ETPC, *Wisse przeciwko Francji*, nr 71611/01, 20 grudnia 2005 r. (francuska wersja językowa).

danej osoby – mogą być źródłami, z których można pobrać dane biometryczne[172], o ile dane te odnoszą się do odziedziczonych lub nabytych cech genetycznych danej osoby, dostarczają unikalnych informacji na temat jej zdrowia lub fizjologii oraz są wynikiem analizy próbki biologicznej pobranej od tej osoby[173].

Anonimizacja

Zgodnie z zasadą ograniczenia przechowywania danych zawartą zarówno w RODO, jak i w zaktualizowanej konwencji nr 108 (omówionej bardziej szczegółowo w rozdziale 3) dane muszą być przechowywane „w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane"[174]. W związku z tym dane musiałyby zostać usunięte lub zanonimizowane, gdyby administrator danych chciał je przechowywać po tym, jak przestały być potrzebne i nie służyły już pierwotnemu celowi.

Proces anonimizacji danych oznacza, że wszystkie elementy identyfikacyjne są eliminowane z zestawu danych osobowych, tak że osoba, której dane dotyczą, nie może być już zidentyfikowana[175]. W swojej opinii 05/2014 Grupa Robocza Art. 29 analizuje skuteczność i ograniczenia różnych technik anonimizacji[176]. Uznaje ona potencjalną wartość takich technik, ale podkreśla się, że niektóre z nich niekoniecznie sprawdzają się we wszystkich przypadkach. Aby znaleźć optymalne rozwiązanie w danej sytuacji, należy indywidualnie dla każdego przypadku podjąć decyzję o odpowiednim procesie anonimizacji. Bez względu na zastosowaną technikę, identyfikacji należy zapobiec w sposób nieodwracalny. Oznacza to, że w celu zachowania anonimowości danych nie można pozostawić żadnych elementów informacji, które przy dołożeniu należytej staranności mogłyby posłużyć do ponownego zidentyfikowania danej osoby lub danych osób[177]. Ryzyko ponownej identyfikacji można ocenić, biorąc pod uwagę „czas, wysiłek lub zasoby potrzebne w świetle charakteru

172 Zob. Grupa Robocza Art. 29 (2007), *Opinion 4/2007 on the concept of personal data*, WP 136, 20 czerwca 2007 r., s. 9; Rada Europy, Recommendation No. Rec (2006) 4 of the Committee of Ministers to member states on research on biological materials of human origin, 15 marca 2006 r.

173 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 13.

174 Tamże, art. 5 ust. 1 lit. e); zaktualizowana konwencja nr 108, Art. 5 ust. 4 lit. e).

175 Ogólne rozporządzenie o ochronie danych, motyw 26.

176 Grupa Robocza Art. 29 (2014), *Opinion 05/2014 on Anonymization Techniques*, WP 216, 10 kwietnia 2014 r.

177 Ogólne rozporządzenie o ochronie danych, motyw 26.

danych, kontekstu ich wykorzystania, dostępnych technologii ponownej identyfikacji i związanych z tym kosztów”[178].

Dane, które zostały skutecznie zanonimizowane, nie są już danymi osobowymi i nie mają już do nich zastosowania przepisy o ochronie danych.

Ogólne rozporządzenie o ochronie danych przewiduje, że na osobę lub organizację kontrolującą przetwarzanie danych osobowych nie można nakładać obowiązku zachowania, uzyskania ani przetwarzania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do tego rozporządzenia. Można jednak wskazać istotny wyjątek od tej zasady: w każdym przypadku, gdy osoba, której dane dotyczą, w celu skorzystania z prawa do dostępu, poprawienia, usunięcia, ograniczenia przetwarzania i możliwości przenoszenia danych, przekazuje administratorowi danych dodatkowe informacje umożliwiające jej identyfikację, wówczas te dane, które zostały uprzednio zanonimizowane, stają się ponownie danymi osobowymi[179].

Pseudonimizacja

Dane osobowe zawierają identyfikatory, takie jak nazwisko, data urodzenia, płeć i adres, jak również inne elementy, które mogą prowadzić do identyfikacji. Podczas pseudonimizacji danych osobowych identyfikatory te zostają zastąpione pseudonimem.

Zgodnie z definicją zawartą w **prawie UE** „pseudonimizacja” oznacza „przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”[180]. W przeciwieństwie do danych zanonimizowanych, dane spseudonimizowane nadal są danymi osobowymi i w związku z tym podlegają przepisom o ochronie danych. Chociaż pseudonimizacja może zmniejszyć zagrożenia dla bezpieczeństwa osób, których dane dotyczą, nie jest ona wyłączona z zakresu RODO.

178 Rada Europy, Committee of Convention 108 (2017), *Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data*, 23 stycznia 2017 r., pkt 6.2.

179 Ogólne rozporządzenie o ochronie danych, art. 11.

180 Tamże, art. 4 pkt 5.

W RODO uznano szereg zastosowań pseudonimizacji jako odpowiedniego środka technicznego dla wzmocnienia ochrony danych i jest on wyraźnie wymieniony w celu zaprojektowania i zabezpieczenia przetwarzania danych[181]. Jest to również właściwe zabezpieczenie, które może być wykorzystane do przetwarzania danych osobowych do celów innych niż te, do których zostały pierwotnie zgromadzone[182].

Dane spseudonimizowane nie zostały wymienione wprost w definicjach prawnych zawartych w zaktualizowanej konwencji nr 108 **RE.** Jednakże w sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 stwierdza się, że „użycie pseudonimu lub jakiegokolwiek identyfikatora cyfrowego/tożsamości cyfrowej nie prowadzi do anonimizacji danych, ponieważ osoba, której dane dotyczą, może być nadal zidentyfikowana lub zindywidualizowana"[183]. Jednym ze sposobów pseudonimizacji danych jest ich szyfrowanie. W chwili dokonania pseudonimizacji powstaje związek z tożsamością w postaci pseudonimu wraz z kluczem do odszyfrowania. Bez takiego klucza trudno jest zidentyfikować dane spseudonimizowane. Osoby uprawnione do użycia klucza do odszyfrowania mogą jednak łatwo dokonać ponownej identyfikacji. Należy w szczególności zapobiec użyciu kluczy do szyfrowania przez osoby nieuprawnione. Wobec tego „[d]ane spseudonimizowane uznaje się za dane osobowe [...]" objęte zakresem zaktualizowanej konwencji nr 108[184].

Uwierzytelnienie

Jest to procedura, dzięki której dana osoba jest w stanie udowodnić, że posiada pewną tożsamość lub jest uprawniona do wykonania pewnych czynności, takich jak wejście do strefy bezpieczeństwa bądź wypłata środków z konta bankowego. Uwierzytelnienia można dokonać za pomocą porównania danych biometrycznych, takich jak fotografia lub odciski palców w paszporcie, z danymi osoby zgłaszającej się np. do kontroli imigracyjnej[185], lub prosząc o informacje, które powinny być znane tylko osobie o pewnej tożsamości lub pewnych uprawnieniach, takie jak osobisty numer identyfikacyjny (kod PIN) bądź hasło; lub żądając przedstawienia pewnego przedmiotu, który powinna posiadać wyłącznie osoba o pewnej tożsamości lub pewnych uprawnieniach, takiego jak specjalna karta chipowa bądź klucz do skrytki bankowej. Oprócz haseł lub kart chipowych, czasem wykorzystywanych w połączeniu z kodem

181 Tamże, art. 25 ust. 1.

182 Tamże, art. 6 ust. 4.

183 Explanatory Report of the Modernised Convention 108, pkt 18.

184 Tamże.

185 Tamże, pkt 56–57.

PIN, narzędziem szczególnie przydatnym przy identyfikacji i uwierzytelnianiu osób w komunikacji elektronicznej są podpisy elektroniczne.

2.1.2. Szczególne kategorie danych osobowych

Zarówno **w prawie UE**, jak i **w prawodawstwie RE** istnieją szczególne kategorie danych osobowych, które ze swojej natury mogą stanowić podczas przetwarzania zagrożenie dla osób, których dane dotyczą, i wymagają zwiększonej ochrony. Dane takie podlegają zasadzie zakazu i istnieje ograniczona liczba warunków, pod jakimi takie przetwarzanie jest zgodne z prawem.

Jeżeli chodzi o definicję danych szczególnie chronionych, zarówno w zaktualizowanej konwencji nr 108 (art. 6), jak i w RODO (art. 9) wymienia się następujące kategorie:

- dane osobowe ujawniające pochodzenie rasowe lub etniczne;
- dane osobowe ujawniające poglądy polityczne, przekonania religijne lub inne, w tym światopoglądowe;
- dane osobowe ujawniające przynależność do związków zawodowych;
- dane genetyczne i dane biometryczne przetwarzane w celu zidentyfikowania osoby;
- dane osobowe dotyczące zdrowia, seksualności lub orientacji seksualnej.

Przykład: Sprawa *Bodil Lindqvist*[186] dotyczyła odniesienia na stronie internetowej do różnych osób imiennie lub za pomocą innych środków, takich jak numer telefonu lub informacja o ich hobby. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że „informacja, iż dana osoba doznała urazu stopy i przebywa na zwolnieniu lekarskim w niepełnym wymiarze, stanowi dane osobowe dotyczące zdrowia"[187].

186 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r., pkt 51.

187 Poprzednia dyrektywa 95/46, art. 8 ust. 1, obecnie ogólne rozporządzenie o ochronie danych, art. 9 ust. 1.

Dane osobowe dotyczące wyroków skazujących i naruszeń prawa

Zaktualizowana konwencja nr 108 włącza dane osobowe odnoszące się do przestępstw, postępowań karnych i wyroków skazujących oraz związanych z nimi środków bezpieczeństwa do wykazu szczególnych kategorii danych osobowych[188]. W ramach RODO dane osobowe odnoszące się do wyroków skazujących i naruszeń prawa lub związanych z nimi środków bezpieczeństwa nie są jako takie wymieniane w wykazie szczególnych kategorii danych, ale są przedmiotem osobnego artykułu. Artykuł 10 RODO stanowi, że przetwarzania takich danych wolno dokonywać wyłącznie „pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą". Z drugiej strony, kompleksowe rejestry zawierające informacje o wyrokach skazujących mogą być prowadzone wyłącznie pod kontrolą określonych władz publicznych[189]. W UE przetwarzanie danych osobowych w kontekście egzekwowania prawa reguluje konkretny akt prawny, mianowicie dyrektywa (UE) 2016/680[190]. Dyrektywa określa szczegółowe zasady ochrony danych, które są wiążące dla właściwych organów, gdy przetwarzają one dane do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych (zob. sekcja 8.2.1).

2.2. Przetwarzanie danych

Najważniejsze kwestie

- „Przetwarzanie danych" dotyczy wszelkich operacji wykonywanych na danych osobowych.
- Pojęcie „przetwarzania" obejmuje przetwarzanie w sposób zautomatyzowany i niezautomatyzowany.

188 Zaktualizowana konwencja nr 108, art. 6 ust. 1

189 Ogólne rozporządzenie o ochronie danych, art. 10.

190 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych, 2008/977/JHA, Dz.U. L 119 z 4.5.2016.

- W prawie UE „przetwarzanie" odnosi się także do ręcznego przetwarzania zorganizowanych zbiorów.
- W prawie RE znaczenie terminu „przetwarzanie" można rozszerzyć prawem krajowym na przetwarzanie ręczne.

2.2.1. Pojęcie przetwarzania danych

Pojęcie przetwarzania danych osobowych w **prawie UE** i **prawie RE** ma charakter kompleksowy: „»Przetwarzanie danych osobowych« [...] oznacza operację [...] taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie"[191] danych osobowych. Zaktualizowana konwencja nr 108 dodaje do tej definicji zatrzymywanie danych osobowych[192].

Przykład: W sprawie *František Ryneš*[193] p. Ryneš, dzięki zainstalowanemu przez niego domowemu monitoringowi kamer przemysłowych służących ochronie jego własności zarejestrował obraz dwóch osób, które wybiły okna w jego domu. Trybunał Sprawiedliwości Unii Europejskiej ustalił, że nadzór kamer wideo polegający na rejestracji i przechowywaniu danych osobowych stanowi zautomatyzowane przetwarzanie danych osobowych objęte zakresem prawa UE dotyczącego ochrony danych.

Przykład: W sprawie *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*[194] p. Manni wniósł o usunięcie jego danych osobowych z rejestru spółki ratingowej, który wiązał go z likwidacją przedsiębiorstwa zajmującego się obrotem nieruchomościami, a tym samym miało negatywny wpływ na jego reputację. Trybunał Sprawiedliwości Unii Europejskiej orzekł, że „poprzez wpisywanie i przechowywanie owych informacji w rejestrze, a także ujawnianie ich,

191 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 2. Zob. także zaktualizowana konwencja nr 108, art. 2 lit. b)

192 Zaktualizowana konwencja nr 108, art. 2 lit. b).

193 TSUE, C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 11 grudnia 2014 r., pkt 25.

194 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 9 marca 2017 r., pkt 35.

w stosownym wypadku, na wniosek osób trzecich, organ odpowiedzialny za prowadzenie tego rejestru »przetwarza dane osobowe«, w odniesieniu do których jest »administratorem«".

Przykład: Pracodawcy gromadzą i przetwarzają dane o swoich pracownikach, w tym informacje dotyczące ich wynagrodzeń. Ich umowy o pracę stanowią dla nich podstawę prawną do dokonania tego zgodnie z prawem.

Pracodawcy będą musieli przekazywać dane dotyczące wynagrodzeń swoich pracowników organom podatkowym. To przekazywanie danych będzie również „przetwarzaniem" w rozumieniu tego terminu w zaktualizowanej konwencji nr 108 i w RODO. Podstawą prawną takiego ujawnienia nie są jednak umowy o pracę. Musi istnieć dodatkowa podstawa prawna dla operacji przetwarzania danych, które prowadzą do przekazywania przez pracodawcę danych o wynagrodzeniach organom podatkowym. Tę podstawę prawną można zazwyczaj znaleźć w przepisach krajowego prawa podatkowego. Bez takich przepisów – i przy braku jakiejkolwiek innej uzasadnionej podstawy przetwarzania – takie przekazywanie danych osobowych byłoby przetwarzaniem niezgodnym z prawem.

2.2.2. Zautomatyzowane przetwarzanie danych

Ochrona danych na mocy zaktualizowanej konwencji nr 108 i RODO ma w pełni zastosowanie do zautomatyzowanego przetwarzania danych.

Zgodnie z **prawem UE** zautomatyzowane przetwarzanie danych dotyczy operacji przeprowadzanych na „danych osobowych w sposób całkowicie lub częściowo zautomatyzowany"[195]. Zaktualizowana konwencja nr 108 zawiera podobną definicję[196]. W praktyce oznacza to, że wszelkie dane osobowe przetwarzane w sposób zautomatyzowany, na przykład przy pomocy komputera osobistego, urządzenia przenośnego lub routera, podlegają zarówno przepisom UE, jak i przepisom RE dotyczącym ochrony danych.

195 Ogólne rozporządzenie o ochronie danych, art. 2 ust. 1 lit. h) i art. 4 pkt 2.

196 Zaktualizowana konwencja nr 108, art. 2 lit. b) i c), Explanatory Report of Modernised Convention 108, pkt 21.

Przykład: Sprawa *Bodil Lindqvist*[197] dotyczyła odniesienia na stronie internetowej do różnych osób imiennie lub za pomocą innych środków, takich jak numer telefonu lub informacja o ich hobby. Trybunał Sprawiedliwości Unii Europejskiej orzekł, że „operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków, np. numeru telefonu lub informacji dotyczących ich warunków pracy i sposobów spędzania przez nie wolnego czasu stanowi »przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany« w rozumieniu art. 3 ust. 1 dyrektywy 95/46"[198].

Przykład: W sprawie *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi*[199] p. González zwrócił się o usunięcie lub zmianę linku między jego nazwiskiem w wyszukiwarce Google a dwiema stronami gazet ogłaszającymi aukcję nieruchomości w celu odzyskania długów z tytułu ubezpieczeń społecznych. Trybunał Sprawiedliwości Unii Europejskiej stwierdził, że „operator wyszukiwarki internetowej, przeszukując Internet w zautomatyzowany, stały i systematyczny sposób w poszukiwaniu opublikowanych w nim informacji, »gromadzi« takie dane, które są »odzyskiwane«, »zapisywane« i »porządkowane« przezeń następnie za pomocą oprogramowania indeksującego, »przechowuje« je na swych serwerach oraz, w odpowiednim przypadku, »ujawnia« i »udostępnia« je swym użytkownikom w postaci listy wyników ich wyszukiwań"[200]. Trybunał stwierdził, że tego rodzaju działania stanowią „przetwarzanie" i „bez znaczenia jest przy tym fakt, iż ten operator wyszukiwarki internetowej przeprowadza te same operacje również w odniesieniu do innego rodzaju informacji i nie wprowadza rozróżnienia między nimi a tymi danymi osobowymi".

2.2.3. Niezautomatyzowane przetwarzanie danych

Ręczne przetwarzanie danych również wymaga ochrony danych.

197 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r., pkt 27.

198 Ogólne rozporządzenie o ochronie danych, art. 2 ust. 1.

199 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r.

200 Tamże, pkt 28.

Ochrona danych na mocy **prawa UE** nie ogranicza się w żaden sposób do zautomatyzowanego przetwarzania danych. W związku z tym na mocy prawa UE ochrona danych ma zastosowanie do przetwarzania danych osobowych w zbiorze ręcznym, czyli zorganizowanym zbiorze w postaci papierowej[201]. Zorganizowany zbiór danych to taki, który klasyfikuje zbiór danych osobowych, czyniąc je dostępnymi według określonych kryteriów. Na przykład, jeżeli pracodawca prowadzi zbiór danych w formie papierowej zatytułowany „urlopy pracownicze", który zawiera wszystkie szczegóły urlopów udzielonych pracownikom w ubiegłym roku i jest uporządkowany alfabetycznie, zbiór ten będzie stanowił ręczny zbiór danych podlegający przepisom UE w zakresie ochrony danych. Powód tego rozszerzenia ochrony danych jest następujący:

- zbiory w postaci papierowej można zorganizować w sposób, który czyni znajdowanie informacji szybkim i łatwym;

- przechowywanie danych osobowych w zorganizowanych zbiorach w postaci papierowej ułatwia obejście określonych w przepisach ograniczeń dotyczących automatycznego przetwarzania danych[202].

Zgodnie z **prawem RE** w definicji automatycznego przetwarzania uznaje się, że niektóre etapy ręcznego wykorzystywania danych osobowych mogą być wymagane między zautomatyzowanymi operacjami[203]. Artykuł 2 lit. c) zaktualizowanej konwencji nr 108 stanowi, że „w przypadku gdy nie stosuje się automatycznego przetwarzania, przetwarzanie danych oznacza operację lub zestaw operacji dokonywanych na danych osobowych w ramach zorganizowanego zestawu takich danych, który jest dostępny lub może być pobrany według określonych kryteriów".

2.3. Użytkownicy danych osobowych

Najważniejsze kwestie

- Każdy, kto ustala sposoby i cele przetwarzania danych osobowych innych osób jest „administratorem" na mocy prawa o ochronie danych; jeżeli taką decyzję podejmuje większa liczba osób wspólnie, mogą one być „współadministratorami".

201 Ogólne rozporządzenie o ochronie danych, art. 2 ust. 1.

202 Ogólne rozporządzenie o ochronie danych, motyw 15.

203 Zaktualizowana konwencja nr 108, art. 2 lit. b) i c).

- „Podmiot przetwarzający" to osoba fizyczna lub prawna, która przetwarza dane osobowe w imieniu administratora.
- Podmiot przetwarzający staje się administratorem, jeżeli ustala sposoby i cele samego przetwarzania danych.
- Osoba, której ujawnia się dane osobowe, jest „odbiorcą".
- „Strona trzecia" oznacza osobę fizyczną lub prawną inną niż osoba, której dane dotyczą, administrator danych, podmiot przetwarzający dane i osoby, które są upoważnione do przetwarzania danych osobowych z upoważnienia administratora danych lub podmiotu przetwarzającego dane.
- Zgoda jako podstawa prawna przetwarzania danych osobowych musi być wyrażona w sposób dobrowolny, świadomy, konkretny i jednoznaczny, w formie wyraźnego działania potwierdzającego zgodę na przetwarzanie danych.
- Przetwarzanie szczególnych kategorii danych na podstawie zgody wymaga wyraźnej zgody.

2.3.1. Administratorzy i podmioty przetwarzające

Najważniejszą konsekwencją bycia administratorem lub podmiotem przetwarzającym jest odpowiedzialność prawna za przestrzeganie odpowiednich obowiązków na mocy prawa o ochronie danych. W sektorze prywatnym są to zazwyczaj osoby fizyczne lub prawne; w sektorze publicznym są to zazwyczaj organy. Istnieje znaczne rozróżnienie między administratorem danych a podmiotem przetwarzającym: pierwszy z tych podmiotów to osoba fizyczna lub prawna, która ustala cele i sposoby przetwarzania, natomiast drugi to osoba fizyczna lub prawna, która przetwarza dane w imieniu administratora danych zgodnie ze ścisłymi instrukcjami. Zasadniczo to administrator danych musi sprawować kontrolę nad przetwarzaniem i ponosi za nie odpowiedzialność, w tym odpowiedzialność prawną. Jednak wraz z reformą przepisów dotyczących ochrony danych podmioty przetwarzające są obecnie zobowiązane do przestrzegania wielu wymogów, które mają zastosowanie do administratorów danych. Na przykład zgodnie z RODO podmioty przetwarzające prowadzą rejestr czynności przetwarzania danych osobowych, aby wykazać zgodność z ciążącymi na nich obowiązkami określonymi w rozporządzeniu[204]. Podmioty przetwarzające są również zobowiązane do wdrożenia odpowiednich środków technicznych i organizacyjnych w celu zapewnienia bezpieczeństwa przetwarzania[205], do

204 Ogólne rozporządzenie o ochronie danych, art. 30 ust. 2.

205 Tamże, art. 32.

wyznaczenia w określonych sytuacjach inspektora ochrony danych[206] oraz do zgłaszania naruszeń ochrony danych administratorowi[207].

To, czy dana osoba ma zdolność do decydowania w zakresie oraz ustalania celu i środków przetwarzania, będzie zależeć od stanu faktycznego lub okoliczności danej sprawy. Zgodnie z definicją administratora danych zawartą w RODO administratorem danych może być osoba fizyczna, osoba prawna lub inne organy. Grupa Robocza Art. 29 podkreśliła jednak, że aby zapewnić osobom fizycznym bardziej stabilny podmiot do celów wykonywania ich praw „za administratora należy raczej uznać spółkę lub sam organ niż konkretną osobę w ramach spółki lub organu"[208]. Na przykład, administratorem danych, który sporządza i prowadzi listę dystrybucyjną wszystkich lekarzy w danym obszarze, jest spółka sprzedająca wyroby medyczne lekarzom, a nie kierownik sprzedaży, który faktycznie korzysta z tej listy i ją prowadzi.

Przykład: Gdy dział marketingu spółki Sunshine zamierza przetwarzać dane na potrzeby badania rynku, administratorem w przypadku takiego przetwarzania jest spółka Sunshine, nie zaś dział marketingu. Dział marketingu nie może być administratorem, gdyż nie posiada odrębnej osobowości prawnej.

Osoby fizyczne mogą być administratorami danych zarówno na gruncie prawa UE, jak i prawa RE. Jednakże w sytuacji gdy przetwarzanie danych dotyczących innych osób odbywa się w ramach działalności czysto osobistej lub domowej, osoby fizyczne nie są objęte zakresem przepisów RODO i zaktualizowanej konwencji nr 108 i nie uznaje się ich za administratorów[209]. Osoba, która prowadzi korespondencję, osobisty dziennik opisujący zdarzenia z udziałem przyjaciół i współpracowników oraz dokumentację zdrowotną członków rodziny, może być zwolniony z przepisów o ochronie danych, ponieważ takie czynności mogą być działalnością czysto osobistą lub domową. Ogólne rozporządzenie o ochronie danych stanowi ponadto, że działalność osobista lub domowa może również polegać na podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej

206 Tamże, art. 37.

207 Tamże, art. 33 ust. 2.

208 Zob. także Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concept of personal data*, WP 169, Bruksela, 16 lutego 2010 r.

209 Ogólne rozporządzenie o ochronie danych, motyw 18, art. 2 ust. 2 lit. c), zaktualizowana konwencja nr 108, art. 3 ust. 2.

działalności[210]. Przepisy o ochronie danych mają natomiast pełne zastosowanie do administratorów i podmiotów przetwarzających, którzy zapewniają środki do przetwarzania danych osobowych na potrzeby działalności osobistej lub domowej (na przykład platformy społecznościowe)[211].

Dostęp obywateli do Internetu oraz możliwość korzystania z platform handlu elektronicznego, portali społecznościowych i stron blogowych w celu dzielenia się informacjami o sobie i o innych osobach sprawiają, że coraz trudniej jest oddzielić przetwarzanie danych osobowych od przetwarzania danych nieosobowych[212]. To, czy jest to działalność czysto osobista czy domowa, zależy od okoliczności[213]. Działalność o charakterze zawodowym lub handlowym nie może być objęta zwolnieniem dla działalności domowej[214]. W związku z tym, jeżeli skala i częstotliwość przetwarzania danych wskazuje na działalność zawodową lub pracę w pełnym wymiarze godzin, osobę fizyczną można uznać za administratora danych. Poza zawodowym lub handlowym charakterem działalności związanej z przetwarzaniem danych, kolejnym czynnikiem, który należy wziąć pod uwagę, jest to, czy dane osobowe są udostępniane dużej liczbie osób, w sposób oczywisty znajdujących się poza sferą prywatną danej osoby. W orzecznictwie związanym z dyrektywą o ochronie danych wykształcił się jednak pogląd, że prawo o ochronie danych znajduje niemniej zastosowanie, gdy osoba prywatna publikuje dane na temat innych osób na publicznej stronie internetowej. Trybunał Sprawiedliwości Unii Europejskiej nie miał jak dotąd sposobności orzekania w przedmiocie podobnych okoliczności faktycznych w świetle RODO, które zawiera więcej wskazówek dotyczących tematów, które można rozpatrywać poza zakresem przepisów o ochronie danych w ramach „wyjątku dotyczącego działalności domowej", takich jak wykorzystanie mediów społecznościowych do celów osobistych.

Przykład: Sprawa *Bodil Lindqvist*[215] dotyczyła odniesienia na stronie internetowej do różnych osób imiennie lub za pomocą innych środków, takich jak numer telefonu lub informacja o ich hobby. Trybunał Sprawiedliwości

210 Ogólne rozporządzenie o ochronie danych, motyw 18.

211 Tamże, motyw 18; Explanatory Report of Modernised Convention 108, pkt 29.

212 Zob. oświadczenie Grupy Roboczej Art. 29 w przedmiocie dyskusji nad pakietem reform dotyczących ochrony danych (2013), *Annex 2: Proposals and Amendments regarding exemption for personal or household activities*, 27 lutego 2013 r.

213 Explanatory Report of Modernised Convention 108, pkt 28.

214 Zob. ogólne rozporządzenie o ochronie danych, motyw 18 oraz Explanatory Report of Modernised Convention 108, pkt 27.

215 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r.

stwierdził, że „operacja polegająca na zamieszczeniu na stronie internetowej danych różnych osób pozwalających je zidentyfikować za pomocą nazwiska albo innych środków [...] stanowi »przetwarzanie danych osobowych w całości lub w części w sposób zautomatyzowany« w rozumieniu art. 3 ust. 1 dyrektywy 95/46/WE o ochronie danych"[216].

Takie przetwarzanie danych osobowych nie wchodzi w zakres czynności o czysto osobistym lub domowym charakterze, których nie dotyczą unijne przepisy o ochronie danych, gdyż takie wyłączenie „powinno być interpretowane jako obejmujące wyłącznie działania wchodzące w zakres życia prywatnego lub rodzinnego jednostki, co w sposób oczywisty nie ma miejsca w przypadku przetwarzania danych osobowych polegającego na ich opublikowaniu w Internecie w taki sposób, że staną się one dostępne dla nieograniczonej liczby osób"[217].

Według TSUE w pewnych okolicznościach zapisy wizualne z prywatnie zainstalowanej kamery bezpieczeństwa mogą być również objęte przepisami UE dotyczącymi ochrony danych.

Przykład: W sprawie *František Ryneš*[218] p. Ryneš, dzięki zainstalowanemu przez niego domowemu monitoringowi kamer przemysłowych służących ochronie jego własności zarejestrował obraz dwóch osób, które wybiły okna w jego domu. Nagranie zostało następnie przekazane policji i wykorzystane w postępowaniu karnym.

Trybunał stwierdził, że „o ile nadzór kamer wideo, taki jak ten w postępowaniu głównym, rozciąga się choćby częściowo na przestrzeń publiczną i tym samym jest skierowany poza sferę prywatną osoby dokonującej w ten sposób przetwarzania danych, o tyle nie powinien on być rozumiany jako czynność o czysto »osobistym lub domowym charakterze« [...]"[219].

216 Tamże, pkt 27, poprzednia dyrektywa 95/46/WE, art. 3 ust. 1, obecnie ogólne rozporządzenie o ochronie danych, art. 2 ust. 1.

217 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r., pkt 47.

218 TSUE, C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 11 grudnia 2014 r., pkt 33.

219 Poprzednia dyrektywa 95/46/WE, art. 3 ust. 2 tiret drugie, obecnie ogólne rozporządzenie o ochronie danych, art. 2 ust. 2 lit. c).

Administrator

W prawie UE administrator oznacza podmiot, który „samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych”[220]. Administrator decyduje o tym, dlaczego i w jaki sposób będą przetwarzane dane.

W prawie RE zaktualizowana konwencja nr 108 definiuje „administratora danych” jako „osobę fizyczną lub prawną, władzę publiczną, służbę, agencję lub każdy inny organ, który samodzielnie lub wspólnie z innymi posiada uprawnienia decyzyjne w odniesieniu do przetwarzania danych”[221]. Takie uprawnienia decyzyjne dotyczą celów i sposobów przetwarzania, jak również kategorii przetwarzanych danych i dostępu do nich[222]. Decyzja o tym, czy uprawnienie znajduje swoją podstawę w przepisach prawa, czy też wynika z okoliczności faktycznych, musi być podejmowana indywidualnie dla każdego przypadku[223].

Przykład: Sprawa *Google Spain*[224] dotyczyła powództwa wytoczonego przez obywatela Hiszpanii, który chciał usunąć z Google stary artykuł prasowy na temat swojej sytuacji finansowej.

Do TSUE zwrócono się z pytaniem, czy Google, jako operator wyszukiwarki, jest „administratorem” w rozumieniu art. 2 lit. d) dyrektywy o ochronie danych[225]. Trybunał rozważył szeroką definicję pojęcia „administratora danych”, celem zapewnienia „skutecznej i pełnej ochrony osobom, których dotyczą dane”[226]. Trybunał Sprawiedliwości stwierdził, że operator wyszukiwarki internetowej określa cele i sposoby prowadzenia tej działalności oraz udostępnia dane zamieszczone na stronach internetowych

220 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 7.

221 Zaktualizowana konwencja nr 108, art. 2 lit. d).

222 Explanatory Report of Modernised Convention 108, pkt 22.

223 Tamże.

224 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r.

225 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 7; TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 21.

226 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 34.

przez wydawców stron internetowych każdemu internaucie, który wyszukuje dane na podstawie nazwiska osoby, której dane dotyczą[227]. Trybunał stwierdził zatem, że Google można uznać za „administratora"[228].

W sytuacji gdy administrator lub podmiot przetwarzający nie mają jednostki organizacyjnej w Unii, spółka ta na piśmie wyznacza swojego przedstawiciela w Unii[229]. W RODO podkreśla się, że przedstawiciel musi mieć siedzibę „w państwie członkowskim, w którym przebywają osoby, których dane dotyczą, których dane osobowe są przetwarzane w związku z oferowaniem im towarów lub usług lub których zachowanie jest monitorowane"[230]. Brak ustanowienia przedstawiciela nie ogranicza prawa do wszczęcia postępowania przeciwko samemu administratorowi lub podmiotowi przetwarzającemu[231].

Współadministrowanie

Ogólne rozporządzenie o ochronie danych przewiduje, że jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. Oznacza to, że w drodze obopólnych uzgodnień decydują się oni przetwarzać dane we wspólnym celu[232]. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 stwierdza się, że istnienie wielu administratorów danych lub współadministrowania możliwe jest również **w ramach prawa RE**[233].

Grupa Robocza Art. 29 zwraca uwagę, że współadministrowanie może przybierać różne formy i że udział różnych administratorów w działaniach kontrolnych może być nierówny[234]. Elastyczność ta umożliwia uwzględnienie coraz bardziej złożonych realiów przetwarzania danych[235]. Współadministratorzy muszą zatem określić

227 Tamże, pkt 35–40.

228 Tamże, pkt 41.

229 Ogólne rozporządzenie o ochronie danych, art. 27 ust. 1.

230 Tamże, art. 27 ust. 3.

231 Tamże, art. 27 ust. 5.

232 Tamże, art. 4 pkt 7 i art. 26.

233 Zaktualizowana konwencja nr 108, art. 2 lit. d), Explanatory Report of Modernised Convention 108, pkt 22.

234 Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Bruksela, 16 lutego 2010 r., s. 19.

235 Tamże.

w konkretnej umowie swoje obowiązki w zakresie wypełniania obowiązków wynikających z rozporządzenia[236].

Współadministrowanie prowadzi do wspólnej odpowiedzialności za przetwarzanie danych[237]. W ramach **prawa UE** oznacza to, że każdy administrator lub podmiot przetwarzający może zostać pociągnięty do pełnej odpowiedzialności za całość szkód spowodowanych przez przetwarzanie w ramach współadministrowania w celu zapewnienia, że osoba, której dane dotyczą, otrzyma skuteczne odszkodowanie[238].

Przykład: Częstym przykładem współadministrowania jest prowadzona wspólnie przez większą liczbę instytucji kredytowych baza danych klientów niewykonujących zobowiązań. Gdy osoba ubiega się o linię kredytową w banku, który jest jednym ze współadministratorów, banki sprawdzają bazę danych, która pomaga im w podejmowaniu świadomych decyzji o zdolności kredytowej wnioskodawcy.

W przepisach nie stwierdza się wyraźnie, czy w celu współadministrowania wymagane jest, aby wspólny cel był taki sam w przypadku każdego z administratorów, czy też wystarczy, aby ich cele pokrywały się tylko częściowo. Nie istnieje jednak jeszcze stosowne orzecznictwo na szczeblu europejskim. W opinii z 2010 r. w sprawie administratorów i podmiotów przetwarzających Grupa Robocza Art. 29 stwierdza, że współadministratorzy mogą mieć wspólne cele i sposoby przetwarzania lub też mogą mieć wspólne tylko niektóre cele, sposoby lub ich część[239]. Pierwsza z tych sytuacji oznaczałaby bardzo bliskie relacje między różnymi podmiotami, natomiast druga wskazywałaby, że relacje te są luźniejsze.

Grupa Robocza Art. 29 opowiada się za szerszą interpretacją pojęcia współadministrowania, co ma zapewnić pewną elastyczność ze względu na rosnącą złożoność obecnych realiów w zakresie przetwarzania danych[240]. Stanowisko grupy roboczej obrazuje sprawa Stowarzyszenia na rzecz Światowej Międzybankowej Teletransmisji Danych Finansowych (SWIFT).

236 Ogólne rozporządzenie o ochronie danych, motyw 79.

237 Tamże, pkt 21.

238 Tamże, art. 82 ust. 4.

239 Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Bruksela, 16 lutego 2010 r., s. 19.

240 Tamże.

Przykład: W tak zwanej sprawie SWIFT europejskie instytucje bankowe wykorzystywały organizację SWIFT, początkowo jako podmiot przetwarzający, do przekazywania danych w trakcie transakcji bankowych. SWIFT ujawniał takie dane dotyczące transakcji bankowych, przechowywane w centrum przetwarzania danych w Stanach Zjednoczonych, Departamentowi Skarbu USA bez wyraźnego polecenia ze strony europejskich instytucji bankowych, które korzystały z jego usług. Oceniając zgodność z prawem tej sytuacji, Grupa Robocza Art. 29 doszła do wniosku, że europejskie instytucje bankowe wykorzystujące SWIFT, jak również samą organizację należy uznać za współadministratorów odpowiedzialnych wobec europejskich klientów za ujawnienie ich danych władzom USA[241].

Podmiot przetwarzający

Podmiot przetwarzający jest zdefiniowany **w prawie UE** jako podmiot, który przetwarza dane osobowe w imieniu administratora[242]. Czynności powierzone podmiotowi przetwarzającemu mogą ograniczać się do ściśle określonego zadania lub kontekstu bądź mogą być określone w sposób dość ogólny i szeroki.

W prawie RE znaczenie terminu „podmiot przetwarzający" jest takie samo jak w prawie UE[243].

Oprócz przetwarzania danych dla innych podmioty przetwarzające są także pełnoprawnymi administratorami danych w odniesieniu do czynności przetwarzania, które wykonują we własnych celach, np. zarządzania własnymi pracownikami, sprzedażą i klientami.

Przykład: Spółka Everready specjalizuje się w przetwarzaniu dla innych przedsiębiorstw danych związanych z zarządzaniem kadrami. W tej funkcji Everready pełni rolę podmiotu przetwarzającego. Gdy jednak Everready przetwarza dane własnych pracowników, staje się administratorem operacji przetwarzania danych w związku z wypełnianiem swoich obowiązków jako pracodawcy.

241 Grupa Robocza Art. 29 (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Bruksela, 22 listopada 2006 r.

242 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 8.

243 Zaktualizowana konwencja nr 108, art. 2 lit. f).

Relacja między administratorem a podmiotem przetwarzającym

Jak opisano wyżej, administratora definiuje się jako podmiot, który określa cele i sposoby przetwarzania. W RODO wyraźnie określono, że podmiot przetwarza dane osobowe wyłącznie na polecenie administratora, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego[244]. Umowa między administratorem a podmiotem przetwarzającym stanowi zasadniczy element ich relacji i jest wymogiem prawnym[245].

Przykład: Dyrektor Sunshine Company postanawia, że Cloudy Company, spółka specjalizująca się w przechowywaniu danych w chmurze, powinna zarządzać danymi klientów spółki Sunshine. Sunshine Company pozostaje administratorem danych, a Cloudy Company jest tylko podmiotem przetwarzającym dane, ponieważ zgodnie z umową Cloudy może wykorzystywać dane klientów Sunshine wyłącznie do celów określonych przez Sunshine.

W przypadku gdy uprawnienie do określenia sposobów przetwarzania zostaje przekazane podmiotowi przetwarzającemu, administrator musi niemniej mieć możliwość kontroli decyzji podmiotu przetwarzającego dotyczących sposobów przetwarzania. Ogólna odpowiedzialność nadal spoczywa na administratorze, który musi nadzorować podmioty przetwarzające w celu zapewnienia, by ich decyzje były zgodne z prawem o ochronie danych i z instrukcjami administratora.

Ponadto jeżeli podmiot przetwarzający nie stosuje się do określonych przez administratora warunków dotyczących wykorzystania danych, podmiot przetwarzający stanie się administratorem co najmniej w zakresie, w jakim postępuje niezgodnie z instrukcjami administratora. Najprawdopodobniej poskutkuje to tym, że podmiot przetwarzający stanie się działającym niezgodnie z prawem administratorem. Pierwotny administrator będzie musiał z kolei wyjaśnić, jak mogło dojść do tego, że podmiot przetwarzający przekroczył swoje uprawnienia[246]. W istocie Grupa Robocza Art. 29 zazwyczaj zakłada w takich przypadkach, że doszło do

244 Ogólne rozporządzenie o ochronie danych, art. 29.

245 Tamże, art. 28 ust. 3.

246 Tamże, art. 82 ust. 2.

współadministrowania, gdyż zapewnia to najlepszą ochronę interesów osób, których dane dotyczą[247].

Mogą również występować kwestie związane z podziałem odpowiedzialności, gdy administrator jest małym przedsiębiorstwem, a podmiot przetwarzający wielką korporacją, która jest w stanie dyktować warunki świadczonych usług. Grupa Robocza Art. 29 uważa jednak, że w takich okolicznościach nie należy obniżać standardów odpowiedzialności ze względu na nierównowagę ekonomiczną, a interpretacja pojęcia administratora powinna pozostać niezmienna[248].

Dla zapewnienia jasności i przejrzystości szczegóły relacji łączącej administratora z podmiotem przetwarzającym powinny zostać określone w pisemnej umowie[249]. Kontakt musi obejmować w szczególności przedmiot, charakter, cel i czas trwania przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą. Powinna ona również określać obowiązki i prawa administratora i podmiotu przetwarzającego, takie jak wymogi dotyczące poufności i bezpieczeństwa. Brak takiej umowy stanowi naruszenie obowiązku administratora w zakresie dostarczenia pisemnej dokumentacji dotyczącej wzajemnych obowiązków i może skutkować sankcjami. Nie tylko administrator, lecz także podmiot przetwarzający odpowiada za szkody spowodowane działaniem poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom[250]. Podmiot przetwarzający musi prowadzić rejestr wszystkich kategorii działań związanych z przetwarzaniem, które wykonuje w imieniu administratora danych[251]. Rejestr należy udostępnić na żądanie organu nadzorczego, ponieważ administrator i podmiot przetwarzający współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań[252]. Aby wykazać zgodność z wymogami RODO administratorzy i podmioty przetwarzające mają także możliwość stosowania się do zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji[253].

247 Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Bruksela, 16 lutego 2010 r., s. 25; Grupa Robocza Art. 29 (2006), *Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, WP 128, Bruksela, 22 listopada 2006 r.

248 Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concepts of "controller" and "processor"*, WP 169, Bruksela, 16 lutego 2010 r., s. 26.

249 Ogólne rozporządzenie o ochronie danych, art. 28 ust. 3 i 9.

250 Tamże, art. 82 ust. 2.

251 Tamże, art. 30 ust. 2.

252 Tamże, art. 30 ust. 4 i art. 31.

253 Tamże, art. 28 ust. 5 i art. 42 ust. 4.

Podmioty przetwarzające mogą chcieć przekazać niektóre zadania dodatkowym podmiotom podprzetwarzajacym. Jest to dopuszczalne prawnie, przy czym szczegóły zależą od uzgodnień umownych między administratorem i podmiotem przetwarzającym, między innymi od tego, czy w każdym przypadku konieczne jest upoważnienie ze strony administratora, czy też wystarcza samo zawiadomienie. Ogólne rozporządzenie o ochronie danych stanowi, że w przypadku gdy podmiot podprzetwarzający nie wywiąże się ze spoczywających na nim obowiązków w zakresie ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu podprzetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym[254].

W prawie RE powyższa interpretacja wyjaśnionych wyżej pojęć administratora i podmiotu przetwarzającego ma pełne zastosowanie[255].

2.3.2. Odbiorcy i strony trzecie

Różnica między tymi dwiema kategoriami osób lub podmiotów, które zdefiniowano w dyrektywie o ochronie danych, polega przede wszystkim na ich relacji z administratorem, a tym samym na ich uprawnieniach do dostępu do danych osobowych będących w posiadaniu administratora.

„Strona trzecia" to podmiot odrębny od administratora i podmiotu przetwarzającego. Zgodnie z art. 4 pkt 10 RODO strona trzecia oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe". Oznacza to, że osoby pracujące w organizacji, która jest podmiotem odrębnym od administratora, nawet jeżeli należy ona do tej samej grupy lub holdingu, są „stronami trzecimi" (lub należą do „strony trzeciej"). „Stronami trzecimi" nie są natomiast oddziały banku przetwarzające dane dotyczące rachunków klientów pod bezpośrednim zwierzchnictwem centrali[256].

„Odbiorca" jest pojęciem szerszym od „strony trzeciej". W rozumieniu art. 4 pkt 9 RODO odbiorca oznacza „osobę fizyczną lub prawną, organ publiczny, jednostkę

254 Tamże, art. 28 ust. 4.

255 Zob. na przykład zaktualizowana konwencja nr 108, art. 2 lit. b) i f); zalecenie w sprawie profilowania, art. 1.

256 Grupa Robocza Art. 29 (2010), *Opinion 1/2010 on the concept of "controller" and "processor"*, WP 169, Bruksela, 16 lutego 2010 r., s. 31.

lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią". Odbiorca może być zarówno osobą spoza podmiotu będącego administratorem lub podmiotem przetwarzającym – jest wówczas stroną trzecią – bądź osobą w obrębie podmiotu będącego administratorem lub podmiotem przetwarzającym, np. pracownikiem lub innym działem w ramach danego przedsiębiorstwa lub organu.

Rozróżnienie między odbiorcami a stronami trzecimi jest ważne tylko ze względu na warunki ujawnienia danych zgodnie z prawem. Pracownicy administratora lub podmiotu przetwarzającego mogą bez żadnych dalszych wymogów prawnych być odbiorcami danych osobowych, jeżeli uczestniczą w operacjach przetwarzania danych prowadzonych przez administratora lub podmiot przetwarzający. Z kolei strona trzecia, jako odrębna od administratora lub podmiotu przetwarzającego, nie jest upoważniona do wykorzystywania danych osobowych przetwarzanych przez administratora, chyba że w konkretnym przypadku istnieje stosowna podstawa prawna.

Przykład: Pracownik administratora, który wykorzystuje dane osobowe przy wykonywaniu zadań powierzonych mu przez pracodawcę, jest odbiorcą danych, ale nie stroną trzecią, gdyż wykorzystuje dane w imieniu administratora i zgodnie z jego instrukcjami. Na przykład, jeśli pracodawca ujawni dane osobowe swoich pracowników działowi kadr w związku ze zbliżającymi się ocenami wyników, to zespół działu kadr będzie odbiorcą danych osobowych, ponieważ dane te zostały im ujawnione w trakcie przetwarzania danych dla administratora.

Jeżeli jednak organizacja przekazuje dane dotyczące swoich pracowników firmie szkoleniowej, która wykorzysta je do dostosowania programu szkoleniowego do potrzeb pracowników, firma szkoleniowa jest stroną trzecią. Powodem jest fakt, że firma szkoleniowa nie posiada określonej legitymacji lub upoważnienia (co w przypadku „działu kadr" wynika ze stosunku pracy z administratorem danych) do przetwarzania tych danych osobowych. Innymi słowy, nie otrzymali tych informacji w trakcie zatrudnienia u administratora danych.

2.4. Zgoda

Najważniejsze kwestie

- Zgoda jako podstawa prawna przetwarzania danych osobowych musi być wyrażona w sposób dobrowolny, świadomy, konkretny i jednoznaczny, w formie wyraźnego działania potwierdzającego zgodę na przetwarzanie danych.
- Przetwarzanie szczególnych kategorii danych wymaga wyraźnej zgody.

Jak zostanie szczegółowo omówione w rozdziale 4, zgoda jest jedną z sześciu uzasadnionych podstaw przetwarzania danych osobowych. Zgoda oznacza dobrowolne, świadome, konkretne i jednoznaczne okazanie woli [osoby, której dane dotyczą][257].

W prawie UE wskazano kilka elementów ważnej zgody, które mają zagwarantować, że osoby, których dane dotyczą, rzeczywiście chciały wyrazić zgodę na wykorzystanie ich danych[258]:

- Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Czynność ta może przybrać formę działania lub oświadczenia.
- Zgoda może zostać odwołana przez osobę, której dane dotyczą, w każdej chwili.
- W kontekście pisemnego oświadczenia, które obejmuje również inne kwestie, takie jak „warunki świadczenia usług", wnioski o wyrażenie zgody muszą być sporządzone jasnym i prostym językiem oraz w zrozumiałej i łatwo dostępnej formie, która wyraźnie odróżnia zgodę od innych kwestii; jeżeli część tego oświadczenia narusza RODO, nie jest ono wiążące.

Zgoda będzie ważna w kontekście prawa o ochronie danych tylko wtedy, gdy wszystkie te wymogi zostaną spełnione. Obowiązkiem administratora jest

257 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 11. Zob. także zaktualizowana konwencja nr 108, art. 5 ust. 2.

258 Ogólne rozporządzenie o ochronie danych, art. 7.

wykazanie, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie jej danych[259]. Elementy ważnej zgody zostaną omówione szerzej w sekcji 4.1.1 dotyczącej zgodnych z prawem podstaw przetwarzania danych osobowych.

Konwencja nr 108 nie zawiera definicji zgody; jej określenie pozostawia się w gestii ustawodawcy krajowego. Jednak zgodnie z **prawem RE** elementy ważnej zgody odpowiadają tym, które wyjaśniono wcześniej[260].

Dodatkowe wymagania na mocy prawa cywilnego warunkujące ważność zgody, takie jak zdolność prawna, obowiązują oczywiście także w kontekście ochrony danych, gdyż są to podstawowe wstępne wymogi prawne. Nieważna zgoda wyrażona przez osoby, które nie mają zdolności prawnej, skutkuje brakiem podstawy prawnej przetwarzania danych na temat takich osób. Jeśli chodzi o zdolność prawną małoletnich do zawierania umów, RODO przewiduje, że przepisy rozporządzenia dotyczące minimalnego wieku, aby uzyskać ważną zgodę, nie mają wpływu na ogólne prawo umów państw członkowskich[261].

Zgoda musi być wyrażona w sposób jasny, tak aby nie pozostawić wątpliwości co do intencji osoby, której dane dotyczą[262]. Zgoda musi być wyraźna w przypadku przetwarzania danych szczególnie chronionych i może być wyrażona ustnie lub pisemnie[263]. Wyrażenie tej ostatniej może odbywać się za pomocą środków elektronicznych[264]. Zarówno w ramach **prawa UE**, jak i **prawa RE** zgoda na przetwarzanie danych osobowych musi być wyrażona w formie oświadczenia lub wyraźnego działania potwierdzającego[265]. Zgody nie można zatem uzyskać na podstawie milczenia, zaznaczonych z góry pól wyboru, wcześniej wypełnionych formularzy lub braku aktywności[266].

259 Tamże, art. 7 ust. 1.

260 Zaktualizowana konwencja nr 108, art. 5 ust. 2; Explanatory Report of Modernised Convention 108, pkt 42–53.

261 Ogólne rozporządzenie o ochronie danych, art. 8 ust. 3.

262 Tamże, art. 6 ust. 1 lit. a) i art. 9 ust. 2 lit. a).

263 Tamże, art. 32.

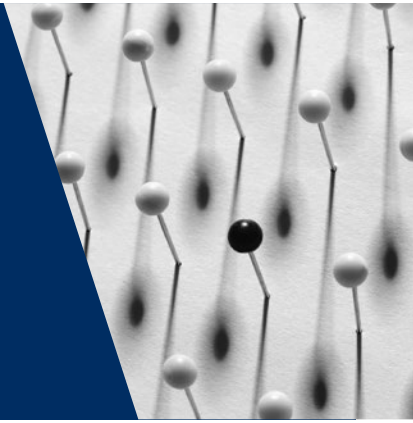
264 Tamże.

265 Tamże, art. 4 pkt 11, Explanatory Report of Modernised Convention 108, pkt 42.

266 Zaktualizowana konwencja nr 108, motyw 32; Explanatory Report of Modernised Convention 108, pkt 42.

3

Najważniejsze zasady europejskiego prawa o ochronie danych



UE	Omówione zagadnienia	RE
Artykuł 5 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych	Zasada zgodności z prawem	Artykuł 5 ust. 3 zaktualizowanej konwencji nr 108
Artykuł 5 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych	Zasada rzetelności	Artykuł 5 ust. 4 lit. a) zaktualizowanej konwencji nr 108 ETPC, *K.H. i in. przeciwko Słowacji*, nr 32881/04, 2009.
Artykuł 5 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 2015	Zasada przejrzystości	Artykuł 5 ust. 4 lit. a) i Artykuł 8 zaktualizowanej konwencji nr 108 ETPC, *Haralambie przeciwko Rumunii*, nr 21737/03, 2009
Artykuł 5 ust. 1 lit. b) ogólnego rozporządzenia o ochronie danych	Zasada ograniczenia celu	Artykuł 5 ust. 4 lit. b) zaktualizowanej konwencji nr 108
Artykuł 5 ust. 1 lit. c) ogólnego rozporządzenia o ochronie danych TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland* oraz *Kärntner Landesregierung i in.* [WI], 2014	Zasada minimalizacji danych	Artykuł 5 ust. 4 lit. c) zaktualizowanej konwencji nr 108

UE	Omówione zagadnienia	RE
Artykuł 5 ust. 1 lit. d) ogólnego rozporządzenia o ochronie danych TSUE, C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M.E.E. Rijkeboerowi*, 2009	**Zasada prawidłowości danych**	Artykuł 5 ust. 4 lit. d) zaktualizowanej konwencji nr 108
Artykuł 5 ust. 1 lit. e) ogólnego rozporządzenia o ochronie danych TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland* oraz *Kärntner Landesregierung i in.* [WI], 2014	**Zasada ograniczenia przechowywania**	Artykuł 5 ust. 4 lit. e) zaktualizowanej konwencji nr 108 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 2008
Artykuł 5 ust. 1 lit. f) i art. 32 ogólnego rozporządzenia o ochronie danych	**Zasada bezpieczeństwa danych (integralności i poufności)**	Artykuł 7 zaktualizowanej konwencji nr 108
Artykuł 5 ust. 2 ogólnego rozporządzenia o ochronie danych	**Zasada rozliczalności**	Artykuł 10 zaktualizowanej konwencji nr 108

W art. 5 ogólnego rozporządzenia o ochronie danych określono zasady regulujące przetwarzanie danych osobowych. Zasady te obejmują:

- zgodność z prawem, rzetelność i przejrzystość,
- ograniczenie celu,
- minimalizację danych,
- prawidłowość danych,
- ograniczenie przechowywania,
- integralność i poufność.

Zasady te stanowią punkt wyjścia dla bardziej szczegółowych przepisów w kolejnych artykułach rozporządzenia. Pojawiają się one również w art. 5, 7, 8 i 10 zaktualizowanej konwencji nr 108. Wszystkie późniejsze przepisy dotyczące ochrony danych na szczeblu RE lub UE muszą być zgodne z tymi zasadami i muszą być

interpretowane z uwzględnieniem tych zasad. Zgodnie z prawem UE ograniczenia zasad przetwarzania danych są dopuszczalne jedynie w zakresie, w jakim odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 oraz muszą szanować istotę podstawowych praw i wolności. Wszelkie wyjątki i ograniczenia od tych kluczowych zasad mogą być przewidziane na poziomie UE lub krajowym[267]; muszą one być przewidziane prawem, służyć zgodnemu z prawem celowi oraz być niezbędnymi i proporcjonalnymi środkami w demokratycznym społeczeństwie[268]. Wszystkie trzy warunki muszą być spełnione.

3.1. Zgodność z prawem, rzetelność i przejrzystość zasad dotyczących przetwarzania

Najważniejsze kwestie

- Zasady zgodności z prawem, rzetelności i przejrzystości mają zastosowanie do wszystkich operacji przetwarzania danych osobowych.
- Zgodnie z RODO zasada zgodności z prawem wymaga spełnienia jednego z następujących warunków:
  - uzyskano zgodę osoby, której dane dotyczą,
  - przetwarzanie jest niezbędne do zawarcia umowy,
  - przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego,
  - przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby,
  - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
  - przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub prawa osoby, której dane dotyczą.

267 Zaktualizowana konwencja nr 108, art. 11 ust. 1, ogólne rozporządzenie o ochronie danych, art. 23 ust. 1.

268 Ogólne rozporządzenie o ochronie danych, art. 23 ust. 1.

- Przetwarzanie danych osobowych powinno odbywać się w sposób rzetelny.
  - Osoba, której dane dotyczą, musi być poinformowana o ryzyku, aby zapewnić, że przetwarzanie danych nie będzie miało nieprzewidywalnych negatywnych skutków.
- Przetwarzanie danych osobowych powinno odbywać się w przejrzysty sposób.
  - Administratorzy danych muszą poinformować osoby, których dane dotyczą, przed przetwarzaniem ich danych, między innymi o celu przetwarzania oraz o tożsamości i adresie administratora.
  - Informacje na temat operacji przetwarzania muszą być przekazywane jasnym i prostym językiem, aby umożliwić osobom, których dane dotyczą, łatwe zrozumienie związanych z nimi zasad, ryzyka, gwarancji i praw.
  - Osoby, których dane dotyczą, mają prawo dostępu do swoich danych w każdym miejscu ich przetwarzania.

3.1.1. Legalność przetwarzania

Przepisy prawa UE i prawa RE dotyczące ochrony danych wymagają zgodnego z prawem przetwarzania danych osobowych[269]. Przetwarzanie zgodne z prawem wymaga zgody osoby, której dane dotyczą, lub innej uzasadnionej podstawy przewidzianej w przepisach o ochronie danych[270]. Obok zgody, artykuł 6 ust. 1 RODO określa pięć zgodnych z prawem podstaw przetwarzania danych, tj. jeżeli przetwarzanie jest niezbędne do wykonania umowy, do wykonania zadania realizowanego w ramach sprawowania władzy publicznej, do wypełnienia obowiązku prawnego, do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią lub do ochrony żywotnych interesów osoby, której dane dotyczą. Kwestia ta zostanie omówiona bardziej szczegółowo w sekcji 4.1.

3.1.2. Rzetelność przetwarzania danych

Oprócz zgodnego z prawem przetwarzania danych przepisy UE i Rady Europy dotyczące ochrony danych wymagają, aby dane osobowe były przetwarzane w sposób

269 Zaktualizowana konwencja nr 108, art. 5 ust. 3, ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. a).

270 Karta praw podstawowych Unii Europejskiej, art. 8 ust. 2; ogólne przepisy o ochronie danych, motyw 40 i art. 6–9; zaktualizowana konwencja nr 108, art. 5 ust. 2; Explanatory Report of the Modernised Convention 108, pkt 41.

rzetelny[271]. Zasada rzetelnego przetwarzania reguluje przede wszystkim stosunki między administratorem danych a osobą, której dane dotyczą.

Administratorzy powinni powiadomić osoby, których dane dotyczą, i ogół społeczeństwa, że będą przetwarzać dane w sposób zgodny z prawem i przejrzysty oraz muszą być w stanie wykazać zgodność operacji przetwarzania z RODO. Operacji przetwarzania nie wolno wykonywać w tajemnicy, a osoby, których dane dotyczą, powinny być świadome potencjalnych zagrożeń. Ponadto administratorzy muszą w miarę możliwości działać w sposób, który dokładnie odpowiada życzeniom osoby, której dane dotyczą, zwłaszcza gdy jej zgoda stanowi podstawę prawną przetwarzania danych.

Przykład: W sprawie *K.H. i in. przeciwko Słowacji*[272] skarżącymi było osiem kobiet pochodzenia romskiego, które znajdowały się podczas ciąży i porodu pod opieką dwóch szpitali we wschodniej Słowacji. W późniejszym okresie, mimo ponawianych prób, żadnej z nich nie udało się zajść w ciążę. Sądy krajowe nakazały szpitalom, aby umożliwiły skarżącym i ich przedstawicielom wgląd w dokumentację medyczną oraz sporządzenie ręcznych odpisów, ale odrzuciły ich wniosek o wykonanie kserokopii dokumentów, rzekomo w celu zapobiegania nadużyciom. Pozytywne obowiązki państw członkowskich na mocy art. 8 EKPC obejmują zobowiązanie do udostępnienia osobom, których dane dotyczą, kopii ich akt. Państwo miało obowiązek określić zasady kopiowania akt zawierających dane osobowe lub, w stosownych przypadkach, wskazać istotne powody odmowy. W przypadku skarżących sądy krajowe uzasadniły zakaz wykonywania kopii dokumentacji medycznej głównie potrzebą ochrony stosownych informacji przed nadużyciami. Europejski Trybunał Praw Człowieka nie dostrzegł jednak możliwości, aby skarżące, które uzyskały w każdym razie dostęp do całości swojej dokumentacji medycznej, mogły nadużyć informacji na własny temat. Ponadto ryzyku takich nadużyć można było zapobiec za pomocą środków innych niż odmowa udostępnienia skarżącym kopii akt, np. zawężając krąg osób uprawnionych do dostępu do akt. Państwo nie wykazało istnienia wystarczająco istotnych powodów, aby odmówić skarżącym skutecznego dostępu do informacji dotyczących ich zdrowia. Trybunał stwierdził, że doszło do naruszenia art. 8.

271 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. a); zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. a).

272 ETPC, *K.H. i in. przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.

W przypadku usług internetowych systemy przetwarzające dane muszą funkcjonować w sposób umożliwiający osobom, których dane dotyczą, zrozumienie, co naprawdę dzieje się z ich danymi. Zasada rzetelności w każdym razie wykracza poza obowiązki w zakresie przejrzystości i można ją także wiązać z etycznym przetwarzaniem danych osobowych.

Przykład: Jednostka badawcza na uniwersytecie prowadzi na 50 osobach eksperyment analizujący zmiany nastrojów. Wymaga się od nich rejestrowania w pliku elektronicznym swoich myśli co godzinę, o konkretnej porze. Pięćdziesiąt osób wyraziło zgodę na udział w tym konkretnym projekcie i to konkretne wykorzystanie danych przez uniwersytet. Jednostka badawcza szybko odkrywa, że elektroniczne rejestrowanie myśli byłoby bardzo przydatne w innym projekcie dotyczącym zdrowia psychicznego, koordynowanym przez inny zespół. Mimo że uniwersytet, jako administrator danych, mógł wykorzystać te same dane do pracy w innym zespole bez podejmowania dalszych kroków w celu zapewnienia zgodności z prawem przetwarzania tych danych, biorąc pod uwagę, że cele są kompatybilne, poinformował on uczestników i zwrócił się o nową zgodę, zgodnie ze swoim kodeksem etyki badań i zasadą uczciwego przetwarzania danych.

3.1.3. Przejrzystość przetwarzania danych

Przepisy prawa UE i prawa RE dotyczące ochrony danych wymagają, aby przetwarzanie danych osobowych odbywało się „w sposób przejrzysty dla osoby, której dane dotyczą”[273].

Zasada ta nakłada na administratora obowiązek podjęcia wszelkich odpowiednich środków w celu informowania osób, których dane dotyczą – którymi mogą być użytkownicy lub klienci – o sposobie wykorzystywania ich danych[274]. Przejrzystość może odnosić się do informacji przekazanych osobie fizycznej przed rozpoczęciem przetwarzania[275], informacji, które powinny być łatwo dostępne dla osób, których dane

273 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. a), zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. a) i art. 8.

274 Ogólne rozporządzenie o ochronie danych, art. 12.

275 Tamże, art. 13 i 14.

dotyczą, w trakcie przetwarzania[276], ale także informacji przekazanych osobom, których dane dotyczą, na wniosek o dostęp do ich własnych danych[277].

> Przykład: W sprawie *Haralambie przeciwko Rumunii*[278] skarżący domagał się dostępu do akt przechowywanych na jego temat przez tajne służby, ale jego żądanie zostało spełnione dopiero pięć lat później. Europejski Trybunał Praw Człowieka powtórzył, że osoby, których dotyczą akta osobowe będące w posiadaniu organów publicznych, mają istotny interes w uzyskaniu do nich dostępu. Władze miały obowiązek zapewnić skuteczną procedurę uzyskiwania dostępu do takich informacji. Trybunał uznał, że ani liczba przekazywanych akt, ani uchybienia w systemie archiwalnym nie uzasadniały pięcioletniego opóźnienia w spełnieniu żądania skarżącego dotyczącego dostępu do jego akt. Władze nie zapewniły skarżącemu skutecznej i dostępnej procedury, aby umożliwić mu uzyskanie dostępu do swoich akt osobowych w rozsądnym czasie. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Operacje przetwarzania danych należy wyjaśnić osobom, których dane dotyczą, w przystępny sposób gwarantujący zrozumienie, co stanie się z ich danymi. Oznacza to, że konkretny cel przetwarzania danych osobowych musi być znany osobie, której dane dotyczą, w momencie zbierania danych osobowych[279]. Zasada przejrzystości wymaga stosowania jasnego i prostego języka[280]. Zainteresowane osoby muszą mieć jasny obraz ryzyka, zasad, gwarancji i praw związanych z przetwarzaniem ich danych osobowych[281].

Prawo RE stanowi również, że niektóre istotne informacje muszą być obowiązkowo i w sposób aktywny przekazywane przez administratora osobom, których dane dotyczą. Informacje o nazwie i adresie administratora (lub współadministratorów), podstawie prawnej i celach przetwarzania danych, kategoriach przetwarzanych danych i odbiorców, a także o sposobach korzystania z praw mogą być przekazywane w dowolnym formacie (za pośrednictwem strony internetowej, narzędzi

276 Grupa Robocza Art. 29 (2017), *Opinion 2/2017 on data processing at work*, WP 249, s. 23.

277 Ogólne rozporządzenie o ochronie danych, art. 15.

278 ETPC, *Haralambie przeciwko Rumunii*, nr 21737/03, 27 października 2009 r.

279 Ogólne rozporządzenie o ochronie danych, motyw 39.

280 Tamże.

281 Tamże.

technologicznych na urządzeniach osobistych itp.), o ile informacje są przedstawiane osobom, których dane dotyczą w sposób rzetelny i skuteczny. Prezentowane informacje powinny być łatwo dostępne, czytelne, zrozumiałe i dostosowane do potrzeb osób, których dane dotyczą (np. w języku przyjaznym dla dzieci, jeżeli jest to konieczne). Należy również przedstawić wszelkie dodatkowe informacje, które są niezbędne do zapewnienia rzetelnego przetwarzania danych lub które są przydatne do tego celu, takie jak okres przechowywania danych, wiedza o argumentacji leżącej u podstaw przetwarzania danych lub informacje dotyczące przekazywania danych odbiorcy na terytorium innej Strony lub podmiotu niebędącego Stroną (w tym, czy dany podmiot niebędący Stroną zapewnia odpowiedni poziom ochrony lub środki podjęte przez administratora w celu zagwarantowania takiego odpowiedniego poziomu ochrony danych)[282].

Zgodnie z prawem dostępu[283] osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, które dane podlegają przetwarzaniu[284]. Ponadto, zgodnie z prawem do informacji[285], osoby, których dane są przetwarzane, muszą być aktywnie informowane przez administratorów lub podmioty przetwarzające między innymi o celach, długości i sposobach przetwarzania, zasadniczo przed rozpoczęciem przetwarzania.

Przykład: Sprawa *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*[286] dotyczyła przekazywania danych podatkowych odnoszących się do dochodów osób prowadzących działalność na własny rachunek z krajowej agencji administracji podatkowej do kasy ubezpieczeń zdrowotnych w Rumunii, na podstawie których wymagane było opłacanie zaległych składek na ubezpieczenie zdrowotne. Zwrócono się do TSUE o ustalenie, czy należało wcześniej poinformować osobę, której dane dotyczą, o tożsamości administratora danych i celu przekazania danych przed ich przetworzeniem przez kasę ubezpieczeń zdrowotnych. Trybunał Sprawiedliwości orzekł, że w przypadku gdy organ administracji publicznej państwa członkowskiego przekazuje dane osobowe innemu organowi

282 Explanatory Report of Modernised Convention 108, pkt 68.

283 Ogólne rozporządzenie o ochronie danych, art. 15.

284 Zaktualizowana konwencja nr 108, art. 8 i art. 9 ust. 1 lit. b).

285 Ogólne rozporządzenie o ochronie danych, art. 13 i 14.

286 TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 1 października 2015 r., pkt 28–46.

administracji publicznej, który dalej przetwarza te dane, osoby, których dane dotyczą, muszą zostać poinformowane o takim przekazaniu lub przetwarzaniu.

W niektórych sytuacjach dopuszcza się odstępstwa od obowiązku informowania osób, których dane dotyczą, o przetwarzaniu danych, które to sytuacje zostaną omówione bardziej szczegółowo w sekcji 6.1 dotyczącej praw osób, których dane dotyczą.

3.2. Zasada ograniczenia celu

Najważniejsze kwestie

- Cel przetwarzania danych musi zostać jasno określony przed rozpoczęciem przetwarzania.
- Niedopuszczalne jest dalsze przetwarzanie danych w sposób niezgodny z pierwotnym celem, chociaż ogólne rozporządzenie o ochronie danych przewiduje wyjątki od tej zasady w przypadku przetwarzania do celów archiwizacji w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.
- Co do istoty zasada ograniczenia celu oznacza, że wszelkie przetwarzanie danych osobowych musi odbywać się w konkretnym, wyraźnie określonym celu i tylko w dodatkowych, określonych celach, które są zgodne z celem pierwotnym.

Zasada ograniczenia celu jest jedną z podstawowych zasad europejskiego prawa ochrony danych. Jest ona ściśle związana z przejrzystością, przewidywalnością i kontrolą sprawowaną przez użytkowników: jeżeli cel przetwarzania danych jest wystarczająco konkretny i jasny, osoby fizyczne wiedzą, czego się spodziewać, a przejrzystość i pewność prawa są większe. Jednocześnie ważne jest jasne określenie celu, aby umożliwić osobom, których dane dotyczą, skuteczne wykonywanie swoich praw, takich jak prawo do sprzeciwu wobec przetwarzania danych[287].

Zgodnie z tą zasadą wszelkie przetwarzanie danych osobowych musi odbywać się w konkretnym, wyraźnie określonym celu i tylko w dodatkowych celach, które są zgodne z celem pierwotnym[288]. Przetwarzanie danych osobowych do celów nie-

287 Grupa Robocza Art. 29 (2013), *Opinion 3/2013 on purpose limitation*, WP 203, 2 kwietnia 2013 r.

288 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. b).

określonych lub nieograniczonych jest zatem niezgodne z prawem. Przetwarzanie danych osobowych bez określonego celu, jedynie ze względu na ich potencjalną użyteczność w przyszłości, również nie jest zgodne z prawem. Legalność przetwarzania danych osobowych będzie zależeć od celu przetwarzania, który musi być wyraźny, konkretny i prawnie uzasadniony.

Każdy nowy cel przetwarzania danych, który nie jest zgodny z celem pierwotnym, musi posiadać własną konkretną podstawę prawną i nie można powoływać się na fakt, że dane zostały pierwotnie pozyskane bądź były przetwarzane w innym prawnie uzasadnionym celu. Prawnie uzasadnione przetwarzanie danych ogranicza się z kolei do pierwotnie określonego celu, a każdy nowy cel przetwarzania wymaga nowej odrębnej podstawy prawnej. Na przykład szczególnie starannie należy rozważyć ujawnienie danych w nowym celu stronom trzecim, gdyż tego rodzaju ujawnienie zazwyczaj wymaga dodatkowej podstawy prawnej, odrębnej od tej wykorzystanej w celu zebrania danych.

Przykład: Linia lotnicza gromadzi od pasażerów dane w celu dokonania rezerwacji i zapewnienia prawidłowej obsługi lotu. Linia potrzebuje danych na temat: numerów miejsc pasażerów, specjalnych ograniczeń fizycznych, jak np. potrzeby korzystania z wózków inwalidzkich, oraz specjalnych wymagań żywieniowych, np. posiłków koszernych lub halal. Jeżeli linie zostaną poproszone o przekazanie tych danych, które są zawarte w danych dotyczących przelotu pasażera, organom imigracyjnym na lotnisku docelowym, dane te są w takim przypadku wykorzystywane do celu kontroli imigracyjnej, który różni się od pierwotnego celu zbierania danych. Przekazanie tych danych organowi imigracyjnemu będzie zatem wymagało nowej i odrębnej podstawy prawnej.

Jeżeli chodzi o zakres i ograniczenia danego celu, w zaktualizowanej konwencji nr 108 oraz ogólnym rozporządzeniu o ochronie danych odwołano się do pojęcia zgodności: wykorzystanie danych do zgodnych celów może nastąpić w oparciu o pierwotną podstawę prawną. Dalsze przetwarzanie danych nie może zatem odbywać się w sposób nieoczekiwany, niewłaściwy lub budzący sprzeciw osoby, której dane dotyczą[289]. Aby ocenić, czy dalsze przetwarzanie należy uznać za zgodne, administrator danych powinien uwzględnić (między innymi) następujące kwestie:

289 Explanatory Report of Modernised Convention 108, pkt 49.

- „wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania,

- kontekst, w którym dane osobowe zostały zebrane, w szczególności rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać dalszego wykorzystania danych, oparte na rodzaju ich powiązania z administratorem,

- charakter danych osobowych,

- konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą, oraz

- istnienie odpowiednich zabezpieczeń zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania"[290]. Można tego dokonać na przykład poprzez szyfrowanie lub pseudonimizację.

Przykład: Spółka Sunshine uzyskała dane dotyczące klientów w ramach zarządzania kontaktami z klientami (CRM). Spółka przekazuje następnie te dane spółce z branży marketingu bezpośredniego, spółce Moonlight, która z kolei chce wykorzystać te dane w kampaniach marketingowych innych firm. Przekazanie przez Sunshine danych inny spółkom do celów marketingowych stanowi dalsze wykorzystanie danych do nowego celu, który jest niezgodny z zarządzaniem kontaktami z klientami, czyli pierwotnym celem zbierania danych klientów przez spółkę Sunshine. W związku z tym przekazanie danych spółce Moonlight wymaga odrębnej podstawy prawnej.

Natomiast wykorzystanie przez spółkę Sunshine danych wykorzystywanych do zarządzania kontaktami z klientami do jej własnych celów marketingowych, czyli wysyłania komunikatów marketingowych do swoich klientów w związku z własnymi produktami, jest generalnie uznawane za cel zgodny.

W ogólnym rozporządzeniu o ochronie danych i w zaktualizowanej konwencji nr 108 stwierdza się, że „dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych"

290 Ogólne rozporządzenie o ochronie danych, motyw 50 i art. 6 ust. 4; Komitet *ad hoc* ds. Ochrony Danych (CAHDATA), Explanatory Report of the Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, pkt 49.

a priori uznaje się za zgodne z celem pierwotnym[291]. Podczas dalszego przetwarzania danych osobowych należy jednak zapewnić odpowiednie zabezpieczenia, takie jak anonimizacja, szyfrowanie lub pseudonimizacja danych, a także ograniczenie dostępu do tych danych[292]. W ogólnym rozporządzeniu o ochronie danych dodaje się, że „[j]eżeli osoba, której dane dotyczą, wyraziła zgodę lub jeżeli przetwarzanie ma za podstawę prawo Unii lub prawo państwa członkowskiego stanowiące w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia w szczególności realizację ważnych celów leżących w ogólnym interesie publicznym, administrator powinien móc dokonać dalszego przetwarzania danych osobowych, bez względu na jego zgodność z pierwotnymi celami"[293]. Podejmując dalsze przetwarzanie, osoba, której dane dotyczą, powinna być zatem poinformowana o celach, jak również o swoich prawach, takich jak prawo do sprzeciwu[294].

Przykład: Spółka Sunshine zbiera i przechowuje dane służące do zarządzania kontaktami z klientami. Dodatkowe wykorzystanie tych danych przez spółkę Sunshine do analizy statystycznej zachowań zakupowych jej klientów jest dopuszczalne, gdyż statystyka jest celem zgodnym. Nie jest potrzebna dodatkowa podstawa prawna, taka jak zgoda osób, których dane dotyczą. Jednakże w celu dalszego przetwarzania danych osobowych do celów statystycznych spółka Sunshine musi wprowadzić odpowiednie zabezpieczenia praw i wolności osoby, której dane dotyczą. Środki techniczne i organizacyjne, które musi wdrożyć spółka Sunshine, mogą obejmować pseudonimizację.

291 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. b), zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. b). Przykładem takich przepisów krajowych jest austriacka ustawa o ochronie danych (*Datenschutzgesetz*), BGBl (austriacki federalny dziennik ustaw) I nr 165/1999, pkt 46.

292 Ogólne rozporządzenie o ochronie danych art. 6 ust. 4, zaktualizowana konwencja nr 108, Explanatory Report of Modernised Convention 108, pkt 50.

293 Ogólne rozporządzenie o ochronie danych, motyw 50.

294 Tamże.

3.3. Zasada minimalizacji danych

Najważniejsze kwestie

- Przetwarzanie danych musi ograniczać się do tego, co jest konieczne do osiągnięcia prawnie uzasadnionego celu.
- Przetwarzanie danych osobowych powinno mieć miejsce wyłącznie wtedy, gdy celu przetwarzania nie można racjonalnie osiągnąć innymi sposobami.
- Przetwarzanie danych nie może w sposób nieproporcjonalny ingerować w interesy, prawa i wolności osób, których dane dotyczą.

Przetwarzanie jest możliwe wyłącznie w odniesieniu do danych, które są „adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane”[295]. Kategorie danych wybranych do przetwarzania muszą być konieczne do osiągnięcia deklarowanego ogólnego celu operacji przetwarzania, a administrator danych powinien ściśle ograniczyć gromadzenie danych do takich informacji, które są bezpośrednio związane z konkretnym celem przetwarzania.

Przykład: W sprawie *Digital Rights Ireland*[296] przedmiotem rozważań TSUE była ważność dyrektywy w sprawie zatrzymywania danych, której celem jest harmonizacja przepisów krajowych dotyczących zatrzymywania danych osobowych generowanych lub przetwarzanych przez publicznie dostępne usługi lub sieci łączności elektronicznej w celu ich ewentualnego przekazania właściwym organom w celu zwalczania poważnej przestępczości, takiej jak przestępczość zorganizowana i terroryzm. Mimo że uznano, że jest to cel, który rzeczywiście odzwierciedla cel leżący w interesie ogólnym, za problematyczny uznano uogólniony sposób, w jaki dyrektywa obejmowała swoim zakresem „wszystkie jednostki, środki łączności elektronicznej i dane o ruchu, przy czym nie przewidziano w niej jakiegokolwiek zróżnicowania, ograniczenia lub wyjątku w zależności od celu dotyczącego zwalczania poważnych przestępstw”[297].

295 Zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. c), ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. c).

296 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

297 Tamże, pkt 44 i 57.

Ponadto dzięki wykorzystaniu specjalnych technologii zwiększających ochronę prywatności można czasami uniknąć wykorzystywania jakichkolwiek danych osobowych bądź wykorzystać środki służące ograniczeniu możliwości przypisania danych osobie, której dane dotyczą (na przykład stosując pseudonimizację), co skutkuje rozwiązaniem sprzyjającym ochronie prywatności. Takie podejście jest szczególnie właściwe w przypadku bardziej rozbudowanych systemów przetwarzania.

Przykład: Rada miasta oferuje za opłatą karty chipowe dla regularnych użytkowników miejskiego systemu transportu publicznego. Na karcie nadrukowano nazwisko użytkownika, które jest też przechowywane w formie elektronicznej w pamięci karty chipowej. Przy każdej podróży autobusem lub tramwajem kartę chipową należy zbliżyć do czytnika w pojeździe. Dane odczytane przez urządzenie są porównywane w systemie elektronicznym z zapisanymi w bazie danych nazwiskami osób, które nabyły karty.

System ten nie jest zoptymalizowany pod kątem zasady minimalizacji danych: sprawdzenia, czy dana osoba jest uprawniona, by korzystać ze środków transportu, można dokonać bez porównywania danych osobowych zapisanych w pamięci karty z bazą danych. Wystarczyłoby na przykład zapisać w pamięci karty specjalny elektroniczny obraz, taki jak np. kod kreskowy, który po odczytaniu przez czytnik potwierdzałby, czy karta jest ważna czy też nie. Taki system nie rejestrowałby, kto i kiedy używał jakiego środka transportu. Byłoby to optymalnym rozwiązaniem z punktu widzenia zasady minimalizacji danych, gdyż zasada ta skutkuje obowiązkiem ograniczenia gromadzenia danych do minimum.

Artykuł 5 ust. 1 zaktualizowanej konwencji nr 108 zawiera wymóg proporcjonalności przetwarzania danych osobowych w stosunku do zamierzonego, prawnie uzasadnionego celu. Na wszystkich etapach przetwarzania musi istnieć odpowiednia równowaga między wszystkimi zaangażowanymi interesami. Oznacza to, że „dane osobowe, które są odpowiednie i istotne, ale które wiązałyby się z nieproporcjonalną ingerencją w podstawowe prawa i wolności osób, których dane dotyczą, należy uznać za nadmierne”[298].

298 Explanatory Report of the Modernised Convention 108, pkt 52, ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. c).

3.4. Zasada prawidłowości danych

Najważniejsze kwestie

- Zasada prawidłowości danych musi być stosowana przez administratora w związku ze wszystkimi operacjami przetwarzania.
- Nieprawidłowe dane osobowe należy niezwłocznie usunąć lub sprostować.
- Może zaistnieć potrzeba regularnej kontroli i aktualizacji danych w celu zapewnienia ich prawidłowości.

Administrator danych osobowych nie może korzystać z tych informacji bez podjęcia kroków w celu zapewnienia z odpowiednią pewnością, że dane te są prawidłowe i aktualne[299].

Obowiązek zapewnienia prawidłowości danych należy rozpatrywać w kontekście celu przetwarzania danych.

Przykład: W sprawie *Rijkeboer*[300] TSUE rozpatrywał wniosek obywatela niderlandzkiego o uzyskanie od organu administracji lokalnej miasta Amsterdamu informacji na temat tożsamości osób, którym w poprzednich dwóch latach przekazano dane dotyczące jego osoby znajdujące się w posiadaniu władz lokalnych, a także na temat treści ujawnionych danych. Trybunał Sprawiedliwości stwierdził, że „prawo do poszanowania życia prywatnego implikuje, że osoba, której dane dotyczą, może upewnić się, iż te dane osobowe są przetwarzane prawidłowo oraz legalnie, to znaczy, w szczególności, że dotyczące jej dane podstawowe są prawidłowe i skierowane do uprawnionych odbiorców". Trybunał Sprawiedliwości odniósł się następnie do preambuły dyrektywy o ochronie danych, zgodnie z którą osoba, której dane dotyczą, musi mieć możliwość skorzystania z prawa dostępu do dotyczących jej danych osobowych, aby móc dokonać weryfikacji ich prawidłowości[301].

299 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. d), zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. d).

300 TSUE, C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M. E. E. Rijkeboerowi*, 7 maja 2009 r.

301 Poprzedni motyw 41 preambuły dyrektywy 95/46/WE.

Mogą też występować przypadki, w których aktualizacja przechowywanych danych jest zabroniona z mocy prawa, gdyż głównym celem przechowywania danych jest udokumentowanie pewnych zdarzeń jako swoistego „kadru z historii".

Przykład: Protokół z operacji medycznej nie może zostać zmieniony (innymi słowy „zaktualizowany"), nawet jeżeli ustalenia w nim zawarte okażą się później błędne. W takich okolicznościach można jedynie sporządzić uzupełnienia do protokołu, jeżeli zostaną one wyraźnie oznaczone jako fragmenty dodane w późniejszym czasie.

Z drugiej strony występują sytuacje, w których bezwzględnie konieczne jest aktualizowanie i regularne sprawdzanie prawidłowości danych, ze względu na potencjalne szkody wyrządzone osobie, której dane dotyczą, jeżeli dane pozostałyby nieprawidłowe.

Przykład: Jeżeli potencjalny klient chce zawrzeć umowę o kredyt z instytucją bankową, bank zazwyczaj sprawdza jego zdolność kredytową. Wykorzystuje w tym celu specjalne bazy danych zawierające dane o historii kredytowej osób fizycznych. Jeżeli taka baza danych zawiera niepoprawne lub nieaktualne dane o danej osobie, osoba taka może odczuć negatywne tego skutki. W związku z tym administratorzy takich baz danych powinni dokładać szczególnych starań, aby przestrzegać zasady prawidłowości.

3.5. Zasada ograniczenia przechowywania

Najważniejsze kwestie

- Zasada ograniczenia przechowywania oznacza, że dane osobowe muszą zostać usunięte lub zanonimizowane, gdy tylko nie są już potrzebne do celów, dla których zostały zgromadzone.

Na gruncie art. 5 ust. 1 lit. e) RODO i, odpowiednio, art. 5 ust. 4 lit. e) zaktualizowanej konwencji nr 108 wymaga się, aby dane osobowe były „przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane". Dlatego też dane

te muszą zostać usunięte lub zanonimizowane po osiągnięciu tych celów. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, „administrator powinien ustalić termin ich usuwania lub okresowego przeglądu”[302].

W sprawie *S. i Marper* ETPC stwierdził, że podstawowe zasady odpowiednich instrumentów Rady Europy oraz prawa i praktyki innych umawiających się państw wymagają, aby zatrzymywanie danych było proporcjonalne w stosunku do celów gromadzenia i ograniczone w czasie, szczególnie w sektorze policji[303].

Przykład: W sprawie *S. i Marper*[304] ETPC stwierdził, że nieograniczone zatrzymywanie odcisków palców, próbek komórek i profili DNA obu skarżących było w społeczeństwie demokratycznym nieproporcjonalne i niepotrzebne, zważywszy, że postępowanie karne przeciwko obu skarżącym zostało zakończone odpowiednio wyrokiem uniewinniającym i umorzeniem postępowania.

Ograniczenie okresu przechowywania danych osobowych ma jednak zastosowanie tylko do danych przechowywanych w formie umożliwiającej identyfikację osób, których dane dotyczą. Dlatego też zgodne z prawem przechowywanie danych, które nie są już potrzebne, można by osiągnąć poprzez anonimizację danych.

Dane archiwizowane w interesie publicznym, do celów naukowych lub historycznych lub do celów statystycznych mogą być przechowywane przez dłuższy okres, pod warunkiem że dane te będą wykorzystywane wyłącznie do wyżej wymienionych celów[305]. Należy wdrożyć odpowiednie środki techniczne i organizacyjne w zakresie bieżącego przechowywania i wykorzystywania danych osobowych w celu ochrony praw i wolności osoby, której dane dotyczą.

Zaktualizowana konwencja nr 108 dopuszcza również wyjątki od zasady ograniczenia przechowywania, pod warunkiem że są one przewidziane prawem, respektują istotę podstawowych praw i wolności oraz są konieczne i proporcjonalne do

302 Ogólne rozporządzenie o ochronie danych, motyw 39.

303 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.; zob. także na przykład: ETPC, *M.M. przeciwko Zjednoczonemu Królestwu*, nr 24029/07, 13 listopada 2012 r.

304 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.

305 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. e), zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. b) i art. 11 ust. 2.

osiągnięcia ograniczonej liczby zgodnych z prawem celów[306]. Obejmują one między innymi ochronę bezpieczeństwa narodowego, dochodzenie i ściganie przestępstw, wykonywanie sankcji karnych, ochronę osoby, której dane dotyczą, oraz ochronę praw i podstawowych wolności innych osób.

Przykład: W sprawie *Digital Rights Ireland*[307] TSUE dokonał przeglądu ważności dyrektywy w sprawie zatrzymywania danych, która miała na celu harmonizację przepisów krajowych dotyczących zatrzymywania danych osobowych generowanych lub przetwarzanych przez publicznie dostępne usługi łączności elektronicznej lub sieci łączności elektronicznej w celu zwalczania poważnej przestępczości, takiej jak przestępczość zorganizowana i terroryzm. Dyrektywa w sprawie zatrzymywania danych przewidywała okres „co najmniej sześciu miesięcy, przy czym nie wskazuje żadnych różnic między kategoriami danych przewidzianymi w art. 5 w zależności od zainteresowanych osób lub ewentualnej użyteczności danych w stosunku do zakładanego celu"[308]. Trybunał Sprawiedliwości podniósł także kwestię braku obiektywnych kryteriów w dyrektywie w sprawie zatrzymywania danych, na podstawie których należy ustalić czas, na jaki dane te zostaną zatrzymane – wynoszący od co najmniej sześciu do maksymalnie dwudziestu czterech miesięcy – aby zagwarantować, że czas ten będzie ograniczał się do tego, co ściśle niezbędne[309].

3.6. Zasada bezpieczeństwa danych

Najważniejsze kwestie

- Bezpieczeństwo i poufność danych osobowych mają kluczowe znaczenie dla zapobiegania niekorzystnym skutkom dla osoby, której dane dotyczą.
- Środki bezpieczeństwa mogą mieć charakter techniczny lub organizacyjny.

306 Zaktualizowana konwencja nr 108, art. 11 ust. 1; Explanatory Report of Modernised Convention 108, pkt 91–98.

307 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

308 Tamże, pkt 63.

309 Tamże, pkt 64.

- Pseudonimizacja jest procesem, który może chronić dane osobowe.
- Stosowność środków bezpieczeństwa musi być określana indywidualnie dla każdego przypadku i poddawana regularnym przeglądom.

Zasada bezpieczeństwa danych wymaga wdrożenia odpowiednich środków technicznych lub organizacyjnych przy przetwarzaniu danych osobowych w celu ochrony danych przed przypadkowym, niedozwolonym lub niezgodnym z prawem dostępem, wykorzystaniem, zmianą, ujawnieniem, utratą, zniszczeniem lub uszkodzeniem[310]. Ogólne rozporządzenie o ochronie danych przewiduje, że wdrażając te środki administrator i podmiot przetwarzający powinni uwzględniać „stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia"[311]. W zależności od konkretnych okoliczności każdego przypadku odpowiednie środki techniczne i organizacyjne mogą obejmować na przykład pseudonimizację i szyfrowanie danych osobowych lub regularne testowanie i ocenę skuteczności środków mających na celu zapewnienie bezpieczeństwa przetwarzania danych[312].

Jak wyjaśniono w sekcji 2.1.1, dane spseudonimizowane oznaczają zastąpienie identyfikatorów w danych osobowych – które umożliwiają identyfikację osoby, której dane dotyczą – pseudonimem oraz przechowanie tych identyfikatorów oddzielnie, w ramach środków technicznych lub organizacyjnych. Procesu pseudonimizacji nie należy mylić z procesem anonimizacji, w którym wszystkie powiązania z identyfikacją osoby zostają zerwane.

Przykład: Zdanie „Charles Spencer, urodzony 3 kwietnia 1967 r., jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek" można spseudonimizować na przykład w następujący sposób:

„C.S. 1967 jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek" lub

„324 jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek", lub

YESz320l jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek".

310 Ogólne rozporządzenie o ochronie danych, motyw 39 i art. 5 pkt 1 lit. f), zaktualizowana konwencja nr 108, art. 7.

311 Ogólne rozporządzenie o ochronie danych, art. 32 ust. 1.

312 Tamże.

Użytkownicy dysponujący dostępem do tych spseudonimizowanych danych zazwyczaj nie są w stanie zidentyfikować „Charlesa Spencera, urodzonego 3 kwietnia 1967 r." na podstawie „324" lub „YESz3201". Spseudonimizowane dane są więc zazwyczaj lepiej zabezpieczone przed niewłaściwym wykorzystaniem.

Dane w pierwszym przykładzie są jednak zabezpieczone słabiej. Zdanie „C.S. 1967 jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek" użyte w niewielkiej wsi, w której mieszka Charles Spencer może prowadzić do łatwego rozpoznania jego osoby. Metoda pseudonimizacji wpływa na skuteczność ochrony danych.

Dane osobowe z zaszyfrowanymi lub odrębnie przechowywanymi identyfikatorami są wykorzystywane w wielu sytuacjach, aby zachować tożsamość osób w tajemnicy. Jest to szczególnie użyteczne, gdy administratorzy danych muszą się upewnić, że mają do czynienia z tymi samymi osobami, których dane dotyczą, ale nie muszą (lub nie powinni) znać prawdziwej tożsamości osób, których dane dotyczą. Przykładem jest sytuacja, gdy badacz bada przebieg choroby u pacjentów, których tożsamość jest znana tylko szpitalowi, w którym są leczeni, i skąd badacz uzyskuje spseudonimizowane historie choroby. Pseudonimizacja stanowi zatem istotny element w arsenale technologii służących zwiększeniu ochrony prywatności. Może ona pełnić ważną rolę przy uwzględnieniu ochrony prywatności już w fazie projektowania. Oznacza to wbudowanie ochrony danych jako nieodłącznego elementu zaawansowanych systemów przetwarzania danych.

Artykuł 25 RODO, który dotyczy ochrony danych w fazie projektowania, wyraźnie odnosi się do pseudonimizacji jako przykładu odpowiedniego środka technicznego i organizacyjnego, który administratorzy powinni wdrożyć, aby dostosować się do zasad ochrony danych i zintegrować niezbędne zabezpieczenia. Czyniąc to, administratorzy danych spełnią wymogi rozporządzenia i będą chronić prawa osób, których dane dotyczą, przetwarzając ich dane osobowe.

Przestrzeganie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może pomóc w wykazaniu zgodności z wymogami w zakresie bezpieczeństwa przetwarzania danych[313]. W swojej opinii w sprawie wpływu przetwarzania danych dotyczących przelotu pasażera na ochronę danych osobowych, Rada Europy podaje inne przykłady odpowiednich środków bezpieczeństwa służących ochronie danych osobowych w systemach rejestrujących dane dotyczące przelotu pasażera, takich jak przechowywanie danych w bezpiecznym środowisku

313 Tamże, art. 32 ust. 3.

fizycznym, ograniczanie kontroli dostępu poprzez warstwowe logowanie oraz ochrona przekazywania danych silną kryptografią[314].

Przykład: Portale społecznościowe i dostawcy poczty elektronicznej umożliwiają użytkownikom dodanie dodatkowej warstwy bezpieczeństwa danych do świadczonych przez nich usług poprzez wprowadzenie dwustopniowego uwierzytelniania. Oprócz wprowadzenia osobistego hasła, użytkownik musi wpisać drugi login, aby wejść na swoje konto osobiste. Może to być na przykład wpisanie kodu bezpieczeństwa wysłanego na numer telefonu komórkowego połączonego z kontem osobistym. W ten sposób dwuetapowa weryfikacja zapewnia lepszą ochronę danych osobowych przed nieuprawnionym dostępem do kont osobistych przez hakerów.

Sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108 zawiera dodatkowe przykłady odpowiednich zabezpieczeń, takich jak wprowadzenie obowiązku zachowania tajemnicy służbowej lub przyjęcie kwalifikowanych technicznych środków bezpieczeństwa, takich jak szyfrowanie danych[315]. Wprowadzając szczególne środki bezpieczeństwa, administrator – lub, w stosownych przypadkach, podmiot przetwarzający – powinien uwzględnić kilka elementów, takich jak charakter i ilość przetwarzanych danych osobowych, potencjalne negatywne konsekwencje dla osób, których dane dotyczą oraz potrzebę ograniczonego dostępu do danych[316]. Wdrażając odpowiednie środki bezpieczeństwa, należy wziąć pod uwagę aktualny stan wiedzy w zakresie metod i technik bezpieczeństwa danych w odniesieniu do przetwarzania danych. Koszt takich środków musi być proporcjonalny do wagi i prawdopodobieństwa wystąpienia potencjalnego ryzyka. Wymagany jest regularny przegląd środków bezpieczeństwa, aby w razie potrzeby mogły one być aktualizowane[317].

W przypadkach naruszenia ochrony danych osobowych zarówno zaktualizowana konwencja nr 108, jak i RODO wymagają od administratora danych niezwłocznego zgłoszenia właściwemu organowi nadzorczemu naruszenia stanowiącego zagrożenie dla praw i wolności osób fizycznych[318]. Podobny obowiązek komunikacyjny

314 Rada Europy, Komitet konwencji nr 108, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 sierpnia 2016 r., s. 9.

315 Explanatory Report of the Modernised Convention 108, pkt 56.

316 Tamże, pkt 62.

317 Tamże, pkt 63.

318 Zaktualizowana konwencja nr 108, art. 7 ust. 2, ogólne rozporządzenie o ochronie danych, art. 33 ust. 1.

względem osoby, której dane dotyczą, istnieje, gdy naruszenie ochrony danych osobowych może spowodować wysokie ryzyko naruszenia jej praw i wolności[319]. Przy zawiadamianiu osób, których dane dotyczą, o takich naruszeniach należy stosować jasny i prosty język[320]. Jeżeli podmiot przetwarzający stwierdzi naruszenie ochrony danych osobowych, musi niezwłocznie zgłosić je administratorowi[321]. W niektórych sytuacjach mogą mieć zastosowanie wyjątki od obowiązku zgłoszenia. Na przykład administrator nie ma obowiązku dokonania zgłoszenia organowi nadzorczemu, gdy „jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych"[322]. Nie jest również konieczne zawiadomienie osoby, której dane dotyczą, w przypadku gdy wdrożone środki bezpieczeństwa uniemożliwiają odczyt tych danych osobom nieuprawnionym lub gdy następne środki eliminują prawdopodobieństwo wysokiego ryzyka[323]. Jeżeli zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony danych wymagałoby niewspółmiernie dużego wysiłku ze strony administratora, publiczny komunikat lub podobny środek mogą zapewnić, że „osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób"[324].

3.7. Zasada rozliczalności

Najważniejsze kwestie

- Rozliczalność wymaga aktywnego i nieustannego wdrażania przez administratorów i podmioty przetwarzające działań na rzecz promowania i zagwarantowania ochrony danych podczas prowadzonych czynności przetwarzania.
- Administratorzy i podmioty przetwarzające są odpowiedzialni za zgodność czynności przetwarzania z prawem o ochronie danych i ciążącymi na nich odpowiednimi zobowiązaniami.

319 Zaktualizowana konwencja nr 108, art. 7 ust. 2, ogólne rozporządzenie o ochronie danych, art. 34 ust. 1.

320 Ogólne rozporządzenie o ochronie danych, art. 34 ust. 2.

321 Tamże, art. 33 ust. 1.

322 Tamże.

323 Tamże, art. 34 ust. 3 lit. a) i b)

324 Tamże, art. 34 ust. 3 lit. c).

- Administratorzy powinni w każdej chwili być w stanie wykazać wobec osób, których dane dotyczą, ogółu społeczeństwa oraz organów nadzorczych, że przestrzegają przepisów w zakresie ochrony danych. Podmioty przetwarzające muszą również wypełniać pewne obowiązki ściśle związane z rozliczalnością (takie jak prowadzenie rejestru operacji przetwarzania i wyznaczenie inspektora ochrony danych).

Ogólne rozporządzenie o ochronie danych i zaktualizowana konwencja nr 108 stanowią, że administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych osobowych opisanych w tym rozdziale i musi być w stanie wykazać ich przestrzeganie[325]. W tym celu administrator danych musi wdrożyć odpowiednie środki techniczne i organizacyjne[326]. Mimo że zasada rozliczalności określona w art. 5 ust. 2 RODO jest skierowana wyłącznie do administratorów, od podmiotów przetwarzających dane oczekuje się również rozliczalności, biorąc pod uwagę fakt, że muszą one wypełniać szereg obowiązków i że są one ściśle związane z rozliczalnością.

Przepisy UE i RE dotyczące ochrony danych stanowią również, że administrator jest odpowiedzialny za przestrzeganie zasad ochrony danych omówionymi w sekcjach 3.1–3.6 i powinien mieć możliwość zapewnienia przestrzegania tych zasad[327]. Grupa Robocza Art. 29 zwraca uwagę, że „rodzaj procedur i mechanizmów różniłby się w zależności od ryzyka związanego z przetwarzaniem i charakterem danych"[328].

Administratorzy mogą ułatwić spełnienie tego wymogu na różne sposoby, które obejmują:

- rejestrowanie czynności przetwarzania i udostępnianie ich na żądanie organu nadzorczego[329],

- w niektórych sytuacjach wyznaczenie inspektora ochrony danych, który jest zaangażowany we wszystkie kwestie związane z ochroną danych osobowych[330],

325 Tamże, art. 5 ust. 2, zaktualizowana konwencja nr 108, art. 10 ust. 1.

326 Ogólne rozporządzenie o ochronie danych, art. 24.

327 Tamże, art. 5 ust. 2, zaktualizowana konwencja nr 108, art. 10 ust. 1.

328 Grupa Robocza Art. 29 (2010), *Opinion 3/2010 on the principle of accountability*, WP 173, Bruksela, 13 lipca 2010 r., pkt 12.

329 Ogólne rozporządzenie o ochronie danych, art. 30.

330 Tamże, art. 37–39.

- przeprowadzanie ocen skutków dla ochrony danych w odniesieniu do rodzajów przetwarzania, które mogą powodować wysokie ryzyko dla praw i wolności osób fizycznych[331],

- zapewnienie ochrony danych w fazie projektowania i domyślnej ochrony danych[332],

- wdrożenie trybów i procedur wykonywania praw przysługujących osobom, których dane dotyczą[333],

- stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji[334].

Chociaż zasada rozliczalności określona w art. 5 ust. 2 RODO nie jest skierowana konkretnie do podmiotów przetwarzających, istnieją przepisy związane z rozliczalnością, które również nakładają na nich obowiązki, takie jak prowadzenie rejestru czynności przetwarzania i wyznaczanie inspektora ochrony danych w odniesieniu do wszelkich czynności przetwarzania, które tego wymagają[335]. Podmioty przetwarzające muszą również zapewnić wdrożenie wszystkich środków niezbędnych do zapewnienia bezpieczeństwa danych[336]. Prawnie wiążąca umowa między administratorem a podmiotem przetwarzającym musi stanowić, że podmiot przetwarzający pomaga administratorowi w spełnieniu niektórych wymogów, takich jak przeprowadzenie oceny skutków dla ochrony danych lub zgłoszenie administratorowi każdego naruszenia ochrony danych osobowych natychmiast po jego stwierdzeniu[337].

Organizacja Współpracy Gospodarczej i Rozwoju (OECD) przyjęła w 2013 r. wytyczne dotyczące prywatności, w których podkreślono, że administratorzy odgrywają ważną rolę w funkcjonowaniu ochrony danych w praktyce. W wytycznych zawarto zasadę rozliczalności w następującym brzmieniu: „administrator danych powinien

331 Tamże, art. 35, zaktualizowana konwencja nr 108, art. 10 ust. 2.

332 Ogólne rozporządzenie o ochronie danych, art. 25; zaktualizowana konwencja nr 108, art. 10 ust. 2 i 3.

333 Tamże, art. 12 i art. 24.

334 Tamże, art. 40 i art. 42.

335 Tamże, art. 5 ust. 2, art. 30 i 37.

336 Tamże, art. 28 ust. 3 lit. c).

337 Tamże, art. 28 ust. 3 lit. d).

być odpowiedzialny za stosowanie środków wdrażających [istotne] zasady wskazane powyżej”[338].

Przykład: Przykładem położenia nacisku na zasadę rozliczalności w ustawodawstwie jest dokonana w 2009 r. zmiana[339] dyrektywy 2002/58/WE o prywatności i łączności elektronicznej. Zgodnie z art. 4 w zmienionym brzmieniu dyrektywa nakłada obowiązek, by „zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych”. Tak więc w odniesieniu do przepisów bezpieczeństwa zawartych w tej dyrektywie prawodawca zdecydował, że konieczne jest wprowadzenie wyraźnego wymogu posiadania i wdrożenia polityki bezpieczeństwa.

Zgodnie z opinią Grupy Roboczej Art. 29[340] istotą rozliczalności jest obowiązek administratora w zakresie:

- wdrożenia środków, które w normalnych warunkach gwarantują przestrzeganie przepisów dotyczących ochrony danych w związku z czynnościami przetwarzania,

- sporządzenia dokumentacji, która wskazuje osobom, których dane dotyczą, oraz organom nadzorczym, jakie środki podjęto, aby zapewnić przestrzeganie przepisów dotyczących ochrony danych.

Tak więc zasada rozliczalności nakłada na administratorów obowiązek aktywnego wykazania, że przestrzegają przepisów, nie zaś czekania, aż osoby, których dane dotyczą, bądź organy nadzorcze wskażą uchybienia.

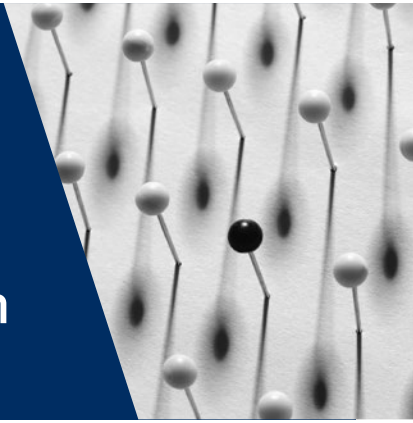
338 OECD (2013), Guidelines on governing the Protection of Privacy and transborder flows of personal data, art. 14.

339 Dyrektywa 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009, s. 11.

340 Grupa Robocza Art. 29 (2010), *Opinion 3/2010 on the principle of accountability*, WP 173, Bruksela, 13 lipca 2010 r.

4

Przepisy europejskiego prawa o ochronie danych



UE	Omówione zagadnienia	RE
Przepisy dotyczące przetwarzania danych zgodnie z prawem		
Artykuł 6 ust. 1 lit. a) ogólnego rozporządzenia o ochronie danych TSUE, C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 2011 TSUE, C-536/15, *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*, 2017	**Zgoda**	Artykuł 3.4 lit. b) i art. 3.6 Profiling Recommendation [zalecenie w sprawie profilowania] Artykuł 5 ust. 2 zaktualizowanej konwencji nr 108
Artykuł 6 ust. 1 lit. b) ogólnego rozporządzenia o ochronie danych	**Stosunek (przed) umowny**	Artykuł 3.4 lit. b) zalecenia w sprawie profilowania
Artykuł 6 ust. 1 lit. c) ogólnego rozporządzenia o ochronie danych	**Obowiązki prawne administratora danych**	Artykuł 3.4 lit. a) zalecenia w sprawie profilowania
Artykuł 6 ust. 1 lit. d) ogólnego rozporządzenia o ochronie danych	**Żywotny interes osoby, której dane dotyczą**	Artykuł 3.4 lit. b) zalecenia w sprawie profilowania
Artykuł 6 ust. 1 lit. e) ogólnego rozporządzenia o ochronie danych TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland*, 2008	**Interes publiczny i wykonywanie władzy publicznej**	Artykuł 3.4 lit. b) zalecenia w sprawie profilowania

UE	Omówione zagadnienia	RE
Artykuł 6 ust. 1 lit. f) ogólnego rozporządzenia o ochronie danych TSUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme”*, 2017 TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 2011	**Prawnie uzasadnione interesy innych osób**	Artykuł 3.4 lit. b) zalecenia w sprawie profilowania ETPC, *Y przeciwko Turcji*, nr 648/10, 2015
Artykuł 6 ust. 4 ogólnego rozporządzenia o ochronie danych	**Wyjątki od zasady ograniczenia celu: dalsze przetwarzanie w innym celu**	Artykuł 5 ust. 4 lit. b) zaktualizowanej konwencji nr 108
Przepisy dotyczące przetwarzania danych szczególnie chronionych zgodnie z prawem		
Artykuł 9 ust. 1 ogólnego rozporządzenia o ochronie danych	**Ogólny zakaz przetwarzania**	Artykuł 6 zaktualizowanej konwencji nr 108
Artykuł 9 ust. 2 ogólnego rozporządzenia o ochronie danych	**Wyjątki od ogólnego zakazu**	Artykuł 6 zaktualizowanej konwencji nr 108
Przepisy dotyczące bezpiecznego przetwarzania		
Artykuł 32 ogólnego rozporządzenia o ochronie danych	**Obowiązek zapewnienia bezpiecznego przetwarzania**	Artykuł 7 ust. 1 zaktualizowanej konwencji nr 108 ETPC, *I przeciwko Finlandii*, nr 20511/03, 2008
Artykuł 28 i art. 32 ust. 1 lit. b) ogólnego rozporządzenia o ochronie danych	**Obowiązek zachowania poufności**	Artykuł 7 ust. 1 zaktualizowanej konwencji nr 108
Artykuł 34 ogólnego rozporządzenia o ochronie danych Artykuł 4 ust. 2 dyrektywy o prywatności i łączności elektronicznej	**Zawiadomienia o naruszeniu ochrony danych**	Artykuł 7 ust. 2 zaktualizowanej konwencji nr 108

UE	Omówione zagadnienia	RE
Przepisy dotyczące rozliczalności i promowania przestrzegania przepisów		
Artykuł 12, 13 i 14 ogólnego rozporządzenia o ochronie danych	**Przejrzystość ogólnie**	Artykuł 8 zaktualizowanej konwencji nr 108
Artykuł 37, 38 i 39 ogólnego rozporządzenia o ochronie danych	**Inspektorzy ochrony danych**	Artykuł 10 ust. 1 zaktualizowanej konwencji nr 108
Artykuł 30 ogólnego rozporządzenia o ochronie danych	**Rejestry czynności przetwarzania**	
Artykuł 35 i 36 ogólnego rozporządzenia o ochronie danych	**Ocena skutków i uprzednie konsultacje**	Artykuł 10 ust. 2 zaktualizowanej konwencji nr 108
Artykuł 33 i 34 ogólnego rozporządzenia o ochronie danych	**Zgłoszenia naruszeń ochrony danych**	Artykuł 7 ust. 2 zaktualizowanej konwencji nr 108
Artykuł 40 i 41 ogólnego rozporządzenia o ochronie danych	**Kodeksy postępowania**	
Artykuł 42 i 43 ogólnego rozporządzenia o ochronie danych	**Certyfikacja**	
Ochrona danych w fazie projektowania oraz domyślna ochrona danych		
Artykuł 25 ust. 1 ogólnego rozporządzenia o ochronie danych	**Ochrona danych w fazie projektowania**	Artykuł 10 ust. 2 zaktualizowanej konwencji nr 108
Artykuł 25 ust. 2 ogólnego rozporządzenia o ochronie danych	**Domyślna ochrona danych**	Artykuł 10 ust. 3 zaktualizowanej konwencji nr 108

Zasady mają z konieczności charakter ogólny. Ich zastosowanie w konkretnych sytuacjach pozostawia pewien margines dla interpretacji i wyboru użytych środków. Na mocy **prawa RE** strony zaktualizowanej konwencji nr 108 powinny doprecyzować ów margines interpretacji w swoim prawie krajowym. W **prawie UE** sytuacja przedstawia się inaczej: aby zapewnić ochronę danych na rynku wewnętrznym, za niezbędne uznano wprowadzenie bardziej szczegółowych przepisów już na szczeblu UE, aby ujednolicić poziom ochrony danych w ustawodawstwie krajowym państw członkowskich. W ogólnym rozporządzeniu o ochronie danych ustanowiono, zgodnie z zasadami określonymi w art. 5, szczegółowe przepisy, które obowiązują bezpośrednio w krajowym porządku prawnym. Poniższe uwagi na temat szczegółowych przepisów dotyczących ochrony danych na szczeblu europejskim dotyczą zatem przede wszystkim prawa UE.

4.1. Zasady przetwarzania danych zgodnie z prawem

Najważniejsze kwestie

- Dane osobowe mogą być przetwarzane zgodnie z prawem, jeżeli spełniają jedno z następujących kryteriów:
  - przetwarzanie następuje na podstawie zgody osoby, której dane dotyczą,
  - stosunek umowny wymaga przetwarzania danych osobowych,
  - przetwarzanie danych jest konieczne dla wypełnienia obowiązku prawnego, któremu administrator danych podlega,
  - przetwarzania danych wymagają żywotne interesy osób, których dane dotyczą, lub innych osób,
  - przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym,
  - przyczyną przetwarzania danych są uzasadnione interesy administratorów lub stron trzecich, jednak tylko jeżeli nie mają wobec nich charakteru nadrzędnego interesy lub podstawowe prawa i wolności osób, których dane dotyczą.
- Przetwarzanie szczególnie chronionych danych osobowych zgodnie z prawem podlega szczególnym, bardziej restrykcyjnym przepisom.

4.1.1. Zgodne z prawem podstawy przetwarzania danych

W rozdziale II ogólnego rozporządzenia o ochronie danych, zatytułowanym „Zasady", stwierdza się, że wszystkie czynności przetwarzania danych osobowych muszą być zgodne, po pierwsze, z zasadami dotyczącymi jakości danych określonymi w art. 5 RODO. Jedna z zasad przewiduje, że dane osobowe powinny być „przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty". Po drugie, aby dane przetwarzane były zgodnie z prawem, przetwarzanie musi być zgodne z jedną

ze zgodnych z prawem podstaw przetwarzania danych wymienionych w art. 6[341] w przypadku danych osobowych niepodlegających szczególnej ochronie oraz w art. 9 w przypadku szczególnych kategorii danych (lub danych szczególnie chronionych). Podobnie rozdział II zaktualizowanej konwencji nr 108, w którym określono „podstawowe zasady ochrony danych osobowych", przewiduje, że aby przetwarzanie danych było zgodne z prawem, musi ono być „proporcjonalne w stosunku do zamierzonego zgodnego z prawem celu".

Niezależnie od zgodnej z prawem podstawy przetwarzania, na której opiera się administrator przy inicjowaniu operacji przetwarzania danych osobowych, będzie on również musiał zastosować zabezpieczenia przewidziane w ogólnym systemie prawa ochrony danych.

Zgoda

W prawie RE art. 5 ust. 2 zaktualizowanej konwencji nr 108 zawiera odniesienia do zgody. Wspomniano o niej także w orzecznictwie ETPC i w kilku zaleceniach RE[342]. **W prawie UE** zgoda jako podstawa zgodnego z prawem przetwarzania danych ma silne podstawy w art. 6 RODO i jest również wyraźnie określona w art. 8 karty. Charakterystykę ważnej zgody wyjaśniono w definicji zgody zawartej w art. 4, natomiast warunki uzyskania ważnej zgody wyszczególniono w art. 7, a szczególne zasady dotyczące zgody dziecka w odniesieniu do usług społeczeństwa informacyjnego określono w art. 8 RODO.

Jak wyjaśniono w sekcji 2.4, zgoda musi być wyrażona w sposób dobrowolny, świadomy, konkretny i jednoznaczny. Zgoda musi być wyrażona w formie wyraźnego działania potwierdzającego zgodę na przetwarzanie danych i może zostać odwołana przez osobę, której dane dotyczą, w każdej chwili. Administratorzy mają obowiązek prowadzenia możliwych do zweryfikowania rejestrów zgód.

341 TSUE, sprawy połączone C-465/00, C-138/01 i C-139/01, *Rechnungshof przeciwko* Österreichischer *Rundfunk i in.* oraz *Christa Neukomm i Jospeh Lauermann przeciwko Österreichischer Rundfunk*, 20 maja 2003 r., pkt 65, TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r., pkt 48; TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* oraz *Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r., pkt 26.

342 Zob. na przykład Rada Europy, Komitet Ministrów (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to the Member States on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 listopada 2010 r., art. 3.4 lit. b).

Dobrowolna zgoda

W ramach **RE** w zaktualizowanej konwencji nr 108 zgoda osoby, której dane dotyczą, musi „stanowić swobodę wyrażania świadomego wyboru”[343]. O dobrowolnej zgodzie można mówić tylko, „jeżeli osoba, której dane dotyczą, ma możliwość dokonania rzeczywistego wyboru, przy czym nie zachodzi ryzyko wprowadzenia w błąd, zastraszenia, przymusu lub znaczących negatywnych konsekwencji, jeśli nie wyrazi zgody”[344]. W tym względzie **prawo UE** stanowi, że zgoda nie jest uważana za udzieloną dobrowolnie „jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez negatywnych konsekwencji”[345]. W RODO podkreśla się, że „[o]ceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy”[346]. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 stwierdzono, że „osoba, której dane dotyczą, nie może być poddana, bezpośrednio lub pośrednio, bezprawnym naciskom lub presji (która może mieć charakter gospodarczy lub inny), a zgody nie należy uznawać za dobrowolną, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego wyboru lub nie może odmówić udzielenia zgody ani jej cofnąć bez konsekwencji”[347].

Przykład: Niektóre gminy w państwie A postanowiły opracować karty pobytu z wbudowanym chipem. Nabycie tych kart elektronicznych przez mieszkańców nie jest obowiązkowe. Mieszkańcy nieposiadający karty nie mają jednak dostępu do szeregu ważnych usług administracyjnych, takich jak możliwość płacenia podatków miejskich przez Internet, składania skarg drogą elektroniczną, korzystając z trzydniowego terminu na udzielenie odpowiedzi, a nawet omijania kolejek, kupowania biletów zniżkowych do miejskiej hali koncertowej i korzystania z czytników w wejściu.

343 Explanatory Report of Modernised Convention 108, pkt 42.

344 Zob. także Grupa Robocza Art. 29 (2011), *Opinion 15/2011 on the notion of consent*, WP 187, Bruksela, 13 lipca 2011 r., s. 12.

345 Ogólne rozporządzenie o ochronie danych, motyw 42.

346 Tamże, art. 7 ust. 4.

347 Explanatory Report of Modernised Convention 108, pkt 42.

Przetwarzanie danych osobowych przez gminy w tym przykładzie nie może być oparte na zgodzie. Ponieważ istnieje przynajmniej pośrednia presja na mieszkańców, aby uzyskali kartę elektroniczną i wyrazili zgodę na przetwarzanie, zgoda nie jest udzielana dobrowolnie. Opracowanie przez gminy systemu kart elektronicznych powinno zatem opierać się na innej prawnie uzasadnionej podstawie uzasadniającej przetwarzanie danych. Gminy mogłyby się na przykład powołać na fakt, że przetwarzanie jest konieczne do realizacji zadania wykonywanego w interesie publicznym, co stanowi zgodną z prawem podstawę przetwarzania na gruncie art. 6 ust. 1 lit. e) RODO[348].

Dobrowolny charakter zgody może również budzić wątpliwości w sytuacjach podporządkowania, w których występuje znaczna nierównowaga ekonomiczna lub inna między starającym się o zgodę administratorem a udzielającą jej osobą, której dane dotyczą[349]. Typowym przykładem takiej nierównowagi i podporządkowania jest przetwarzanie przez pracodawcę danych osobowych w kontekście stosunku pracy. Według Grupy Roboczej Art. 29 „Pracownicy praktycznie nigdy nie są w stanie dobrowolnie udzielić zgody, odmówić zgody ani cofnąć zgody, z uwagi na zależność wynikającą ze stosunku pracy między pracodawcą a pracownikiem. Z powodu tej nierównowagi sił pracownicy mogą udzielić dobrowolnej zgody wyłącznie w wyjątkowych okolicznościach, w których przyjęcie lub odrzucenie propozycji nie pociąga za sobą żadnych konsekwencji "[350].

Przykład: Duże przedsiębiorstwo planuje stworzyć spis zawierający nazwiska wszystkich pracowników, ich stanowiska i służbowe dane kontaktowe – wyłącznie w celu usprawnienia komunikacji wewnętrznej firmy. Kierownik działu kadr proponuje zamieścić w spisie zdjęcia wszystkich pracowników,

348 Grupa Robocza Art. 29 (2011), *Opinion 15/2011 on the definition of consent*, WP 187, Bruksela, 13 lipca 2011 r., s. 16. Dalsze przykłady przypadków, w których przetwarzanie danych nie może być oparte na zgodzie, lecz wymaga innej podstawy prawnej dla uzasadnienia przetwarzania, można znaleźć na s. 14 i 17 opinii.

349 Zob. także Grupa Robocza Art. 29 (2001), *Opinion 8/2001 on the processing of personal data in the employment context*, WP 48, Bruksela, 13 września 2001 r., Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1) dyrektywy 95/46/WE z dnia 24 października 1995 r.*, WP 114, Bruksela, 25 listopada 2005 r., Grupa Robocza Art. 29 (2017), *Opinion 2/2017 on data processing at work*, WP 249, Bruksela, 8 czerwca 2017 r.

350 Grupa Robocza Art. 29 (2017), *Opinion 2/2017 on data processing at work*, WP 249, Bruksela, 8 czerwca 2017 r.

aby ułatwić rozpoznawanie współpracowników podczas spotkań. Przedstawiciele pracowników domagają się, aby było to uzależnione od zgody poszczególnych pracowników.

W tej sytuacji zgodę pracownika należy uznać za podstawę prawną przetwarzania zdjęć w spisie, gdyż jest wiarygodne, że niezależnie od tego, czy pracownik zgodzi się na zamieszczenie zdjęcia w spisie czy też nie, nie będzie to miało dla niego negatywnych konsekwencji .

Przykład: Przedsiębiorstwo A planuje spotkanie trzech swoich pracowników z dyrektorami przedsiębiorstwa B w celu przedyskutowania potencjalnej przyszłej współpracy przy projekcie. Spotkanie odbędzie się w siedzibie przedsiębiorstwa B, które wymaga od przedsiębiorstwa A wysłania pocztą elektroniczną nazwisk, życiorysów i zdjęć uczestników spotkania. Przedsiębiorstwo B twierdzi, że potrzebuje imion i nazwisk oraz zdjęć uczestników, aby umożliwić pracownikom ochrony przy wejściu do budynku sprawdzenie, czy są to właściwe osoby, podczas gdy życiorysy pozwolą dyrektorom lepiej przygotować się do spotkania. W takim przypadku przekazanie danych osobowych pracowników przez przedsiębiorstwo A nie może być oparte na zgodzie. Zgody nie można uznać za „dobrowolną", ponieważ istnieje możliwość, że pracownicy mogą ponieść negatywne konsekwencje w przypadku odrzucenia oferty (na przykład mogą zostać zastąpieni przez innego współpracownika nie tylko podczas udziału w spotkaniu, ale również w kontaktach z przedsiębiorstwem B i ogólnie w pracach związanych z realizacją projektu). Dlatego też przetwarzanie musi opierać się na innej podstawie prawnej przetwarzania danych.

Nie oznacza to jednak, że zgoda nigdy nie może być ważna w sytuacji, gdy brak zgody miałby negatywne konsekwencje. Na przykład, jeżeli brak zgody na wydanie karty stałego klienta supermarketu skutkuje jedynie nieuzyskaniem niewielkich rabatów na pewne towary, zgoda pozostaje ważną podstawą prawną przetwarzania danych osobowych tych klientów, którzy wyrazili zgodę na wydanie im takiej karty. Nie występuje tutaj sytuacja podporządkowania między przedsiębiorstwem a klientem, a konsekwencje braku zgody nie są wystarczająco poważne dla osoby, której dane dotyczą, aby uniemożliwić wolny wybór (o ile obniżka ceny jest wystarczająco niewielka, aby nie wpływała na ich wolny wybór).

Jednak w przypadku gdy towary lub usługi można uzyskać wyłącznie pod warunkiem ujawnienia pewnych danych osobowych administratorowi lub dalej stronom trzecim, zgody osoby, której dane dotyczą, na ujawnienie jej danych, która nie jest niezbędna do zawarcia umowy, nie można zwykle uznać za decyzję dobrowolną, zatem zgoda taka nie jest ważna na mocy prawa o ochronie danych[351]. W RODO dość surowo zabrania się łączenia zgody z dostawą towarów i usług[352].

Przykład: Zgoda wyrażona przez pasażerów na przekazywanie przez linie lotnicze danych dotyczących przelotu pasażera (PNR), które zawierają informacje o tożsamości, nawykach żywieniowych bądź problemach zdrowotnych, władzom imigracyjnym konkretnego kraju, nie może zostać uznana za ważną zgodę na mocy prawa o ochronie danych, gdyż pasażerowie nie mają wyboru, jeżeli chcą odwiedzić ten kraj. Jeżeli takie dane mają zostać przekazane zgodnie z prawem, niezbędna jest podstawa prawna inna niż zgoda; zazwyczaj jest to specjalna ustawa.

Świadoma zgoda

Osoba, której dane dotyczą, musi dysponować wystarczającymi informacjami przed podjęciem decyzji. Zazwyczaj świadoma zgoda wymaga przedstawienia dokładnego i łatwo zrozumiałego opisu tego, czego dotyczy wymagana zgoda. Jak wyjaśnia Grupa Robocza Art. 29, zgoda musi opierać się na uznaniu i zrozumieniu okoliczności faktycznych oraz konsekwencji działania osoby, której dane dotyczą, polegającego na udzieleniu zgody na przetwarzanie danych. Wobec tego „danej osobie należy jasno i zrozumiale przekazać dokładne i pełne informacje dotyczące wszystkich stosownych kwestii [...], m.in. odnoszących się do charakteru przetwarzanych danych, celów przetwarzania, odbiorców możliwych transferów danych oraz praw osoby, której dane dotyczą”[353]. Aby można było uznać zgodę za świadomą, osoby fizyczne muszą być również świadome konsekwencji nieudzielenia zgody na przetwarzanie danych.

Ze względu na znaczenie świadomej zgody RODO i sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108 miały na celu wyjaśnienie tego pojęcia. Zgodnie

351 Ogólne rozporządzenie o ochronie danych, art. 7 ust. 4.

352 Tamże.

353 Grupa Robocza Art. 29 (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Bruksela, 15 lutego 2007 r.

z motywami RODO świadoma zgoda oznacza, że „osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych”[354].

W wyjątkowym przypadku zgody wykorzystanej jako odstępstwo w celu zapewnienia podstawy prawnej dla międzynarodowego przekazania danych, aby zgoda ta została uznana za ważną administrator musi poinformować osobę, której dane dotyczą, o możliwym ryzyku związanym z takim przekazaniem, ze względu na brak decyzji stwierdzającej odpowiedni poziom ochrony i odpowiednich zabezpieczeń[355].

W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 stwierdza się, że należy udzielić informacji na temat skutków decyzji osoby, której dane dotyczą, a mianowicie „co pociąga za sobą fakt wyrażenia zgody i w jakim zakresie jest ona udzielana”[356].

Ważnym aspektem jest jakość informacji. Jakość informacji oznacza, że język, w jakim podawane są informacje, należy dostosować do możliwych do przewidzenia odbiorców. Informacje muszą być podawane bez żargonu, jasnym i prostym języku, który powinien być zrozumiały dla zwykłego użytkownika[357]. Informacje muszą być również łatwo dostępne dla osoby, której dane dotyczą, i mogą być przekazane ustnie lub na piśmie. Dostępność i widoczność informacji są ważnymi elementami: informacje muszą być wyraźnie widoczne i wyeksponowane. W środowisku online dobrym rozwiązaniem mogą być wielowarstwowe powiadomienia informacyjne, ponieważ umożliwiają one osobom, których dane dotyczą, wybór między dostępem do zwięzłych lub bardziej obszernych wersji informacji.

Konkretna zgoda

Aby zgoda była ważna, musi też być konkretna w świetle celu przetwarzania, który musi być opisany w sposób jasny i jednoznaczny. Ma to ścisły związek z jakością informacji na temat celu, w którym ma być wyrażona zgoda. W tym kontekście znaczenie mają racjonalne oczekiwania przeciętnej osoby, której dane dotyczą. Osobę, której dane dotyczą, trzeba ponownie poprosić o zgodę, jeżeli zakres czynności

354 Ogólne rozporządzenie o ochronie danych, motyw 42.

355 Tamże, art. 49 ust. 1 lit. a).

356 Explanatory Report of Modernised Convention 108, pkt 42.

357 Grupa Robocza Art. 29 (2011), *Opinion 15/2011 on the definition of consent*, WP 187, 13 lipca 2011 r., s. 19.

przetwarzania ma zostać poszerzony lub mają one ulec zmianie w sposób, którego nie można było racjonalnie przewidzieć w chwili udzielania pierwotnej zgody, i tym samym prowadzi to do zmiany celu. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele[358].

Przykłady: W sprawie *Deutsche Telekom AG*[359] TSUE zajął się zagadnieniem, czy usługodawca telekomunikacyjny, który musiał przekazać dane osobowe abonentów w celu umieszczenia ich w spisach abonentów, potrzebował ponownej zgody osób, których dane dotyczą, gdyż w chwili udzielania pierwotnej zgody nie podano odbiorców danych[360].

Trybunał Sprawiedliwości orzekł, że na gruncie art. 12 dyrektywy o prywatności i łączności elektronicznej ponowna zgoda przed przekazaniem danych nie była niezbędna. Z uwagi na to, że osoby, których dane dotyczą, miały jedynie możliwość wyrażenia zgody na cel przetwarzania, którym była publikacja ich danych, nie mogły wybrać spisów, w których te dane mogą być publikowane.

Jak podkreślił TSUE „z wykładni kontekstualnej i systemowej art. 12 dyrektywy o prywatności i łączności elektronicznej wynika, że zgoda, o której mowa w ust. 2 tego artykułu, odnosi się do celu publikacji danych osobowych w publicznym spisie abonentów, nie zaś do tożsamości konkretnego dostawcy tego spisu"[361]. Ponadto „samo opublikowanie danych osobowych w spisie mającym szczególne przeznaczenie" – a nie kwestia tożsamości publikującego – „może okazać się dla abonenta niekorzystne"[362].

Sprawa *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*[363] dotyczyła wniosku belgijskiej spółki oferującej usługi biura numerów i spisu abonentów skierowanego do przedsiębiorstw,

358 Ogólne rozporządzenie o ochronie danych, motyw 32.

359 TSUE, C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 5 maja 2011 r. Zob. w szczególności pkt 53 i 54.

360 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.U. L 201 z 31.7.2002 (dyrektywa o prywatności i łączności elektronicznej).

361 TSUE, C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 5 maja 2011 r., pkt 61.

362 Tamże, pkt 62.

363 TSUE, C-536/15, *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*, 15 marca 2017 r.

które przypisują numery telefoniczne abonentom, o udostępnienie jej danych dotyczących tych abonentów. Spółka belgijska powołała się na obowiązek wynikający z dyrektywy o usłudze powszechnej[364]. Dyrektywa ta nakłada na przedsiębiorstwa, które przypisują numery telefoniczne abonentom, obowiązek udostępnienia tych numerów wnioskodawcom do celów świadczenia usług biura numerów, jeżeli abonenci wyrazili zgodę na opublikowanie swoich numerów. Przedsiębiorstwa niderlandzkie odmówiły ich udostępnienia, podnosząc, że nie były zobowiązane do przekazania spornych danych przedsiębiorstwu mającemu siedzibę w innym państwie członkowskim. Przedsiębiorstwa argumentowały, że użytkownicy wyrazili zgodę na opublikowanie swoich numerów przy założeniu, że zostałyby opublikowane w niderlandzkim spisie abonentów. Trybunał orzekł, że dyrektywa o usłudze powszechnej obejmuje swoim zakresem wszystkie wnioski skierowane przez przedsiębiorstwa oferujące usługi spisu abonentów, niezależnie od tego, w jakim państwie członkowskim mają one swoją siedzibę. Trybunał orzekł również, że przekazanie tych samych danych innemu przedsiębiorstwu w celu opublikowania publicznego spisu abonentów bez ponownego uzyskania zgody abonentów nie może naruszać istoty prawa do ochrony danych osobowych[365]. W konsekwencji, przedsiębiorstwo przypisujące numery telefoniczne swoim abonentom nie ma obowiązku dokonywania rozróżnienia w zakresie formułowania swojego wniosku o wyrażenie zgody skierowanego do abonenta w zależności od państwa członkowskiego, do którego dotyczące go dane mogą zostać przekazane[366].

Jednoznaczna zgoda

Każda zgoda musi być udzielona w sposób jednoznaczny[367]. Oznacza to, że nie powinno być żadnych uzasadnionych wątpliwości, że osoba, której dane dotyczą, chciała wyrazić zgodę na przetwarzanie jej danych. Na przykład niepodjęcie działania przez osobę, której dane dotyczą, nie stanowi jednoznacznej zgody.

364 Dyrektywa 2002/22/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników (dyrektywa o usłudze powszechnej), Dz.U. L 108 z 24.4.2002, s. 51, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. (dyrektywa o usłudze powszechnej), Dz.U. L 337 z 18.12.2009, s. 11.

365 TSUE, C-536/15, *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*, 15 marca 2017 r., pkt 36.

366 Tamże, pkt 40-41.

367 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 11.

Taka sytuacja ma miejsce w przypadku uzyskania przez administratora danych zgody na przetwarzanie danych osobowych za pomocą oświadczeń zawartych w jego polityce prywatności, takich jak: „korzystając z naszego serwisu, wyrażają Państwo zgodę na przetwarzanie Państwa danych osobowych". W takim przypadku administratorzy mogą być zmuszeni do zapewnienia, aby użytkownicy ręcznie i indywidualnie wyrażali zgodę na tego rodzaju politykę.

Jeżeli udzielenie zgody odbywa się w formie pisemnej i jest częścią umowy zgoda na przetwarzanie danych osobowych powinna być zindywidualizowana, a w każdym razie „powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu"[368].

Wymogi dotyczące zgody udzielanej przez dzieci

Ogólne rozporządzenie o ochronie danych przewiduje szczególną ochronę dla dzieci w kontekście świadczenia usług społeczeństwa informacyjnego, gdyż „mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych"[369]. Wobec tego w **prawie UE**, gdy dostawcy usług społeczeństwa informacyjnego przetwarzają dane osobowe dzieci poniżej 16. roku życia na podstawie zgody, przetwarzanie takie będzie zgodne z prawem „wyłącznie w przypadkach, gdy zgodę wyraziła lub zaaprobowała osoba sprawująca władzę rodzicielską lub opiekę nad dzieckiem oraz wyłącznie w zakresie wyrażonej zgody"[370]. Państwa członkowskie mogą przewidzieć w swoim prawie niższą granicę wiekową, lecz nie niższą niż 13 lat[371]. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie jest konieczna „w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku"[372]. Informacje i komunikaty w przypadku gdy przetwarzanie dotyczy dziecka powinny być sformułowane jasnym i prostym językiem, łatwym do zrozumienia dla dziecka[373].

368 Tamże, motyw 42.

369 Tamże, motyw 38.

370 Tamże, art. 8 ust. 1 tiret pierwsze. Pojęcie usług społeczeństwa informacyjnego zdefiniowano w art. 4 pkt 25 ogólnego rozporządzenia o ochronie danych.

371 Ogólne rozporządzenie o ochronie danych, art. 8 ust. 1 tiret pierwsze.

372 Tamże, motyw 38.

373 Tamże, motyw 58. Zob. także zaktualizowana konwencja nr 108, art. 15 ust. 2. Explanatory Report of Modernised Convention 108, pkt 68 i 125.

Prawo do wycofania zgody w dowolnym momencie

Ogólne rozporządzenie o ochronie danych przewiduje ogólne prawo do wycofania zgody w dowolnym momencie[374]. Osoba, której dane dotyczą, musi zostać poinformowana o takim prawie przed wyrażeniem zgody i może z niego skorzystać według własnego uznania. Nie powinno być wymagane uzasadnienie wycofania zgody i nie powinno się z nim wiązać ryzyko niekorzystnych konsekwencji wychodzących poza utratę wszelkich korzyści wynikających z wyrażonej wcześniej zgody na wykorzystanie danych. Wycofanie zgody musi być równie łatwe jak jej wyrażenie[375]. Nie można mówić o dobrowolnej zgodzie, jeżeli osoba, której dane dotyczą, nie ma możliwości wycofania swojej zgody bez niekorzystnych konsekwencji[376].

Przykład: Klient zgadza się otrzymywać wiadomości promocyjne na adres, który podaje administratorowi danych. Jeżeli klient wycofa zgodę, administrator musi natychmiast zaprzestać wysyłania wiadomości promocyjnych. Nie powinien przy tym nakładać kar, na przykład opłat. Wycofanie jest jednak stosowane w odniesieniu do przyszłości i nie ma mocy wstecznej. Okres, w którym dane osobowe klienta były przetwarzane zgodnie z prawem – za jego zgodą – był prawnie uzasadniony. Wycofanie uniemożliwia dalsze przetwarzanie tych danych, chyba że jest ono zgodne z prawem do ich usunięcia[377].

Konieczność w celu wykonania umowy

W prawie UE art. 6 ust. 1 lit. b) RODO przewiduje kolejną podstawę prawnie uzasadnionego przetwarzania, mianowicie jeżeli jest to „niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą". Przepis ten obejmuje także stosunki przedumowne. Może chodzić o sytuacje gdy strona zamierza zawrzeć umowę, ale jeszcze tego nie uczyniła, na przykład ze względu na konieczność sprawdzenia pewnych kwestii. Jeżeli jedna ze stron musi przetwarzać w tym celu dane, takie

374 Ogólne rozporządzenie o ochronie danych, art. 7 ust. 3. Explanatory Report of Modernised Convention 108, pkt 45.

375 Ogólne rozporządzenie o ochronie danych, art. 7 ust. 3.

376 Ogólne rozporządzenie o ochronie danych, motyw 42; Explanatory Report of Modernised Convention 108, pkt 42.

377 Ogólne rozporządzenie o ochronie danych, art. 17 ust. 1 lit. b).

przetwarzanie jest zgodne z prawem, jeżeli jest to „niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy”[378].

Pojęcie przetwarzania danych jako „uzasadnionej podstawy przewidzianej ustawą” w art. 5 ust. 2 zaktualizowanej konwencji nr 108 obejmuje swoim zakresem także „przetwarzanie danych w celu wykonania umowy (lub środki przedumowne na żądanie osoby, której dane dotyczą), której stroną jest osoba, której dane dotyczą”[379].

Obowiązki prawne administratora danych

W **prawie UE** określono kolejne kryterium przetwarzania danych zgodnie z prawem, a mianowicie jeżeli jest ono „niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze” (art. 6 ust. 1 lit. c) RODO). Przepis ten odnosi się do administratorów działających zarówno w sektorze prywatnym, jak i publicznym; obowiązki prawne administratorów danych z sektora publicznego określono w art. 6 ust. 1 lit. e) RODO. Istnieje wiele przypadków, w których administratorzy z sektora prywatnego mają obowiązek prawny przetwarzania danych na temat konkretnych osób, których dane dotyczą. Na przykład pracodawcy muszą przetwarzać dane o swoich pracownikach do celów ubezpieczeń społecznych i do celów podatkowych, a przedsiębiorstwa muszą przetwarzać dane swoich klientów do celów podatkowych.

Źródłem obowiązku prawnego może być prawo Unii lub prawo państwa członkowskiego, które mogłoby stanowić podstawę dla jednej lub więcej operacji przetwarzania. Prawo powinno określać cel przetwarzania, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania[380]. Każde takie prawo, które stanowi podstawę przetwarzania danych osobowych, musi być zgodne zarówno z art. 7 i 8 karty, jak i z art. 8 EKPC.

378 Tamże, art. 6 ust. 1 lit. b).

379 Explanatory Report of Modernised Convention 108, pkt 46, Rada Europy, Komitet Ministrów (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Profiling Recommendation), 23 listopada 2010 r., art. 3.4 lit. b).

380 Ogólne rozporządzenie o ochronie danych, motyw 45.

Zobowiązania prawne administratora stanowią podstawę przetwarzania danych zgodnie z prawem także **w prawie RE**[381]. Jak wcześniej wspomniano, obowiązki prawne administratora z sektora prywatnego są tylko jednym konkretnym przypadkiem uzasadnionego interesu innych, jak wspomniano w art. 8 ust. 2 EKPC. Przykład pracodawców przetwarzających dane dotyczące swoich pracowników jest także istotny z punktu widzenia prawa RE.

Żywotne interesy osoby, której dane dotyczą, lub interesy innej osoby fizycznej

W prawie UE, w art. 6 ust. 1 lit. d) RODO stwierdza się, że przetwarzanie danych osobowych jest zgodne z prawem, jeżeli „jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej". Tę prawnie uzasadnioną przesłankę można powołać wyłącznie w celu przetwarzania danych osobowych w oparciu o żywotne interesy innej osoby fizycznej, jeżeli „ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej"[382]. Czasami dany rodzaj przetwarzania może służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, lub interesom innej osoby. Taka sytuacja ma miejsce, na przykład, w czasie monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych.

W prawie RE, w art. 8 EKPC nie wspomina się o żywotnych interesach osoby, której dane dotyczą. Żywotne interesy osoby, której dane dotyczą, najwyraźniej uznaje się za dorozumiane w pojęciu „prawnie uzasadnionej podstawy" z art. 5 ust. 2 zaktualizowanej konwencji nr 108, który dotyczy prawnego uzasadnienia przetwarzania danych[383].

Interes publiczny i wykonywanie władzy publicznej

Ze względu na wiele możliwych sposobów zorganizowania spraw publicznych art. 6 ust. 1 lit. e) RODO stanowi, że przetwarzanie danych osobowych zgodnie z prawem jest możliwe, jeżeli „jest niezbędne do wykonania zadania realizowanego

381 Rada Europy, Komitet Ministrów (2010), Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling (Profiling Recommendation), 23 listopada 2010 r., art. 3.4 lit. a).

382 Ogólne rozporządzenie o ochronie danych, motyw 46.

383 Explanatory Report of Modernised Convention 108, pkt 46.

w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi [...]"[384].

Przykład: W sprawie *Huber przeciwko Bundesrepublik Deutschland*[385] zamieszkały w Niemczech obywatel austriacki zażądał, aby Federalny Urząd ds. Migracji i Uchodźców usunął dane na jego temat z Centralnego Rejestru Cudzoziemców („AZR"). Rejestr ten, zawierający dane osobowe niebędących obywatelami niemieckimi obywateli UE, którzy mieszkają w Niemczech dłużej niż przez trzy miesiące, jest wykorzystywany do celów statystycznych oraz przez organy ścigania i wymiaru sprawiedliwości podczas dochodzeń i ścigania czynów przestępczych lub zagrażających bezpieczeństwu publicznemu. Sąd odsyłający zadał pytanie, czy przetwarzanie danych osobowych w ramach rejestru, takiego jak Centralny Rejestr Cudzoziemców, do którego dostęp mają również inne organy publiczne, jest zgodne z prawem UE, biorąc pod uwagę, że nie istnieje taki rejestr dotyczący obywateli niemieckich.

Trybunał Sprawiedliwości orzekł, że na mocy art. 7 lit. e) dyrektywy 95/46[386] dane osobowe mogą być przetwarzane zgodnie z prawem tylko, jeżeli jest to niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej.

Według Trybunału „zważywszy na cel polegający na zapewnieniu jednolitego poziomu ochrony we wszystkich państwach członkowskich, pojęcie konieczności w rozumieniu art. 7 lit. e) dyrektywy 95/46[387] [...] nie może mieć różnego zakresu w poszczególnych państwach członkowskich. Mamy tutaj zatem do czynienia z autonomicznym pojęciem prawa wspólnotowego, którego wykładnia winna w pełni odpowiadać celowi tej dyrektywy sformułowanemu w jej art. 1 ust. 1"[388].

384 Zob. ogólne rozporządzenie o ochronie danych, motyw 45.

385 TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r.

386 Poprzednia dyrektywa o ochronie danych, art. 7 lit. e), obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. e).

387 Tamże.

388 TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r., pkt 52.

Trybunał zauważa, że prawo do swobodnego przemieszczania się obywatela Unii na terytorium państwa członkowskiego, którego nie jest obywatelem, nie jest bezwarunkowe, lecz może podlegać ograniczeniom i warunkom przewidzianym przez Traktat ustanawiający Wspólnotę Europejską oraz przepisy przyjęte w celu jego wykonania. Zatem o ile korzystanie przez państwo członkowskie z rejestru takiego jak AZR w celu wspomagania organów właściwych do stosowania przepisów dotyczących prawa pobytu jest co do zasady zgodne z prawem, taki rejestr nie może zawierać żadnych innych informacji poza tymi, które są konieczne do tego konkretnego celu. Trybunał stwierdził, że taki system przetwarzania danych osobowych jest zgodny z prawem UE, jeżeli zawiera wyłącznie dane konieczne do stosowania tych przepisów oraz jeżeli jego scentralizowany charakter pozwala na bardziej skuteczne stosowanie tych przepisów. Sąd krajowy powinien zbadać, czy te warunki zostały spełnione w tym konkretnym przypadku. W przeciwnym wypadku przechowywanie i przetwarzanie danych osobowych w ramach rejestru takiego jak AZR do celów statystycznych nie może na żadnej podstawie zostać uznane za konieczne w rozumieniu art. 7 lit. e)[389] dyrektywy 95/46/WE[390].

Wreszcie, jeżeli chodzi o kwestię wykorzystania danych zawartych w rejestrze w celu zwalczania przestępczości, Trybunał stwierdza, że ma ono na celu „w sposób konieczny ściganie popełnionych zbrodni i przestępstw, niezależnie od przynależności państwowej osób, które ich się dopuściły". Rejestr, którego dotyczy sprawa, nie zawiera danych osobowych odnoszących się do obywateli danego państwa członkowskiego, i ta różnica w traktowaniu stanowi dyskryminację zakazaną przez art. 18 TFUE. W związku z tym ten przepis, zgodnie z wykładnią Trybunału, „stoi [...] na przeszkodzie ustanowieniu przez państwo członkowskie w celu zwalczania przestępczości szczególnego systemu przetwarzania danych osobowych dla obywateli Unii niebędących obywatelami tego państwa członkowskiego"[391].

389 Poprzednia dyrektywa o ochronie danych, art. 7 lit. e), obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. e).

390 TSUE, C-524/06, *Heinz Huber przciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r., pkt 54, 58–59 i 66–68.

391 Tamże, pkt 78 i 81.

Wykorzystywanie danych osobowych przez organy publiczne podlega także art. 8 **ETPC** i, gdy to właściwe, powinno podlegać art. 5 ust. 2 zaktualizowanej konwencji nr 108[392].

Uzasadnione interesy administratora lub strony trzeciej

W **prawie UE** osoba, której dane dotyczą, nie jest jedynym podmiotem posiadającym uzasadnione interesy. Artykuł 6 ust. 1 lit. f) RODO stanowi, że dane osobowe mogą być przetwarzane zgodnie z prawem, jeżeli jest ono „niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią [z wyjątkiem organów publicznych w ramach realizacji swoich zadań], którym ujawnia się dane, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony [...]"[393].

Stwierdzenie istnienia prawnie uzasadnionego interesu wymaga dokładnej oceny w każdym konkretnym przypadku[394]. W przypadku zidentyfikowania uzasadnionych interesów administratora danych należy dokonać wyważenia między tymi interesami a interesami lub podstawowymi prawami i wolnościami osoby, której dane dotyczą[395]. Podczas takiej oceny należy wziąć pod uwagę rozsądne oczekiwania osoby, której dane dotyczą, aby ustalić, czy interesy administratora są nadrzędne w stosunku do interesów lub praw podstawowych osoby, której dane dotyczą[396]. Jeżeli prawa osoby, której dane dotyczą, są nadrzędne wobec prawnie uzasadnionych interesów administratora danych, może on podjąć środki i wdrożyć zabezpieczenia w celu zminimalizowania wpływu na prawa osoby, której dane dotyczą, (takie jak pseudonimizacja danych) i odwrócenia „równowagi", zanim będzie mógł on zgodnie z prawem polegać na tej zgodnej z prawem podstawie przetwarzania. W swojej opinii w sprawie pojęcia prawnie uzasadnionych interesów administratora danych Grupa Robocza Art. 29 podkreśliła kluczową rolę rozliczalności i przejrzystości oraz praw osoby, której dane dotyczą, do sprzeciwienia się przetwarzaniu jej danych lub dostępowi, zmianie, usunięciu lub przeniesieniu ich, przy wyważaniu

392 Explanatory Report of Modernised Convention 108, pkt 46 i 47.

393 W porównaniu do dyrektywy 95/46 ogólne rozporządzenie o ochronie danych zawiera więcej przykładów przypadków uznawanych za prawnie uzasadniony interes.

394 Ogólne rozporządzenie o ochronie danych, preambuła, motyw 47.

395 Grupa Robocza Art. 29 (2014), *Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC*, WP 217, 4 kwietnia 2014 r.

396 Tamże.

prawnie uzasadnionych interesów administratora danych i interesów związanych z prawami podstawowymi osoby, której dane dotyczą[397].

W motywach RODO przedstawiono pewne przykłady przypadków stanowiących prawnie uzasadniony interes administratora danych, którego sprawa dotyczy. Na przykład przetwarzanie danych osobowych jest dopuszczalne bez zgody osoby, której dane dotyczą, w sytuacji gdy odbywa się to do celów marketingu bezpośredniego lub gdy tego rodzaju przetwarzanie jest „bezwzględnie niezbędne do zapobiegania oszustwom"[398].

W swoim orzecznictwie TSUE przedstawił szerzej kryteria pozwalające ustalić, co stanowi prawnie uzasadniony interes.

Przykład: Sprawa *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde*[399] dotyczyła szkody poniesionej przez przedsiębiorstwo trolejbusowe Rīgas wskutek uszkodzenia trolejbusu przez nagłe otwarcie drzwi taksówki przez pasażera. Rīgas satiksme chciało pozwać pasażera, domagając się odszkodowania. Policja przekazała jednak wyłącznie imię i nazwisko pasażera i odmówiła podania numeru dowodu tożsamości i adresu, podnosząc, że tego rodzaju ujawnienie byłoby niezgodne z prawem w świetle krajowych przepisów o ochronie danych.

Łotewski sąd odsyłający skierował do TSUE prośbę o wydanie orzeczenia prejudycjalnego w przedmiocie tego, czy przepisy prawa UE dotyczące ochrony danych nakładają obowiązek ujawnienia wszystkich danych osobowych niezbędnych do wszczęcia postępowania cywilnego przeciwko osobie, która jest domniemanym sprawcą wykroczenia administracyjnego[400].

Trybunał Sprawiedliwości wyjaśnił, że prawo UE dotyczące ochrony danych przewiduje możliwość, a nie obowiązek, przekazania danych stronie trzeciej z uwagi na prawnie uzasadniony interes tej strony trzeciej[401]. Trybunał Sprawiedliwości określił trzy łączne warunki, które muszą być spełnione,

397 Tamże.

398 Ogólne rozporządzenie o ochronie danych, preambuła, motyw 47.

399 TSUE, C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme"*, 4 maja 2017 r.

400 Tamże, pkt 23.

401 Tamże, pkt 26.

aby przetwarzanie danych osobowych było zgodne z prawem ze względu na „uzasadnione interesy”[402]. Po pierwsze, strona trzecia, której ujawnia się dane, musi realizować prawnie uzasadniony interes. W tym konkretnym przypadku oznacza to, że żądanie udostępnienia danych osobowych w celu pozwania osoby za wyrządzenie szkody majątkowej stanowi prawnie uzasadniony interes osoby trzeciej. Po drugie, przetwarzanie danych osobowych musi być konieczne do celów realizacji prawnie uzasadnionych interesów. W tym przypadku uzyskanie danych osobowych, takich jak adres lub numer dokumentu tożsamości, jest bezwzględnie konieczne do zidentyfikowania tej osoby. Po trzecie, podstawowe prawa i wolności osoby, której dane dotyczą, nie mogą mieć pierwszeństwa przed prawnie uzasadnionymi interesami administratora danych lub stron trzecich. W indywidualnych przypadkach należy dokonać wyważenia interesów, biorąc pod uwagę takie elementy, jak waga naruszenia praw osoby, której dane dotyczą, lub nawet wiek tej osoby w pewnych okolicznościach. Jednak w tej konkretnej sprawie TSUE nie uznał odmowy ujawnienia danych za prawnie uzasadnioną tylko dlatego, że osoba, której dane dotyczą, była nieletnia.

W wyroku w sprawie *ASNEF i FECEMD* TSUE wyraźnie orzekł w sprawie przetwarzania danych na podstawie „prawnie uzasadnionych interesów”, którą to przesłankę w owym czasie przewidywał art. 7 lit. f) dyrektywy o ochronie danych[403].

Przykład: W sprawie *ASNEF i FECEMD*[404] Trybunał Sprawiedliwości Unii Europejskiej wyjaśnił, że w prawie krajowym nie można zapisać dodatkowych warunków przetwarzania danych zgodnie z prawem oprócz tych wymienionych w art. 7 lit. f) dyrektywy[405]. Wyrok dotyczył przepisu w hiszpańskim prawie o ochronie danych, na mocy którego inne podmioty prywatne mogły twierdzić, że mają prawnie uzasadniony interes w przetwarzaniu danych osobowych tylko wówczas, gdy dana informacja pojawiła się wcześniej w źródłach publicznych.

402 Tamże, pkt 28–34.

403 Poprzednia dyrektywa o ochronie danych, art. 7 lit. f), obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. f).

404 TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* oraz *Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r.

405 Poprzednia dyrektywa o ochronie danych, art. 7 lit. f), obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. f).

Trybunał zauważył, po pierwsze, że celem dyrektywy 95/46[406] jest zapewnienie równoważności stopnia ochrony praw i wolności jednostek w zakresie przetwarzania danych osobowych we wszystkich państwach członkowskich. Ponadto zbliżanie ustawodawstw krajowych w tej dziedzinie nie może skutkować zmniejszeniem ochrony, jaką gwarantują. Przeciwnie – musi ono służyć zapewnieniu jak najwyższego stopnia ochrony w Unii[407]. W związku z tym TSUE stwierdził, że „z celu polegającego na zapewnieniu równoważnego poziomu ochrony we wszystkich państwach członkowskich wynika, że art. 7 dyrektywy 95/46[408] przewiduje zamknięty i wyczerpujący wykaz przypadków, w których przetwarzanie danych osobowych może zostać uznane za legalne". Ponadto „państwa członkowskie nie mogą dodawać nowych kryteriów legalności przetwarzania danych osobowych względem kryteriów ustanowionych w art. 7 dyrektywy 95/46[409] ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu jednego z sześciu kryteriów przewidzianych" w art. 7[410]. Trybunał przyznał, że, co się tyczy ważenia niezbędnego na mocy art. 7 lit. f) dyrektywy 95/46/WE, możliwe jest uwzględnienie faktu, że powaga naruszenia praw podstawowych osoby, której dane dotyczą, w wyniku przetwarzania może różnić się w zależności od tego, czy sporne dane figurują już w powszechnie dostępnych źródłach.

Jednakże art. 7 lit. f) tej dyrektywy „stoi na przeszkodzie temu, by państwo członkowskie wykluczyło w sposób kategoryczny i ogólny w odniesieniu do określonych kategorii danych osobowych możliwość ich przetwarzania, nie dopuszczając do ważenia przeciwstawnych praw i interesów występujących w indywidualnym przypadku".

406 Poprzednia dyrektywa o ochronie danych, obecnie ogólne rozporządzenie o ochronie danych.

407 TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* oraz *Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r., pkt 28. Ogólne rozporządzenie o ochronie danych, motywy 8 i 10.

408 Poprzednia dyrektywa o ochronie danych, art. 7, obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. f).

409 Poprzednia dyrektywa o ochronie danych, art. 7, obecnie ogólne rozporządzenie o ochronie danych, art. 6.

410 Tamże.

> W świetle tych rozważań Trybunał stwierdził, że art. 7 lit. f) dyrektywy 95/46[411] należy interpretować w ten sposób, iż „stoi on na przeszkodzie przepisom krajowym, które w braku zgody osoby, której dotyczą dane, i celem dopuszczenia przetwarzania jej danych osobowych niezbędnego dla realizacji potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej lub osób trzecich, którym dane są ujawniane, wymagają, poza poszanowaniem podstawowych praw i wolności tej osoby, by dane te były zawarte w powszechnie dostępnych źródłach, wykluczając tym samym w sposób kategoryczny i ogólny wszelką możliwość przetwarzania danych niezawartych w takich źródłach"[412].

Zgodnie z art. 21 ust. 1 RODO w każdym przypadku przetwarzania danych w oparciu o „prawnie uzasadnione interesy" osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania. Administrator musi zaprzestać przetwarzania, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do jego kontynuowania.

Jeśli chodzi o **prawo RE**, podobne sformułowania można znaleźć w zaktualizowanej konwencji nr 108[413] oraz w zaleceniach RE. W zaleceniu w sprawie profilowania uznaje się, że przetwarzanie danych osobowych do celów profilowania jest uzasadnione, gdy jest ono konieczne w związku z uzasadnionym interesem innych osób „z wyjątkiem przypadków, kiedy interesy takie podporządkowane są podstawowym prawom i wolnościom osób, których dane dotyczą"[414]. Ponadto „ochrona praw i wolności osób" została uwzględniona w art. 8 ust. 2 EKPC jako jedna z prawnie uzasadnionych przesłanek ograniczenia prawa do ochrony danych.

411 Poprzednia dyrektywa o ochronie danych, art. 7 lit. f), obecnie ogólne rozporządzenie o ochronie danych, art. 6 ust. 1 lit. f).

412 TSUE, sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF)* oraz *Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r., pkt 40, 44 i 48–49.

413 Explanatory Report of Modernised Convention 108, pkt 46.

414 Rada Europy, Komitet Ministrów (2010), Recommendation CM/Rec(2010)13 and explanatory memorandum on the protection of individuals with regard to automatic processing of personal data in the context of profiling, 23 listopada 2010 r., art. 3.4 lit. b) (zalecenie w sprawie profilowania).

Przykład: W sprawie *Y przeciwko Turcji*[415] skarżący był nosicielem wirusa HIV. Z uwagi na to, że w chwili przybycia do szpitala był on nieprzytomny załoga karetki pogotowia poinformowała personel szpitala, że jest on nosicielem wirusa HIV. Skarżący argumentował przed ETPC, że ujawnienie tych informacji naruszyło jego prawo do poszanowania życia prywatnego. Biorąc jednak pod uwagę potrzebę ochrony bezpieczeństwa personelu szpitala, wymiana informacji nie została uznana za naruszenie jego praw.

4.1.2. Przetwarzanie szczególnych kategorii danych (danych szczególnie chronionych)

W prawie RE określenie odpowiednich zabezpieczeń dotyczących wykorzystania danych szczególnie chronionych pozostawia się przepisom prawa krajowego, pod warunkiem spełnienia warunków określonych w art. 6 zaktualizowanej konwencji nr 108, a mianowicie uwzględnienia w prawie odpowiednich zabezpieczeń uzupełniających inne przepisy konwencji. **W prawie UE**, w art. 9 RODO, określono szczegółowe zasady przetwarzania szczególnych kategorii danych (zwanych także „danymi szczególnie chronionymi"), które ujawniają pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, oraz przetwarzania danych genetycznych i biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, a także danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Przetwarzanie danych szczególnie chronionych jest co do zasady zabronione[416].

Stworzono jednak wyczerpujący wykaz wyłączeń od tego zakazu, który znajduje się w art. 9 ust. 2 rozporządzenia, gdzie wyłączenia te stanowią zgodne z prawem przesłanki przetwarzania danych szczególnie chronionych. Wyłączenia te obejmują sytuacje, w których:

- osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych,
- przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej przez niezarobkowy podmiot o celach politycznych, światopoglądowych,

415 ETPC, *Y przeciwko Turcji*, nr 648/10, 17 lutego 2015 r.

416 Poprzednia dyrektywa o ochronie danych, art. 7 lit. f), obecnie ogólne rozporządzenie o ochronie danych, art. 9 ust. 1.

religijnych lub związkowych i dotyczy wyłącznie członków (lub byłych członków) tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami,

- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,

- przetwarzanie jest niezbędne:

    - do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,

    - do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (gdy osoba, której dane dotyczą, nie może wyrazić zgody),

    - do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,

    - do celów profilaktyki zdrowotnej lub medycyny pracy: „do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia”,

    - do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych ,

    - ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, lub

    - ze względów związanych z ważnym interesem publicznym.

Aby przetwarzać szczególne kategorie danych, stosunek umowny z osobą, której dane dotyczą, nie jest zatem postrzegany jako podstawa prawna zgodnego z prawem przetwarzania danych szczególnie chronionych, z wyjątkiem umowy

z pracownikiem służby zdrowia podlegającym obowiązkowi zachowania tajemnicy zawodowej[417].

Wyraźna zgoda osoby, której dane dotyczą

W prawie UE pierwszą możliwą przesłanką przetwarzania jakichkolwiek danych zgodnie z prawem, niezależnie od tego, czy są to dane szczególnie chronione, jest zgoda osoby, której dane dotyczą. W przypadku danych szczególnie chronionych zgoda taka musi być wyraźna. W prawie UE lub prawie krajowym państwa członkowskiego można jednak zawrzeć zapis, że zakaz przetwarzania danych szczególnie chronionych nie może być zniesiony przez osobę fizyczną[418]. Zasada ta miałaby zastosowanie na przykład w sytuacji, gdy przetwarzanie wiąże się ze szczególnym ryzykiem dla osoby, której dane dotyczą.

Prawo pracy, zabezpieczenia społecznego i ochrony socjalnej

W prawie UE zakaz przewidziany w art. 9 ust. 1 może zostać zniesiony, jeżeli przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy lub zabezpieczenia społecznego. Przetwarzanie musi być jednak dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującym odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą[419]. Dokumentacja zatrudnienia przechowywana przez organizację może zawierać dane szczególnie chronione pod pewnymi warunkami określonymi w RODO i odpowiednich przepisach prawa krajowego. Przykłady danych szczególnie chronionych mogą obejmować członkostwo w związkach zawodowych lub informacje dotyczące zdrowia.

Żywotne interesy osoby, której dane dotyczą, lub interesy innej osoby fizycznej

W prawie UE, podobnie jak w przypadku danych innych niż szczególnie chronione, dane szczególnie chronione mogą być przetwarzane ze względu na żywotne interesy osoby, której dane dotyczą, lub innej osoby fizycznej[420]. W sytuacji gdy

417 Ogólne rozporządzenie o ochronie danych, art. 9 ust. 2 lit. h) i i).

418 Tamże, art. 9 ust. 2 lit. a)

419 Ogólne rozporządzenie o ochronie danych, art. 9 ust. 2 lit. b).

420 Tamże, art. 9 ust. 2 lit. c).

podstawą przetwarzania jest żywotny interes innej osoby fizycznej, powołanie tej przesłanki jest możliwe wyłącznie w przypadkach, gdy „ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej"[421]. W niektórych przypadkach przetwarzanie danych osobowych może służyć zarówno interesom osoby fizycznej, jak i interesowi publicznemu, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych[422].

Aby przetwarzanie danych szczególnie chronionych na tej podstawie było zgodne z prawem, niezbędne jest, aby poproszenie o zgodę osoby, której dane dotyczą, nie było możliwe na przykład ze względu na to, że osoba, której dane dotyczą, jest nieprzytomna lub też nieobecna i nie można się z nią skontaktować. Innymi słowy, osoba ta nie była fizycznie lub prawnie zdolna do wyrażenia zgody.

Organizacje charytatywne lub podmioty niezarobkowe

Przetwarzanie danych osobowych jest także dopuszczalne w ramach uprawnionej działalności prowadzonej przez fundacje, stowarzyszenia lub inny niezarobkowe podmioty o celach politycznych, światopoglądowych, religijnych lub związkowych. Przetwarzanie musi jednak dotyczyć wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty[423]. Dane szczególnie chronione nie mogą być ujawniane poza tym podmiotem bez zgody osoby, której dane dotyczą.

Dane w sposób oczywisty upublicznione przez osobę, której dane dotyczą

Artykuł 9 ust. 2 lit. e) RODO przewiduje, że przetwarzanie nie jest zakazane, jeżeli obejmuje dane w sposób oczywisty upublicznione przez osobę, której dane dotyczą. Mimo że w rozporządzeniu nie zdefiniowano pojęcia „w sposób oczywisty upublicznione przez osobę, której dane dotyczą", ponieważ stanowi ono wyjątek od zakazu przetwarzania danych szczególnie chronionych, należy je interpretować ściśle i jako oznaczające fakt, że osoba, której dane dotyczą, celowo podała swoje dane osobowe do wiadomości publicznej. Tak więc w przypadku gdy telewizja transmituje nagranie z kamery przemysłowej, pokazujące między innymi zranienie strażaka próbującego ewakuować budynek, nie można uznać, że strażak w sposób oczywisty

421 Tamże, motyw 46.

422 Tamże.

423 Tamże, art. 9 ust. 2 lit. d).

podał dane do wiadomości publicznej. Z drugiej strony, jeżeli strażak zdecyduje się opisać zdarzenie i opublikować film i zdjęcia na publicznej stronie internetowej, podjąłby celowe, pozytywne działanie w celu upublicznienia danych osobowych. Należy zauważyć, że upublicznienie danych nie oznacza zgody, ale jest kolejnym pozwoleniem na przetwarzanie szczególnych kategorii danych.

Fakt, że osoba, której dane dotyczą, podała do wiadomości publicznej przetwarzane dane osobowe, nie zwalnia administratorów danych z ich obowiązków wynikających z prawa o ochronie danych. Na przykład zasada ograniczenia celu nadal ma zastosowanie do danych osobowych, nawet jeżeli dane te zostały podane do wiadomości publicznej[424].

Roszczenia

Przetwarzanie szczególnych kategorii danych, które jest „niezbędne do ustalenia, dochodzenia lub obrony roszczeń" w ramach postępowania sądowego, administracyjnego lub pozasądowego[425] również jest dopuszczalne na gruncie RODO[426]. W takim przypadku przetwarzanie musi być istotne w kontekście konkretnego roszczenia oraz odpowiednio jego dochodzenia lub obrony i może być przedmiotem żądania każdej ze stron sporu.

Działając w ramach sprawowania wymiaru sprawiedliwości, sądy mogą przetwarzać szczególne kategorie danych w kontekście rozpatrywania sporu natury prawnej[427]. Przykłady tych szczególnych kategorii danych przetwarzanych w tym kontekście mogłyby obejmować na przykład dane genetyczne przy ustalaniu pokrewieństwa lub stanu zdrowia, jeżeli część dowodów dotyczy szczegółów szkody poniesionej przez ofiarę przestępstwa.

Względy związane z ważnym interesem publicznym

W myśl art. 9 ust. 2 lit. g) RODO państwa członkowskie mogą wskazać dalsze okoliczności, w których dopuszczalne jest przetwarzanie danych szczególnie chronionych, pod warunkiem że:

424 Grupa Robocza Art. 29 (2013), *Opinion 3/13 on purpose limitation*, WP 203, Bruksela, 2 kwietnia 2013 r., s. 14.

425 Ogólne rozporządzenie o ochronie danych, preambuła, motyw 52.

426 Tamże, art. 9 ust. 2 lit. f).

427 Tamże.

- przetwarzanie danych jest niezbędne ze względów związanych z ważnym interesem publicznym,

- jest ono przewidziane w prawie Unii lub prawie krajowym,

- przepisy prawa Unii lub prawa krajowego są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą[428].

Ważnym przykładem są systemy elektronicznych kart zdrowia. Takie systemy umożliwiają udostępnienie danych dotyczących zdrowia zgromadzonych przez podmioty świadczące opiekę zdrowotną podczas leczenia pacjenta innym podmiotom świadczącym opiekę zdrowotną temu pacjentowi na szeroką skalę, zazwyczaj na terenie całego kraju.

Grupa Robocza Art. 29 stwierdziła, że takie systemy nie mogą zostać ustanowione na mocy obowiązujących przepisów prawnych dotyczących przetwarzania danych o pacjentach[429]. Możliwe jest jednak istnienie systemów elektronicznych kart zdrowia, jeżeli opierają się one na „względach związanych z ważnym interesem publicznym"[430]. Wymagałoby to dla ich ustanowienia wyraźnej podstawy prawnej, a także niezbędnych zabezpieczeń w celu zapewnienia bezpiecznego działania systemu[431].

Inne podstawy przetwarzania danych szczególnie chronionych

Zgodnie z RODO przetwarzanie danych szczególnie chronionych jest możliwe, gdy jest to niezbędne[432]:

- do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami

428 Tamże, art. 9 ust. 2 lit. g).

429 Grupa Robocza Art. 29 (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR)*, WP 131, Bruksela, 15 lutego 2007 r. Ogólne rozporządzenie o ochronie danych, art. 9 ust. 3.

430 Ogólne rozporządzenie o ochronie danych, art. 9 ust. 2 lit. g).

431 Grupa Robocza Art. 29 (2007), *Working Document on the processing of personal data relating to health in electronic health records (EHR),* WP 131, Bruksela, 15 lutego 2007 r.

432 Ogólne rozporządzenie o ochronie danych, art. 9 ust. 2 lit. h), i) i j).

opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;

- ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego. Prawo to musi przewidywać odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą;

- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na podstawie prawa Unii lub prawa państwa członkowskiego. Przepisy prawa muszą być proporcjonalne do wyznaczonego celu, nie mogą naruszać istoty prawa do ochrony danych i muszą przewidywać odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Dalsze warunki na gruncie prawa krajowego

Zgodnie z RODO państwa członkowskie mogą wprowadzić lub zachować dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia[433].

4.2. Przepisy dotyczące bezpieczeństwa przetwarzania

Najważniejsze kwestie

- Przepisy dotyczące bezpieczeństwa przetwarzania implikują obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych przez administratora oraz podmiot przetwarzający w celu zapobieżenia nieuprawnionej ingerencji w czynności przetwarzania danych.
- Niezbędny poziom bezpieczeństwa danych jest uzależniony od:

433 Tamże, art. 9 ust. 2 lit. h) i art. 9 ust. 4.

  - zabezpieczeń dostępnych na rynku w odniesieniu do konkretnego rodzaju przetwarzania;
  - kosztów;
  - ryzyka związanego z przetwarzaniem danych w kontekście podstawowych praw i wolności osób, których dane dotyczą.
- Zapewnienie poufności danych osobowych jest częścią ogólnej zasady uznanej w ogólnym rozporządzeniu o ochronie danych.

Zarówno na mocy **prawa UE**, jak i **prawa RE** administratorzy mają ogólny obowiązek przestrzegania wymogów przejrzystości i rozliczalności podczas przetwarzania danych osobowych, w szczególności w odniesieniu do naruszeń ochrony danych w przypadku, gdy takie naruszenia mają miejsce. W przypadku naruszenia ochrony danych osobowych administratorzy muszą zgłosić je organom nadzorczym, chyba że jest mało prawdopodobne, by naruszenie to stanowiło zagrożenie dla praw lub wolności osób fizycznych. Osoby, których dane dotyczą, powinny być również informowane o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

4.2.1. Elementy bezpieczeństwa danych

Zgodnie z odpowiednimi przepisami **prawa UE**:

> *„Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku […]"*[434].

Środki te obejmują między innymi:

- pseudonimizację i szyfrowanie danych osobowych[435];
- zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania[436];

434 Tamże, art. 32 ust. 1.

435 Tamże, art. 32 ust. 1 lit. a).

436 Tamże, art. 32 ust. 1 lit. b).

- szybkie przywrócenie dostępności danych osobowych i dostępu do nich w razie utraty danych[437];

- regularne testowanie, mierzenie i ocenianie skuteczności środków mających zapewnić bezpieczeństwo przetwarzania[438].

Podobny przepis istnieje w **prawie RE**:

> *„Każda Strona zapewnia, że administrator i, w stosownych przypadkach, podmiot przetwarzający podejmują odpowiednie środki bezpieczeństwa chroniące przed zagrożeniami takimi jak przypadkowy lub nieupoważniony dostęp do danych osobowych, ich zniszczenie, utrata, wykorzystanie, modyfikacja lub ujawnienie"*[439].

Zgodnie z **prawem UE i prawem RE** naruszenie danych, które może mieć wpływ na prawa i wolności osób fizycznych, zobowiązuje administratora danych do powiadomienia organu nadzorczego o tym naruszeniu (zob. sekcja 4.2.3).

Często istnieją też normy przemysłowe, krajowe i międzynarodowe, opracowane, aby zapewnić bezpieczne przetwarzanie danych. Na przykład EuroPriSe (europejski znak jakościochrony danych osobowych) jest unijnym projektem realizowanym w ramach eTEN (transeuropejskich sieci telekomunikacyjnych), którego celem było zbadanie możliwości certyfikacji produktów, w tym zwłaszcza oprogramowania, jako zgodnych z europejskim prawem o ochronie danych. Agencję Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) ustanowiono, aby zwiększyć zdolność UE, państw członkowskich UE i przedsiębiorców do zapobiegania problemom związanym z bezpieczeństwem sieci i informacji, zajmowania się nimi oraz reagowania na nie[440]. Agencja regularnie publikuje analizy aktualnych zagrożeń i zalecenia dotyczące radzenia sobie z nimi[441].

437 Tamże, art. 32 ust. 1 lit. c).

438 Tamże, art. 32 ust. 1 lit. d).

439 Zaktualizowana konwencja nr 108, art. 7 ust. 1.

440 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 526/2013 z dnia 21 maja 2013 r. w sprawie Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) oraz uchylające rozporządzenie (WE) nr 460/2004, Dz.U. L 165 z 18.6.2013.

441 Na przykład ENISA, (2016), Cyber Security and Resilience of smart cars. Good practices and recommendations; ENISA (2016), Security of Mobile Payments and Digital Wallets.

Aby zapewnić bezpieczeństwo danych, nie wystarcza wdrożenie odpowiedniego sprzętu i oprogramowania. Niezbędne są również właściwe regulaminy wewnętrzne. Takie regulaminy powinny w miarę możliwości obejmować następujące zagadnienia:

- regularne informowanie wszystkich pracowników o zasadach bezpieczeństwa danych i ich obowiązkach wynikających z przepisów o ochronie danych, a zwłaszcza obowiązkach dotyczących poufności;

- jasny podział obowiązków i wyraźne określenie kompetencji w zakresie przetwarzania danych, zwłaszcza w odniesieniu do decyzji o przetwarzaniu danych osobowych oraz o przekazywaniu danych stronom trzecim lub osobom, których dane dotyczą;

- wykorzystanie danych osobowych wyłącznie zgodnie z poleceniami właściwej osoby lub zgodnie z ogólnie ustalonymi zasadami;

- ochrona dostępu do obiektów oraz do sprzętu i oprogramowania administratora lub podmiotu przetwarzającego, w tym sprawdzanie uprawnień dostępu;

- zapewnienie, aby uprawnienia do dostępu do danych osobowych były przyznawane przez właściwą osobę i wymagały odpowiedniego udokumentowania;

- zautomatyzowane protokoły dostępu do danych osobowych drogą elektroniczną oraz regularne kontrole takich protokołów przez wewnętrzną komórkę nadzorczą (stąd wymóg rejestrowania wszystkich czynności przetwarzania danych);

- staranne dokumentowanie form ujawniania innych niż automatyczny dostęp do danych, aby było możliwe wykazanie, że nie doszło do nielegalnego przekazania danych.

Ważnymi elementami skutecznych zabezpieczeń są także zapewnienie odpowiednich szkoleń w zakresie bezpieczeństwa danych i edukacja pracowników. Trzeba także stosować procedury weryfikacji (np. audyty wewnętrzne lub zewnętrzne) w celu zapewnienia, aby odpowiednie środki zostały nie tylko zapisane w dokumentach, ale także zostały wdrożone i działały w praktyce.

Środki służące poprawie poziomu bezpieczeństwa administratora lub podmiotu przetwarzającego obejmują mianowanie inspektorów ochrony danych, edukację pracowników pod kątem bezpieczeństwa, regularne audyty, testy penetracyjne i znaki jakości.

Przykład: W sprawie *I przeciwko Finlandii*[442] skarżąca nie była w stanie udowodnić, że inni pracownicy szpitala, w którym pracowała, uzyskali niezgodnie z prawem dostęp do jej dokumentacji zdrowotnej. Jej roszczenie o naruszenie prawa do ochrony danych zostało zatem odrzucone przez sądy krajowe. ETPC uznał, że doszło do naruszenia art. 8 EKPC, gdyż szpitalny rejestr dokumentacji zdrowotnej „uniemożliwiał późniejsze ustalenie, w jaki sposób korzystano z dokumentacji pacjenta, gdyż odnotowywał tylko pięć ostatnich przypadków dostępu, a informacje te były usuwane po zwrocie akt do archiwum". Z punktu widzenia Trybunału decydującym czynnikiem było to, że system zarządzania dokumentacją w szpitalu był w oczywisty sposób niezgodny z wymogami prawnymi zapisanymi w prawie krajowym, czego nie wzięły w wystarczającym stopniu pod uwagę sądy krajowe.

Unia Europejska wdrożyła dyrektywę w sprawie bezpieczeństwa sieci i systemów informatycznych (dyrektywę NIS)[443], która jest pierwszym ogólnounijnym instrumentem prawnym w dziedzinie cyberbezpieczeństwa. Dyrektywa ma na celu z jednej strony poprawę cyberbezpieczeństwa na szczeblu krajowym, a z drugiej strony zwiększenie poziomu współpracy w ramach UE. Nakłada również na operatorów podstawowych usług (w tym operatorów w sektorach energii, zdrowia, bankowości, transportu, infrastruktury cyfrowej itp.) i dostawców usług cyfrowych obowiązki w zakresie zarządzania ryzykiem, zapewnienia bezpieczeństwa ich sieci i systemów informatycznych oraz zgłaszania incydentów w zakresie bezpieczeństwa.

Perspektywa

We wrześniu 2017 r. Komisja Europejska przedstawiła projekt rozporządzenia mającego na celu zreformowanie mandatu ENISA, aby uwzględnić nowe kompetencje i obowiązki agencji wynikające z dyrektywy NIS. Celem proponowanego rozporządzenia jest rozwinięcie zadań ENISA i wzmocnienie jej roli jako „punktu odniesienia

442 ETPC, *I przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.

443 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii, Dz.U. L 194 z 19.7.2016.

w ekosystemie cyberbezpieczeństwa UE"[444]. Proponowane rozporządzenie nie powinno naruszać zasad RODO, a poprzez wyjaśnienie niezbędnych elementów składających się na europejskie systemy certyfikacji w zakresie cyberbezpieczeństwa powinno również zwiększyć bezpieczeństwo danych osobowych. Jednocześnie we wrześniu 2017 r. Komisja Europejska przedstawiła projekt rozporządzenia wykonawczego określającego elementy, które dostawcy usług cyfrowych powinni uwzględnić w celu zapewnienia bezpieczeństwa swoich sieci i systemów informatycznych, zgodnie z art. 16 ust. 8 dyrektywy NIS. W czasie opracowywania podręcznika trwały dyskusje na temat tych dwóch wniosków.

4.2.2. Poufność

W prawie UE w RODO uznano poufność danych osobowych za część zasady ogólnej[445]. Dostawcy publicznie dostępnych usług łączności elektronicznej muszą zapewnić poufność. Są oni również zobowiązani do zapewnienia bezpieczeństwa świadczonych usług[446].

Przykład: Pracownik towarzystwa ubezpieczeń odbiera w pracy telefon od osoby przedstawiającej się jako klient, która chce uzyskać wszystkie informacje na temat swojej umowy ubezpieczenia.

W związku z obowiązkiem zachowania poufności danych klientów pracownik powinien przed ujawnieniem danych osobowych zastosować co najmniej minimalne środki bezpieczeństwa. Może na przykład zaproponować oddzwonienie na numer telefoniczny podany w aktach klienta.

Zgodnie z art. 5 ust. 1 lit. f) dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

444 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ENISA, „Agencji UE ds. Cyberbezpieczeństwa " i uchylającego rozporządzenie (UE) nr 526/2013 oraz certyfikacji bezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych („akt ws. cyberbezpieczeństwa"), COM(2017)477, 13 września 2017 r., s. 6.

445 Ogólne rozporządzenie o ochronie danych, art. 5 ust. 1 lit. f).

446 Dyrektywa o prywatności i łączności elektronicznej, art. 5 ust. 1.

Na mocy art. 32 administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić wysoki stopień bezpieczeństwa. Środki tego rodzaju obejmują między innymi pseudonimizację i szyfrowanie danych osobowych, zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania, ocenianie i testowanie skuteczności środków technicznych i organizacyjnych oraz zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego. Ponadto przestrzeganie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może stanowić element pomocny w wykazaniu zgodności z zasadą integralności i poufności. Zgodnie z art. 28 RODO umowa wiążąca administratora i podmiot przetwarzający musi określać, że podmiot przetwarzający zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy.

Obowiązek zachowania poufności nie obejmuje sytuacji, w których dane stają się znane osobie będącej osobą prywatną, a nie pracownikiem administratora lub podmiotu przetwarzającego. W tym przypadku art. 32 i 28 RODO nie mają zastosowania, ponieważ wykorzystanie danych osobowych przez osoby fizyczne jest całkowicie wyłączone z zakresu stosowania rozporządzenia, w przypadku gdy takie wykorzystanie mieści się w granicach tzw. wyłączenia dla działalności domowej[447]. Wyłączenie dla działalności domowej to wykorzystywanie danych osobowych „przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze"[448]. Od czasu orzeczenia TSUE w sprawie *Bodil Lindqvist*[449] wyłączenie to należy jednak interpretować w sposób zawężający, zwłaszcza w odniesieniu do ujawniania danych. W szczególności wyłączenie dla działalności domowej nie obejmuje publikacji danych osobowych na użytek nieograniczonej liczby odbiorców w Internecie ani przetwarzania danych, które ma cechy działalności zawodowej lub handlowej (więcej szczegółów dotyczących sprawy – zob. sekcje 2.1.2, 2.2.2 i 2.3.1).

„Poufność komunikatów" to kolejny aspekt poufności podlegający *lex specialis*. Przepisy szczególne służące zapewnieniu poufności łączności elektronicznej na mocy dyrektywy o prywatności i łączności elektronicznej zobowiązują państwa członkowskie do zakazywania słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez

447 Ogólne rozporządzenie o ochronie danych, art. 2 ust. 2 lit. c).

448 Tamże.

449 TSUE, C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r.

osoby inne niż użytkownicy lub bez zgody zainteresowanych użytkowników[450]. W prawie krajowym można ustanowić wyjątki od tej zasady wyłącznie ze względów bezpieczeństwa narodowego, obronności, zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych i wyłącznie wówczas, gdy środki te są niezbędne i proporcjonalne w świetle zamierzonych celów[451]. Te same zasady będą miały zastosowanie na mocy przyszłego rozporządzenia w sprawie prywatności i łączności elektronicznej, jednak zakres aktu prawnego dotyczącego prywatności i łączności elektronicznej zostanie rozszerzony z publicznie dostępnych usług łączności elektronicznej, tak aby obejmował również łączność wykonywaną za pośrednictwem usług OTT (takich jak aplikacje mobilne).

W prawie RE obowiązek zachowania poufności wynika z pojęcia bezpieczeństwa danych, o którym mowa w art. 7 ust. 1 zaktualizowanej konwencji nr 108 dotyczącym bezpieczeństwa danych.

W przypadku podmiotów przetwarzających poufność oznacza, że nie mogą one ujawniać danych stronom trzecim lub innym odbiorcom bez zezwolenia. W przypadku pracowników administratora lub podmiotu przetwarzającego zachowanie poufności wymaga wykorzystywania danych osobowych wyłącznie zgodnie z poleceniami właściwych przełożonych.

Obowiązek zachowania poufności musi być zapisany w każdej umowie między administratorami i podmiotami przetwarzającymi. Ponadto administratorzy i podmioty przetwarzające będą musieli podjąć konkretne środki w celu nałożenia na swoich pracowników prawnego obowiązku zachowania poufności, co jest zazwyczaj realizowane przez włączenie klauzul o zachowaniu poufności do umowy o pracę.

Naruszenie obowiązków zawodowych dotyczących zachowania poufności podlega ściganiu w ramach postępowania karnego w wielu państwach członkowskich UE i stronach zaktualizowanej konwencji nr 108.

4.2.3. Zgłoszenia naruszenia ochrony danych osobowych

Naruszenie ochrony danych osobowych odnosi się do naruszenia bezpieczeństwa prowadzącego do przypadkowego lub niezgodnego z prawem zniszczenia,

450 Dyrektywa o prywatności i łączności elektronicznej, art. 5 ust. 1.

451 Tamże, art. 15 ust. 1.

utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych[452]. Chociaż nowe technologie, takie jak szyfrowanie, dają obecnie więcej możliwości zapewnienia bezpieczeństwa przetwarzania danych, przypadki naruszania ochrony danych są nadal powszechnym zjawiskiem. Przyczyny naruszeń ochrony danych mogą być różne: od przypadkowych błędów popełnianych przez osoby pracujące w organizacji po zagrożenia zewnętrzne, takie jak hakerzy i organizacje cyberprzestępcze.

Naruszenie ochrony danych może nieść ze sobą bardzo niekorzystne skutki dla prawa do prywatności i ochrony danych osób fizycznych, które w wyniku takiego naruszenia tracą kontrolę nad swoimi danymi osobowymi. Naruszenia mogą prowadzić do kradzieży tożsamości lub oszustwa, strat finansowych lub szkód materialnych, utraty poufności danych osobowych chronionych tajemnicą zawodową oraz uszczerbku na reputacji osoby, której dane dotyczą. W swoich wytycznych w sprawie zgłaszania naruszeń ochrony danych osobowych na mocy rozporządzenia 2016/679 Grupa Robocza Art. 29 wyjaśnia, że naruszenia mogą mieć trojaki wpływ na dane osobowe i prowadzić do: ujawnienia, utraty lub zmiany[453]. Oprócz obowiązku podjęcia środków w celu zapewnienia bezpieczeństwa przetwarzania danych, jak wyjaśniono w sekcji 4.2, równie ważne jest zapewnienie, aby w przypadku naruszenia administratorzy danych odpowiednio i terminowo na nie reagowali.

Organy nadzorcze i osoby fizyczne są często nieświadome występowania naruszenia ochrony danych, co uniemożliwia osobom fizycznym podejmowanie kroków mających na celu ochronę przed jego negatywnymi konsekwencjami. W celu potwierdzenia praw osób fizycznych i ograniczenia skutków naruszeń ochrony danych **UE i RE** w pewnych okolicznościach nakładają na administratorów danych wymóg zgłoszenia.

Na mocy zaktualizowanej konwencji nr 108 **RE** umawiające się strony muszą, co najmniej, wymagać od administratorów danych zgłoszenia właściwemu organowi nadzorczemu naruszeń ochrony danych, które mogą stanowić poważną ingerencję

452 Ogólne rozporządzenie o ochronie danych, art. 4 pkt 12; zob. także Grupa Robocza Art. 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 października 2017 r., s. 8.

453 Grupa Robocza Art. 29 (2017), *Guidelines on Personal data breach notification under Regulation 2016/679*, WP 250, 3 października 2017 r., s. 6.

w prawa osób, których dane dotyczą. Zgłoszenie takie powinno zostać dokonane „niezwłocznie”[454].

W prawie UE ustanowiono szczegółowy system regulujący terminy i treść zgłoszeń[455]. Wobec tego administratorzy muszą zgłaszać organom nadzorczym określone naruszenia ochrony danych bez zbędnej zwłoki i, w miarę możliwości, nie później niż w ciągu 72 godzin od stwierdzenia naruszenia. W razie przekroczenia 72-godzinnego terminu do zgłoszenia dołącza się wyjaśnienie przyczyn opóźnienia. Administratorzy są zwolnieni z obowiązku zgłoszenia wyłącznie w sytuacji, gdy są w stanie wykazać, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, których sprawa dotyczy.

W rozporządzeniu określono minimalny zakres informacji, jakie należy uwzględnić w zgłoszeniu, aby umożliwić organowi nadzorczemu podjęcie odpowiednich działań[456]. Zgłoszenie musi zawierać co najmniej opis charakteru naruszenia ochrony danych oraz kategorii i przybliżonej liczby osób, których dane dotyczą i których dotyczy naruszenie, a także opis możliwych konsekwencji naruszenia oraz środków wdrożonych przez administratora danych w celu uwzględnienia i złagodzenia ich skutków. Ponadto należy podać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego organ nadzorczy będzie mógł w razie konieczności uzyskać więcej informacji.

Jeżeli naruszenie ochrony danych powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych, administratorzy muszą zawiadomić te osoby (osoby, których dane dotyczą) o naruszeniu bez zbędnej zwłoki[457]. Informacje kierowane do osób, których dane dotyczą, w tym opis naruszenia ochrony danych, muszą być sformułowane w sposób jasny i zrozumiały oraz muszą zawierać informacje podobne do tych, które są wymagane w przypadku zgłoszeń kierowanych do organów nadzorczych. W pewnych okolicznościach administratorzy mogą być zwolnieni z obowiązku zgłoszenia tego rodzaju naruszeń osobom, których dane dotyczą. Wyłączenia mają zastosowanie w przypadku gdy administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak

454 Zaktualizowana konwencja nr 108, art. 7 ust. 2; Explanatory Report of Modernised Convention 108, pkt 64–66.

455 Ogólne rozporządzenie o ochronie danych, art. 33 i 34.

456 Tamże, art. 33 ust. 3.

457 Tamże, art. 34.

szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych. Działania podjęte przez administratora w następstwie naruszenia w celu wyeliminowania prawdopodobieństwa naruszenia praw lub wolności osób, których dane dotyczą, mogą także skutkować zwolnieniem administratora z obowiązku zgłoszenia naruszenia osobom, których dane dotyczą. Wreszcie, jeżeli zgłoszenie wymaga niewspółmiernie dużego wysiłku ze strony administratora osoby, których dane dotyczą, mogą zostać poinformowane w inny sposób, taki jak publiczny komunikat lub podobne środki[458].

Obowiązek zawiadamiania organów nadzorczych i osób, których dane dotyczą, o naruszeniach ochrony danych skierowany jest do administratorów danych. Naruszenie ochrony danych może jednak nastąpić niezależnie od tego, czy przetwarzania dokonuje administrator czy podmiot przetwarzający. Z tego powodu konieczne jest zapewnienie, by podmioty przetwarzające także podlegały obowiązkowi zgłoszenia naruszeń ochrony danych. W takim przypadku podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych bez zbędnej zwłoki zgłasza je administratorowi[459]. Następnie administrator ponosi odpowiedzialność za zgłoszenie naruszenia organom nadzorczym i osobom, których dotyczy naruszenie, z zastrzeżeniem wspomnianych wyżej zasad i terminów.

4.3. Przepisy dotyczące rozliczalności i promowania przestrzegania przepisów

Najważniejsze kwestie

- Aby zapewnić rozliczalność w procesie przetwarzania danych osobowych administratorzy i podmioty przetwarzające muszą prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni oraz udostępniać je na żądanie organów nadzorczych.
- W ogólnym rozporządzeniu o ochronie danych wymieniono kilka instrumentów promujących przestrzeganie przepisów:
  - wyznaczanie inspektorów ochrony danych w określonych sytuacjach;
  - przeprowadzenie oceny skutków przed rozpoczęciem przetwarzania danych, które może powodować wysokie ryzyko dla praw i wolności osób fizycznych;

458 Tamże, art. 34 ust. 3 lit. c).

459 Tamże, art. 33 ust. 2.

  - uprzednie konsultacje z właściwym organem nadzorczym, jeżeli ocena skutków wykaże, że przetwarzanie danych wiąże się z ryzykiem, którego nie można złagodzić;
  - kodeksy postępowania dla administratorów i podmiotów przetwarzających określające stosowanie rozporządzenia w różnych sektorach przetwarzania;
  - mechanizmy certyfikacji, znaki jakości i oznaczenia.
- W prawie RE, w zaktualizowanej konwencji nr 108, proponuje się podobne instrumenty promowania zgodności z przepisami.

Zasada rozliczalności ma szczególne znaczenie dla zagwarantowania egzekwowania przepisów o ochronie danych w Europie. Administrator danych jest odpowiedzialny za zgodność z przepisami o ochronie danych i musi być w stanie wykazać taką zgodność. Rozliczalność powinna być stosowana nie tylko po zaistnieniu naruszenia. Na administratorach ciąży raczej aktywny obowiązek przestrzegania odpowiednich polityk zarządzania danymi na wszystkich etapach przetwarzania danych. Europejskie prawo ochrony danych wymaga, aby administratorzy wdrożyli środki techniczne i organizacyjne w celu zapewnienia i wykazania, że przetwarzanie odbywa się zgodnie z tym prawem. Środki te obejmują wyznaczanie inspektorów ochrony danych, prowadzenie rejestrów i dokumentacji związanej z przetwarzaniem danych oraz przeprowadzanie ocen skutków dla ochrony prywatności.

4.3.1. Inspektorzy ochrony danych

Inspektorzy ochrony danych (IOD) to osoby, które doradzają w zakresie zgodności z przepisami dotyczącymi ochrony danych w organizacjach zajmujących się przetwarzaniem danych. Są one „podstawą rozliczalności", ponieważ ułatwiają przestrzeganie przepisów, a jednocześnie działają jako pośrednicy między organami nadzorczymi, osobami, których dane dotyczą i organizacją, która wyznaczyła ich do pełnienia tej funkcji.

W prawie RE art. 10 ust. 1 zaktualizowanej konwencji nr 108 nakłada ogólny obowiązek w zakresie rozliczalności na administratorów i podmioty przetwarzające. Wymaga to od administratorów i podmiotów przetwarzających podjęcia wszelkich odpowiednich środków w celu zapewnienia zgodności z przepisami o ochronie danych określonymi w konwencji oraz wykazania, że przetwarzanie danych pod ich kontrolą jest zgodne z postanowieniami konwencji. Mimo że konwencja nie określa konkretnych środków, jakie powinni przyjąć administratorzy i podmioty przetwarzające, sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108 wskazuje,

że wyznaczenie IOD byłoby jednym z możliwych środków pomocnych w wykazaniu zgodności z przepisami. Inspektorom ochrony danych należy zapewnić wszelkie środki niezbędne do wykonania ich zadań[460].

W przeciwieństwie do prawa RE, **w prawie UE** wyznaczenie IOD nie zawsze leży w gestii administratorów i podmiotów przetwarzających, ale w pewnych warunkach jest obowiązkowe. Ogólne rozporządzenie o ochronie danych uznaje, że IOD odgrywa kluczową rolę w nowym systemie zarządzania i zawiera szczegółowe przepisy dotyczące wyznaczania inspektora, jego stanowiska, obowiązków i zadań[461].

Rozporządzenie wprowadza obowiązek wyznaczenia IOD w trzech konkretnych przypadkach: gdy przetwarzania dokonują organ lub podmiot publiczny; gdy główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub gdy główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa[462]. Mimo że terminy takie jak „systematyczne monitorowanie na dużą skalę" i „działania podstawowe" nie zostały zdefiniowane w rozporządzeniu, Grupa Robocza Art. 29 wydała wytyczne dotyczące sposobu ich interpretacji[463].

Przykład: Za administratorów danych, których operacje przetwarzania wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, można by prawdopodobnie uznać przedsiębiorstwa z branży mediów społecznościowych i operatorów wyszukiwarek internetowych. Model biznesowy takich przedsiębiorstw opiera się na przetwarzaniu dużych ilości danych osobowych i generują one znaczące przychody poprzez oferowanie ukierunkowanych usług reklamowych oraz umożliwienie spółkom reklamowania się na stronach internetowych. Ukierunkowana reklama jest sposobem umieszczania reklam w oparciu o dane demograficzne oraz

460 Explanatory Report of Modernised Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), pkt 87.

461 Ogólne rozporządzenie o ochronie danych, art. 37–39.

462 Tamże, art. 37 ust. 1.

463 Grupa Robocza Art. 29 (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

wcześniejszą historię zakupów lub zachowanie konsumentów. Wymaga to zatem systematycznego monitorowania przyzwyczajeń i zachowań osób, których dane dotyczą, w środowisku online.

Przykład: Szpital i towarzystwo ubezpieczeń zdrowotnych to typowe przykłady administratorów danych, których działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych. Dane ujawniające informacje dotyczące stanu zdrowia osób fizycznych stanowią szczególną kategorię danych osobowych zarówno na mocy prawa RE, jak i prawa UE, a zatem wymagają zwiększonej ochrony. Prawo UE za szczególne kategorie uznaje ponadto dane genetyczne i biometryczne. W zakresie, w jakim zakłady opieki zdrowotnej i towarzystwa ubezpieczeniowe przetwarzają takie dane na dużą skalę, RODO wymaga od nich wyznaczenia inspektora ochrony danych.

Ponadto art. 37 ust. 4 RODO stanowi, że w przypadkach innych niż trzy obowiązkowe, o których mowa w art. 37 ust. 1, administrator, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie administratorów lub podmiotów przetwarzających mogą wyznaczyć, lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznaczają inspektora ochrony danych.

Wszystkie pozostałe organizacje nie są prawnie zobowiązane do wyznaczenia IOD. Jednakże RODO przewiduje, że administratorzy i podmioty przetwarzające mogą zdecydować się na dobrowolne wyznaczenie inspektora ochrony danych, dając jednocześnie państwom członkowskim możliwość wprowadzenia obowiązku takiego wyznaczenia dla większej liczby rodzajów organizacji niż przewidziano w rozporządzeniu[464].

Po wyznaczeniu IOD administrator musi zapewnić, by inspektor „był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych" w organizacji[465]. Na przykład IOD powinni być zaangażowani w doradztwo w zakresie przeprowadzania ocen skutków dla ochrony danych oraz w tworzenie i przechowywanie rejestrów czynności przetwarzania danych w organizacji. Aby umożliwić IOD skuteczne wypełnianie swoich zadań, administratorzy i podmioty przetwarzające muszą zapewnić im niezbędne zasoby, w tym zasoby finansowe, infrastrukturę i sprzęt. Dodatkowe wymogi obejmują zapewnienie IOD odpowiedniego czasu na

464 Ogólne rozporządzenie o ochronie danych, art. 37 ust. 3 i 4.

465 Tamże, art. 38 ust. 1.

wypełnianie swoich funkcji oraz ustawiczne szkolenia umożliwiające im zdobycie wiedzy specjalistycznej i śledzenie na bieżąco wszelkich zmian w prawie o ochronie danych[466].

W RODO określono pewne podstawowe gwarancje, aby zapewnić, by IOD działał w sposób niezależny. Administratorzy i podmioty przetwarzające muszą zapewnić, by wykonując swoje zadania w zakresie ochrony danych IOD nie otrzymywał instrukcji ze strony spółki, w tym od najwyższego kierownictwa. Ponadto nie może on być odwoływany ani w żaden sposób karany za wypełnianie swoich zadań[467]. Weźmy na przykład sytuację, gdzie IOD zaleca administratorowi lub podmiotowi przetwarzającemu przeprowadzenie oceny skutków dla ochrony danych, ponieważ uważa, że przetwarzanie może spowodować wysokie ryzyko dla osób, których dane dotyczą. Spółka nie zgadza się z opinią IOD, nie uważa jej za uzasadnioną i w związku z tym postanawia nie przeprowadzać oceny skutków. Spółka może zignorować tę poradę, ale nie może zwolnić IOD ani ukarać go za jej udzielenie.

Wreszcie zadania i obowiązki IOD wyszczególniono w art. 39 RODO. Obejmują one wymóg informowania spółki oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich z mocy prawa i doradzanie im w tej sprawie, jak również monitorowanie przestrzegania przepisów prawa Unii lub państw członkowskich o ochronie danych poprzez przeprowadzanie audytów i szkoleń personelu uczestniczącego w operacjach przetwarzania. Inspektorzy ochrony danych muszą także współpracować z organem nadzorczym i pełnić funkcję punktu kontaktowego dla tego ostatniego w kwestiach związanych z przetwarzaniem danych, takich jak na przykład naruszenie ochrony danych.

Jeśli chodzi o dane osobowe przetwarzane przez instytucje i organy UE, rozporządzenie (WE) nr 45/2001 przewiduje, że każda instytucja i każdy organ UE musi wyznaczyć IOD. Inspektorowi ochrony danych powierza się zadanie polegające na zapewnieniu, by przepisy rozporządzenia były prawidłowo stosowane w instytucjach i organach UE oraz by zarówno osoby, których dane dotyczą, jak i administratorzy danych byli informowani o swoich prawach i obowiązkach[468]. Jest on również odpowiedzialny za odpowiadanie na prośby EIOD i współpracę z nim w razie potrzeby. Podobnie jak RODO, rozporządzenie (WE) nr 45/2001 zawiera przepisy

466 Grupa Robocza Art. 29 (2017), *Guidelines on Data Protection Officers ('DPOs')*, WP 243 rev.01, ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r., pkt 3.1.

467 Ogólne rozporządzenie o ochronie danych, art. 38 ust. 2 i 3.

468 Zob. art. 24 ust. 1 rozporządzenia (WE) nr 45/2001, aby zapoznać się z pełnym wykazem zadań IOD.

dotyczące niezależności IOD w wykonywaniu ich zadań oraz konieczności zapewnienia im niezbędnego personelu i zasobów[469]. Inspektor ochrony danych musi zostać powiadomiony, zanim instytucja lub organ UE (lub służby tych organizacji) przeprowadzi jakiekolwiek operacje przetwarzania danych i musi on prowadzić rejestr wszystkich zgłoszonych operacji przetwarzania danych[470].

4.3.2. Rejestry czynności przetwarzania

Aby móc wykazać zgodność z przepisami i ponosić odpowiedzialność, spółki często mają prawny obowiązek dokumentowania i rejestrowania swojej działalności. Ważnym przykładem jest prawo podatkowe i audyt, które wymagają od wszystkich spółek prowadzenia obszernej dokumentacji i ewidencji. Istotne jest również ustanowienie podobnych wymogów w innych dziedzinach prawa, w szczególności w zakresie prawa ochrony danych, ponieważ prowadzenie rejestrów jest ważnym sposobem na ułatwienie przestrzegania przepisów o ochronie danych. **Prawo UE** stanowi zatem, że administratorzy danych lub ich przedstawiciele muszą prowadzić rejestr czynności przetwarzania, za które odpowiadają[471]. Obowiązek ten ma na celu zapewnienie, aby w razie konieczności organy nadzorcze dysponowały niezbędną dokumentacją umożliwiającą im potwierdzenie, że przetwarzanie danych jest zgodne z prawem.

Dokumentacja obejmuje następujące informacje:

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także, gdy ma to zastosowanie – przedstawiciela administratora oraz IOD;
- cele przetwarzania;
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych związanych z przetwarzaniem;
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione;

469 Rozporządzenie (WE) nr 45/2001, art. 24 ust. 6 i 7.

470 Tamże, art. 25 i 26.

471 Ogólne rozporządzenie o ochronie danych, art. 30.

- informacje, czy doszło lub dojdzie do przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych;

- jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych osobowych, jak również przegląd technicznych i organizacyjnych środków służących zapewnieniu bezpieczeństwa przetwarzania[472].

Obowiązek prowadzenia rejestrów czynności przetwarzania zgodnie z RODO dotyczy nie tylko administratorów danych, ale także podmiotów przetwarzających. Jest to ważna zmiana, ponieważ przed przyjęciem rozporządzenia umowa zawarta między administratorem a podmiotem przetwarzającym obejmowała przede wszystkim zobowiązania podmiotu przetwarzającego. Ich obowiązek prowadzenia dokumentacji jest obecnie bezpośrednio przewidziany w prawie.

Ogólne rozporządzenie o ochronie danych przewiduje wyjątek od tego obowiązku. Wymóg prowadzenia rejestru nie ma zastosowania do przedsiębiorstwa lub organizacji (administratora lub podmiotu przetwarzającego), które zatrudniają mniej niż 250 osób. Wyjątek ten jest jednak uzależniony od spełnienia wymogu, zgodnie z którym dana organizacja nie podejmuje się przetwarzania, które może powodować ryzyko dla praw i wolności osób, których dane dotyczą, przetwarzanie to ma charakter sporadyczny i nie obejmuje szczególnych kategorii danych, o których mowa w art. 9 ust. 1, ani danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o których mowa w art. 10.

Prowadzenie rejestrów czynności przetwarzania powinno umożliwić administratorom i podmiotom przetwarzającym wykazanie zgodności z rozporządzeniem. Powinno również umożliwiać organom nadzorczym monitorowanie, czy przetwarzanie danych jest zgodne z prawem. Jeżeli organ nadzorczy zażąda dostępu do tych rejestrów, administratorzy i podmioty przetwarzające są zobowiązani do współpracy i udostępnienia ich.

4.3.3. Ocena skutków dla ochrony danych i uprzednie konsultacje

Operacje przetwarzania wiążą się z pewnym nieodłącznym ryzykiem dla praw osób fizycznych. Dane osobowe mogą zostać utracone, ujawnione osobom

472 Tamże, art. 30 ust. 1.

nieupoważnionym lub przetworzone w sposób niezgodny z prawem. Oczywiście ryzyko różni się w zależności od charakteru i zakresu przetwarzania. Operacje na dużą skalę obejmujące na przykład przetwarzanie danych szczególnie chronionych wiążą się ze znacznie większym ryzykiem dla osób, których dane dotyczą, w porównaniu z potencjalnym ryzykiem związanym z przetwarzaniem przez małe przedsiębiorstwo adresów i osobistych numerów telefonu swoich pracowników.

W miarę pojawiania się nowych technologii i coraz bardziej złożonego charakteru przetwarzania, administratorzy danych muszą uwzględniać takie zagrożenia poprzez zbadanie prawdopodobnych skutków planowanego przetwarzania przed rozpoczęciem operacji przetwarzania. Umożliwia to organizacjom właściwe rozpoznanie, przeciwdziałanie i łagodzenie ryzyka z wyprzedzeniem, znacznie ograniczając prawdopodobieństwo negatywnych skutków przetwarzania danych dla osób fizycznych.

Oceny skutków w zakresie ochrony danych są przewidziane **zarówno w prawie RE, jak i w prawie UE.** W obrębie ram prawnych RE art. 10 ust. 2 zaktualizowanej konwencji nr 108 wymaga od umawiających się stron zapewnienia, aby administratorzy i podmioty przetwarzające „analizowali prawdopodobne skutki planowanego przetwarzania danych dla praw i podstawowych wolności osób, których dane dotyczą, przed rozpoczęciem takiego przetwarzania" oraz, po dokonaniu oceny, zaprojektowali przetwarzanie w taki sposób, aby zapobiec ryzyku związanemu z przetwarzaniem lub je zminimalizować.

Prawo UE nakłada podobny, bardziej szczegółowy obowiązek na administratorów objętych zakresem RODO. Artykuł 35 przewiduje, że oceny skutków należy dokonać, w przypadku gdy przetwarzanie może powodować wysokie ryzyko dla praw i wolności osób fizycznych. W rozporządzeniu nie określono, w jaki sposób należy oceniać prawdopodobieństwo wystąpienia ryzyka, lecz raczej wskazano na różne możliwości jego wystąpienia[473]. Rozporządzenie zawiera wykaz operacji przetwarzania uznanych za powodujące wysokie ryzyko i w odniesieniu do których uprzednia ocena skutków jest szczególnie konieczna, mianowicie w przypadkach gdy:

- dane osobowe przetwarza się w celu podjęcia decyzji wobec osób fizycznych po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych (profilowania);

473 Ogólne rozporządzenie o ochronie danych, preambuła, motyw 75.

- dane szczególnie chronione lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa przetwarza się na dużą skalę;

- przetwarzanie wiąże się z systematycznym monitorowaniem na dużą skalę miejsc dostępnych publicznie.

Organy nadzorcze ustanawiają i podają do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków. Organy nadzorcze mogą także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania niepodlegających temu wymogowi[474].

W przypadku gdy wymagana jest ocena skutków, administratorzy danych muszą ocenić konieczność i proporcjonalność przetwarzania danych oraz ewentualne ryzyko dla praw osób fizycznych. Ocena skutków musi również zawierać planowane środki bezpieczeństwa mające na celu przeciwdziałanie zidentyfikowanym zagrożeniom. W celu sporządzenia wykazów organy nadzorcze państw członkowskich mają obowiązek wzajemnej współpracy oraz współpracy z Europejską Radą Ochrony Danych. Zapewni to spójne podejście w całej UE do tych operacji, które wymagają oceny skutków, a administratorzy danych będą podlegać podobnym wymogom niezależnie od ich lokalizacji.

Jeżeli ocena skutków wskaże, że przetwarzanie powodowałoby wysokie ryzyko dla praw osób fizycznych i nie zastosowano środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem operacji przetwarzania administrator konsultuje się z odpowiednim organem nadzorczym[475].

Grupa Robocza Art. 29 wydała wytyczne dotyczące oceny skutków dla ochrony danych oraz sposobu ustalania, czy przetwarzanie danych może powodować wysokie ryzyko[476]. Grupa opracowała dziewięć kryteriów, które mają pomóc w określeniu, czy w konkretnym przypadku wymagana jest ocena skutków dla ochrony danych[477]: (1) ocena lub punktacja; (2) zautomatyzowane podejmowanie decyzji

474 Tamże, art. 35 ust. 4 i 5.

475 Tamże, art. 36 ust. 1; Grupa Robocza Art. 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruksela, 4 października 2017 r.

476 Grupa Robocza Art. 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, Bruksela, 4 października 2017 r.

477 Tamże, s. 9–11.

o znaczących skutkach prawnych lub podobnych znaczących skutkach; (3) systematyczne monitorowanie; (4) dane szczególnie chronione; (5) dane przetwarzane na dużą skalę; (6) zestawy danych, które zostały skojarzone lub połączone; (7) dane dotyczące osób, których dane dotyczą, wymagających szczególnej opieki; (8) innowacyjne wykorzystanie lub zastosowanie rozwiązań technologicznych lub organizacyjnych; (9) gdy przetwarzanie samo w sobie „uniemożliwia osobie, której dane dotyczą, wykonywanie prawa lub korzystanie z usługi lub umowy". Grupa Robocza Art. 29 wprowadziła zasadę, że operacje przetwarzania, które spełniają mniej niż dwa kryteria, stanowią niższy poziom ryzyka i nie wymagają oceny skutków dla ochrony danych, podczas gdy operacje, które spełniają dwa lub więcej kryteriów, wymagają takiej oceny. W przypadkach, w których nie jest jasne, czy wymagana jest ocena skutków dla ochrony danych, Grupa Robocza Art. 29 zaleca przeprowadzenie takiej oceny, ponieważ stanowi ona „przydatne narzędzie ułatwiające administratorom przestrzeganie przepisów o ochronie danych"[478]. W przypadku wprowadzenia nowej technologii przetwarzania danych ważne jest przeprowadzenie oceny skutków dla ochrony danych[479].

4.3.4. Kodeksy postępowania

Kodeksy postępowania mają być stosowane w różnych sektorach przemysłu w celu nakreślenia i sprecyzowania stosowania RODO w poszczególnych sektorach. W odniesieniu do administratorów i podmiotów przetwarzających dane osobowe stworzenie takich kodeksów może znacznie poprawić zgodność z przepisami i usprawnić wdrażanie unijnych przepisów o ochronie danych. Wiedza fachowa członków sektora będzie sprzyjać znajdowaniu rozwiązań praktycznych, a zatem możliwych do zastosowania w przyszłości. Uznając znaczenie takich kodeksów dla skutecznego stosowania prawa o ochronie danych, w RODO wzywa się państwa członkowskie, organy nadzorcze, Komisję i Europejską Radę Ochrony Danych do propagowania sporządzania kodeksów postępowania mających pomóc we właściwym stosowaniu rozporządzenia w całej UE[480]. Kodeksy mogłyby określać stosowanie rozporządzenia w poszczególnych sektorach, w tym w takich kwestiach, jak zbieranie danych osobowych, informacje, które należy przekazywać osobom, których dane dotyczą, i opinii publicznej, oraz wykonywanie praw osób, których dane dotyczą.

478 Tamże, s. 9.

479 Tamże.

480 Ogólne rozporządzenie o ochronie danych, art. 40 ust. 1.

W celu zapewnienia zgodności kodeksów postępowania z zasadami określonymi w RODO, kodeksy te muszą zostać przedłożone właściwemu organowi nadzorczemu przed ich przyjęciem. Organ nadzorczy wydaje opinię, czy przedstawiony projekt kodeksu sprzyja zapewnieniu zgodności z rozporządzeniem i zatwierdza taki projekt kodeksu, jeżeli uzna, że ustanawia on odpowiednie zabezpieczenia[481]. Organ nadzorczy musi opublikować zatwierdzony kodeks wraz z kryteriami stanowiącymi podstawę jego zatwierdzenia. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, właściwy organ nadzorczy przed zatwierdzeniem projektu kodeksu, zmiany lub rozszerzenia przedkłada go Europejskiej Radzie Ochrony Danych, która wydaje opinię o zgodności kodeksu z RODO. Komisja może, w drodze aktów wykonawczych, stwierdzić, że przedłożony jej zatwierdzony kodeks postępowania jest powszechnie obowiązujący w Unii.

Przestrzeganie kodeksu postępowania przynosi istotne korzyści zarówno osobom, których dane dotyczą, jak i administratorom i podmiotom przetwarzającym. Kodeksy takie zawierają szczegółowe wytyczne, które dostosowują wymogi prawne do poszczególnych sektorów i zwiększają przejrzystość czynności przetwarzania. Administratorzy i podmioty przetwarzające mogą również wykorzystać przestrzeganie kodeksów jako wyraźny dowód ich zgodności z prawem UE oraz jako środek służący poprawie ich wizerunku publicznego jako organizacji, które w swoich działaniach traktują ochronę danych priorytetowo i zobowiązują się do przestrzegania jej zasad. Zatwierdzone kodeksy postępowania, wraz z wiążącymi i egzekwowalnymi zobowiązaniami, mogą być stosowane jako odpowiednie zabezpieczenia przy przekazywaniu danych do państw trzecich. Aby zapewnić rzeczywiste stosowanie kodeksów postępowania można wyznaczyć specjalny podmiot (akredytowany przez właściwy organ nadzorczy) w celu monitorowania i zapewnienia ich przestrzegania. Aby organ ten mógł skutecznie wypełniać swoje zadania, musi być niezależny, posiadać udokumentowaną wiedzę fachową w kwestiach regulowanych kodeksem postępowania oraz przejrzyste procedury i struktury umożliwiające mu rozpatrywanie skarg dotyczących naruszeń kodeksu[482].

W prawie RE zaktualizowana konwencja nr 108 stanowi, że poziom ochrony danych gwarantowany przez prawo krajowe może zostać skutecznie wzmocniony dzięki dobrowolnym środkom regulacyjnym, takim jak kodeksy dobrych praktyk lub kodeksy postępowania zawodowego. Jednakże są to jedynie środki dobrowolne na

481 Tamże, art. 40 ust. 5.

482 Tamże, art. 41 ust. 1 i 2.

gruncie zaktualizowanej konwencji nr 108: nie mogą stanowić podstawy dla żadnego zobowiązania prawnego do wprowadzenia takich środków, chociaż jest to wskazane, a środki takie same w sobie nie są wystarczające do zapewnienia pełnej zgodności z konwencją[483].

4.3.5. Certyfikacja

Oprócz kodeksów postępowania, kolejnym sposobem wykazania zgodności z RODO przez administratorów i podmioty przetwarzające są mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych. W tym celu rozporządzenie przewiduje dobrowolny system certyfikacji, w ramach którego niektóre jednostki lub organy nadzorcze mogą wydawać certyfikaty. Administratorzy i podmioty przetwarzające, którzy zdecydują się przystąpić do mechanizmu certyfikacji, mogą zyskać większą widoczność i wiarygodność, ponieważ certyfikacje, znaki jakości i oznaczenia umożliwiają osobom, których dane dotyczą, szybką ocenę poziomu ochrony organizacji w zakresie przetwarzania danych. Co ważne, fakt posiadania takiego certyfikatu przez administratora lub podmiot przetwarzający nie ogranicza jego obowiązków i odpowiedzialności w zakresie spełnienia wszystkich wymogów rozporządzenia.

4.4. Ochrona danych w fazie projektowania oraz domyślna ochrona danych

Ochrona danych w fazie projektowania

Prawo UE wymaga od administratorów wprowadzenia środków służących skutecznemu wdrażaniu zasad ochrony danych i nadaniu przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi rozporządzenia oraz chronić prawa osób, których dane dotyczą[484]. Środki te powinny zostać wdrożone zarówno podczas samego przetwarzania, jak i przy określaniu sposobów przetwarzania. Wdrażając te środki, administrator musi wziąć pod uwagę aktualny stan wiedzy technicznej, koszty

483 Explanatory Report of Modernised Convention 108, pkt 33.

484 Ogólne rozporządzenie o ochronie danych, art. 25 ust. 1.

wdrażania, charakter, zakres i cele przetwarzania danych osobowych oraz ryzyko naruszenia praw i wolności osoby, której dane dotyczą, i jego wagę[485].

Prawo RE wymaga, aby przed rozpoczęciem przetwarzania administratorzy i podmioty przetwarzające dokonali oceny prawdopodobnego wpływu przetwarzania danych osobowych na prawa i wolności osób, których dane dotyczą. Ponadto administratorzy i podmioty przetwarzające są zobowiązani do zaprojektowania przetwarzania danych w taki sposób, aby zapobiec ryzyku ingerencji w te prawa i wolności lub zminimalizować to ryzyko oraz do wdrożenia środków technicznych i organizacyjnych, które uwzględniają skutki prawa do ochrony danych osobowych na wszystkich etapach przetwarzania[486].

Domyślna ochrona danych

Prawo UE wymaga, aby administrator wdrażał odpowiednie środki w celu zapewnienia, by domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia celu. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności[487]. W szczególności środek taki zapewnia, by dane osobowe osób, których dane dotyczą, nie były udostępniane wszystkim pracownikom administratorów. Dalsze wytyczne EIOD opracował w dokumencie zatytułowanym *Necessity Toolkit*[488].

Prawo RE wymaga od administratorów i podmiotów przetwarzających wdrożenia środków technicznych i organizacyjnych w celu rozważenia skutków prawa do ochrony danych oraz wdrożenia środków technicznych i organizacyjnych, które uwzględniają skutki prawa do ochrony danych osobowych na wszystkich etapach przetwarzania[489].

485 Zob. Grupa Robocza Art. 29 (2017), *Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679*, WP 248 rev.01, 4 października 2017 r. Zob. także ENISA (2015), *Privacy and Data Protection by Design-from policy to engineering*, 12 stycznia 2015 r.

486 Zaktualizowana konwencja nr 108, art. 10 ust. 2 i 3, Explanatory Report of Modernised Convention 108, pkt 89.

487 Ogólne rozporządzenie o ochronie danych, art. 25 ust. 2.

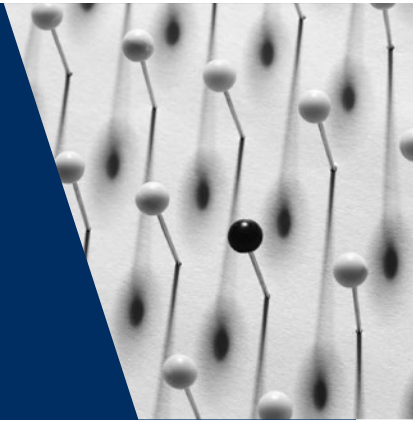
488 Europejski Inspektor Ochrony Danych (EIOD), (2017), *Necessity Toolkit*, Bruksela, 11 kwietnia 2017 r.

489 Zaktualizowana konwencja nr 108, art. 10 ust. 3, Explanatory Report of the Modernised Convention 108, pkt 89.

W 2016 r. ENISA opublikowała sprawozdanie na temat dostępnych narzędzi i usług w zakresie ochrony prywatności[490]. Ocena ta zawiera między innymi wykaz kryteriów i parametrów, które są wskaźnikami dobrych lub złych praktyk w zakresie ochrony prywatności. Podczas gdy niektóre kryteria odnoszą się bezpośrednio do przepisów RODO – takich jak stosowanie pseudonimizacji i zatwierdzonych mechanizmów certyfikacji – inne dostarczają innowacyjnych inicjatyw w celu zapewnienia ochrony prywatności w fazie projektowania i domyślnej ochrony prywatności. Na przykład kryterium użyteczności, choć nie jest bezpośrednio związane z prywatnością, może zwiększyć prywatność, ponieważ może umożliwić szersze zastosowanie narzędzia lub usługi związanej z prywatnością. Narzędzia służące ochronie prywatności, które są trudne do wdrożenia w praktyce, mogą być przyjmowane przez ogół społeczeństwa na bardzo niskim poziomie, nawet jeżeli oferują bardzo silne gwarancje ochrony prywatności. Ponadto kluczowe znaczenie ma kryterium dojrzałości i stabilności narzędzia ochrony prywatności – czyli sposób, w jaki narzędzie to ewoluuje w czasie i odpowiada na istniejące lub nowe wyzwania związane z prywatnością. Inne technologie zwiększające ochronę prywatności, na przykład w kontekście bezpiecznej komunikacji, obejmują szyfrowanie typu end-to-end (komunikacja, w której jedynymi osobami, które mogą odczytać wiadomości, są osoby komunikujące się); szyfrowanie typu klient-serwer (szyfrowanie kanału komunikacyjnego utworzonego między klientem a serwerem); uwierzytelnianie (weryfikacja tożsamości komunikujących się stron); oraz komunikację anonimową (żadna osoba trzecia nie jest w stanie zidentyfikować komunikujących się stron).

490 ENISA, PETs controls matrix: A systematic approach for assessing online and mobile privacy tools, 20 grudnia 2016 r.

5 Niezależny nadzór



UE	Omówione zagadnienia	RE
Artykuł 8 ust. 3 Karty praw podstawowych Artykuł 16 ust. 2 Traktatu o funkcjonowaniu Unii Europejskiej Artykuły 51–59 ogólnego rozporządzenia o ochronie danych TSUE, C-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec* [WI], 2010 TSUE, C-614/10, *Komisja Europejska przeciwko Republice Austrii* [WI], 2012 TSUE, C-288/12, *Komisja Europejska przeciwko Węgrom* [WI], 2014 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 2015	**Organy nadzorcze**	Artykuł 15 zaktualizowanej konwencji nr 108
Artykuły 60–67 ogólnego rozporządzenia o ochronie danych	**Współpraca między organami nadzorczymi**	Artykuły 16–21 zaktualizowanej konwencji nr 108
Artykuły 68–76 ogólnego rozporządzenia o ochronie danych	**Europejska Rada Ochrony Danych**	

Najważniejsze kwestie

- Niezależny nadzór jest zasadniczym elementem europejskiego prawa ochrony danych i jest zapisany w art. 8 ust. 3 karty.
- Aby zapewnić skuteczną ochronę danych, na mocy prawa krajowego muszą zostać ustanowione niezależne organy nadzorcze.
- Organy nadzorcze muszą działać w sposób całkowicie niezależny, co trzeba zagwarantować w ustanawiającym je prawie i musi to znaleźć odzwierciedlenie w konkretnej strukturze organizacyjnej organu nadzorczego.
- Organy nadzorcze posiadają szczególne uprawnienia i realizują szczególne zadania. Do zadań organów nadzorczych należy między innymi:
  - monitorowanie i promowanie ochrony danych na szczeblu krajowym;
  - doradzanie osobom, których dane dotyczą, i administratorom, jak również rządowi oraz ogółowi społeczeństwa;
  - rozpatrywanie skarg i pomoc osobom, których dane dotyczą, w przypadku zarzucanych naruszeń prawa do ochrony danych;
  - nadzór nad administratorami i podmiotami przetwarzającymi;
- W razie konieczności organy nadzorcze są także uprawnione do interwencji przez:
  - ostrzeganie, upominanie bądź nawet karanie administratorów i podmiotów przetwarzających;
  - nakazywanie sprostowania, zablokowania lub usunięcia danych;
  - nakładanie zakazu przetwarzania lub administracyjnej kary pieniężnej;
  - kierowanie spraw do sądu.
- Ponieważ przetwarzanie danych osobowych często obejmuje administratorów, podmioty przetwarzające i osoby, których dane dotyczą, znajdujące się w różnych państwach, organy nadzorcze są zobowiązane do wzajemnej współpracy w kwestiach transgranicznych w celu zapewnienia skutecznej ochrony osób fizycznych w Europie.

- Ogólne rozporządzenie o ochronie danych ustanawia w UE mechanizm kompleksowej współpracy w sprawach dotyczących przetwarzania transgranicznego. Niektóre przedsiębiorstwa prowadzą działalność transgraniczną w zakresie przetwarzania danych wynikającą z przetwarzania danych osobowych w ramach działalności jednostek organizacyjnych w więcej niż jednym państwie członkowskim lub w ramach działalności pojedynczej jednostki organizacyjnej w Unii, ale która znacznie wpływa na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim. W ramach tego mechanizmu takie przedsiębiorstwa będą miały do czynienia tylko z jednym krajowym organem nadzorczym w zakresie ochrony danych.
- Mechanizm współpracy i spójności pozwoli na skoordynowane podejście wszystkich organów nadzorczych zaangażowanych w daną sprawę. Wiodący organ nadzorczy – główny lub pojedynczej jednostki organizacyjnej – skonsultuje się z pozostałymi organami nadzorczymi, których sprawa dotyczy, i przedstawi im projekt decyzji.
- Podobnie jak obecna Grupa Robocza Art. 29, organ nadzorczy każdego państwa członkowskiego i Europejski Inspektor Ochrony Danych (EIOD) będą członkami Europejskiej Rady Ochrony Danych.
- Do zadań Europejskiej Rady Ochrony Danych należy na przykład monitorowanie prawidłowego stosowania rozporządzenia, doradzanie Komisji w istotnych kwestiach oraz wydawanie opinii, wytycznych lub najlepszych praktyk w różnych dziedzinach.
- Główna różnica polega na tym, że Europejska Rada Ochrony Danych nie tylko będzie wydawać opinie, jak na mocy dyrektywy 95/46/WE. Będzie ona również wydawać wiążące decyzje dotyczące spraw, w których organ nadzorczy wniósł mający znaczenie dla sprawy i uzasadniony sprzeciw w przypadku mechanizmów kompleksowej współpracy, w których występują sprzeczne opinie co do tego, który z organów nadzorczych jest wiodącym organem, oraz w których właściwy organ nadzorczy nie zwraca się o opinię lub nie zastosuje się do opinii EROD. Celem jest zapewnienie spójnego stosowania rozporządzenia we wszystkich państwach członkowskich.

Niezależny nadzór jest zasadniczym elementem europejskiego prawa ochrony danych. Zarówno prawo UE, jak i prawo RE uznają istnienie niezależnych organów nadzorczych za niezbędne dla skutecznej ochrony praw i wolności osób fizycznych w zakresie przetwarzania ich danych osobowych. Ponieważ przetwarzanie danych jest obecnie coraz powszechniejsze i coraz trudniejsze do zrozumienia dla osób fizycznych, organy te są strażnikami w erze cyfrowej. W UE istnienie niezależnych organów nadzorczych uznaje się za jeden z najważniejszych elementów prawa do ochrony danych osobowych, zapisanego w prawie pierwotnym UE. W art. 8 ust. 3 Karty praw podstawowych UE i art. 16 ust. 2 TFUE uznaje się ochronę danych osobowych za prawo podstawowe i potwierdza, że przestrzeganie przepisów o ochronie danych musi podlegać kontroli niezależnego organu.

Znaczenie niezależnego nadzoru dla prawa ochrony danych zostało również uznane w orzecznictwie.

Przykład: W sprawie *Schrems*[491] TSUE rozważał, czy przekazywanie danych osobowych Stanom Zjednoczonym (USA) w ramach pierwszego porozumienia UE–USA w sprawie „bezpiecznej przystani" jest zgodne z prawem UE dotyczącym ochrony danych w świetle doniesień Edwarda Snowdena na temat prowadzenia przez amerykańską National Security Agency masowej inwigilacji. Przekazywanie danych osobowych do USA opierało się na decyzji Komisji Europejskiej przyjętej w 2000 r., w której zezwolono na przekazywanie danych osobowych z UE do organizacji amerykańskich, które dokonują samocertyfikacji o przystąpieniu do programu „bezpiecznej przystani", pod warunkiem że zapewnia on odpowiedni poziom ochrony danych osobowych. Irlandzki organ nadzorczy odrzucił skargę skarżącego w przedmiocie zgodności z prawem przekazywania danych po doniesieniach Snowdena, ponieważ istnienie decyzji Komisji w sprawie adekwatności amerykańskiego systemu ochrony danych, odzwierciedlonej w zasadach „bezpiecznej przystani" („decyzja w sprawie »bezpiecznej przystani«"), uniemożliwiło mu dalsze badanie skargi.

Trybunał Sprawiedliwości stwierdził jednak, że istnienie decyzji Komisji zezwalającej na przekazywanie danych do państw trzecich, które zapewniają odpowiedni poziom ochrony, nie eliminuje ani nie ogranicza uprawnień krajowych organów nadzorczych. Trybunał zauważył, że uprawnienia tych organów do monitorowania i zapewniania przestrzegania unijnych przepisów o ochronie danych wynikają z prawa pierwotnego UE, w szczególności z art. 8 ust. 3 karty i art. 16 ust. 2 TFUE. „Ustanowienie w państwach członkowskich niezależnych organów nadzorczych stanowi zatem [...] istotny element ochrony osób w związku z przetwarzaniem danych osobowych"[492].

Trybunał orzekł zatem, że nawet w przypadku, gdy przekazanie danych osobowych było przedmiotem decyzji Komisji w sprawie odpowiedniego poziomu ochrony, w przypadku złożenia skargi do krajowego organu nadzorczego organ ten zobowiązany jest do rozpatrzenia tej skargi z wszelką wymaganą

491 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

492 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r., pkt 41.

starannością. Organ nadzorczy może odrzucić skargę, jeśli uzna ją za bezzasadną. W takim przypadku, jak podkreślił TSUE, prawo do skutecznego środka prawnego wymaga, by osoby fizyczne miały możliwość zaskarżenia takiej decyzji do sądów krajowych, które mogą skierować sprawę do TSUE w celu wydania orzeczenia w trybie prejudycjalnym w przedmiocie ważności decyzji Komisji. W przypadku gdy organ nadzorczy uzna skargę za zasadną, musi mieć możliwość wszczęcia postępowania sądowego i wniesienia sprawy do sądów krajowych. Sądy krajowe mogą skierować sprawę do TSUE, ponieważ jest on jedynym organem uprawnionym do orzekania w przedmiocie ważności decyzji Komisji w sprawie adekwatności[493].

Następnie TSUE zbadał ważność decyzji w sprawie „bezpiecznej przystani", aby ustalić, czy system przekazywania danych jest zgodny z unijnymi przepisami o ochronie danych. Trybunał stwierdził, że art. 3 decyzji w sprawie „bezpiecznej przystani" ograniczył uprawnienia krajowych organów nadzorczych (przyznane na mocy dyrektywy o ochronie danych) do podejmowania działań zapobiegających przekazywaniu danych w przypadku nieodpowiedniego poziomu ochrony danych osobowych w USA. Ze względu na znaczenie niezależnych organów nadzorczych dla zapewnienia zgodności z prawem o ochronie danych TSUE uznał, że na mocy dyrektywy o ochronie danych i w świetle karty Komisja nie jest uprawniona do ograniczania w ten sposób uprawnień niezależnych organów nadzorczych. Ograniczenie uprawnień organów nadzorczych było jedną z przyczyn, dla których TSUE stwierdził nieważność decyzji w sprawie „bezpiecznej przystani".

W związku z tym prawo europejskie wymaga niezależnego nadzoru jako ważnego mechanizmu zapewniającego skuteczną ochronę danych. Niezależne organy nadzorcze są pierwszym punktem kontaktowym dla osób, których dane dotyczą, w przypadku naruszenia prywatności[494]. Zgodnie z prawem UE i prawem RE ustanowienie organów nadzorczych jest obowiązkowe. Obydwie ramy prawne opisują zadania i uprawnienia tych organów w sposób podobny do tych zawartych w RODO. W związku z tym organy nadzorcze powinny zasadniczo funkcjonować w taki sam sposób na mocy prawa UE i prawa RE[495].

493 Tamże, pkt 53–66.

494 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 2 lit. d).

495 Tamże, art. 51, zaktualizowana konwencja nr 108, art. 12a.

5.1. Niezależność

Prawo UE i **prawo RE** wymagają, by każdy organ nadzorczy podczas wypełniania swoich zadań i wykonywania swoich uprawnień działał w sposób w pełni niezależny[496]. Niezależność organu nadzorczego i jego członków, jak również personelu od bezpośrednich lub pośrednich wpływów zewnętrznych, ma zasadnicze znaczenie dla zagwarantowania pełnej obiektywności przy podejmowaniu decyzji w sprawach dotyczących ochrony danych. Ustawa, na mocy której ustanawiany jest organ nadzorczy, musi zawierać konkretne przepisy gwarantujące jego niezależność, a ponadto struktura organizacyjna tego organu musi dowodzić jego niezależności. W 2010 r. TSUE zajął się po raz pierwszy pytaniem o zakres wymogu niezależności organów nadzorczych[497]. Rozumowanie Trybunału w przedmiocie definicji pojęcia „całkowitej niezależności" obrazują poniższe przykłady.

Przykład: W sprawie *Komisja Europejska przeciwko Republice Federalnej Niemiec*[498] Komisja Europejska zwróciła się do TSUE o stwierdzenie, że Niemcy dokonały nieprawidłowej transpozycji wymogu „całkowitej niezależności" organów nadzorczych odpowiedzialnych za zapewnienie ochrony danych, a tym samym uchybiły zobowiązaniom ciążącym na nich na mocy art. 28 ust. 1 dyrektywy o ochronie danych. Zdaniem Komisji uchybienie wymogowi niezależności polegało na tym, że Niemcy poddały nadzorowi państwa organy odpowiedzialne za monitorowanie przetwarzania danych osobowych poza sektorem publicznym w poszczególnych krajach związkowych w celu zapewnienia zgodności z prawem o ochronie danych.

Trybunał podkreślił, że słowa „całkowicie niezależne" należy interpretować w oparciu o rzeczywiste brzmienie tego przepisu oraz cele i systematykę prawa UE o ochronie danych[499]. Trybunał zaznaczył, że organy nadzorcze są „strażnikami" praw związanych z przetwarzaniem danych osobowych. Wobec tego ich ustanowienie w państwach członkowskich jest uznawane za „istotny

496 Ogólne rozporządzenie o ochronie danych, art. 52 ust. 1; zaktualizowana konwencja nr 108, art. 15 ust. 5.

497 FRA (2010), Fundamental rights: challenges and achievements in 2010, Annual report 2010, s. 59; FRA (2010), Data protection in the European Union: the role of National Data Protection Authorities, maja 2010 r.

498 TSUE, C-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec* [WI], 9 marca 2010 r., pkt 27.

499 Tamże, pkt 17 i 29.

element ochrony osób w związku z przetwarzaniem danych osobowych”[500]. Trybunał stwierdził, że „przy wykonywaniu swoich obowiązków organy nadzorczych powinny działać w sposób obiektywny i bezstronny. W tym celu powinny pozostawać poza jakimkolwiek wpływem z zewnątrz, w tym bezpośrednim czy pośrednim wpływem państwa”[501].

TSUE ustalił również, że pojęcie „całkowitej niezależności” należy interpretować w świetle niezależności EIOD zgodnie z definicją zawartą w rozporządzeniu o ochronie danych przez instytucje UE. W tym rozporządzeniu pojęcie niezależności wymaga, by podczas wykonywania swoich obowiązków EIOD nie oczekiwał i nie przyjmował instrukcji od nikogo.

W związku z tym TSUE orzekł, że organy nadzorcze w Niemczech – ze względu na nadzór organów publicznych – nie są całkowicie niezależne w rozumieniu unijnego prawa o ochronie danych.

Przykład: W sprawie *Komisja Europejska przeciwko Republice Austrii*[502] TSUE wskazał podobne problemy dotyczące sytuacji niektórych członków i pracowników austriackiego urzędu ochrony danych (Komisji Ochrony Danych – DSK). Trybunał stwierdził, że fakt, iż Bundeskanzleramt zapewniał organowi nadzorczemu pracowników, podważa wymóg niezależności określony w unijnym prawie o ochronie danych. Trybunał orzekł także, że wymóg stałego informowania Bundeskanzleramt o jego pracy zaprzecza pełnej niezależności organu nadzorczego.

Przykład: W sprawie *Komisja Europejska przeciwko Węgrom*[503] zakazano podobnych praktyk krajowych mających wpływ na niezależność pracowników. Trybunał Sprawiedliwości wskazał, że „wymóg [...], wedle którego należy zapewnić, aby każdy organ nadzorczy wykonywał w sposób całkowicie niezależny powierzone mu funkcje, oznacza ciążący na danym państwie członkowskim obowiązek poszanowania kadencji takiego organu aż do jej pierwotnie przewidzianego zakończenia”. Trybunał orzekł także, że

500 Tamże, pkt 23.

501 Tamże, pkt 25.

502 TSUE, C-614/10, *Komisja Europejska przeciwko Republice Austrii* [WI], 16 października 2012 r., pkt 59 i 63.

503 TSUE, C-288/12, *Komisja Europejska przeciwko Węgrom* [WI], 8 kwietnia 2014 r., pkt 50 i 67.

> „Węgry uchybiły zobowiązaniom, które na nich ciążą na mocy dyrektywy 95/46/WE [...], w ten sposób, że skróciły kadencję organu nadzorczego ochrony danych osobowych".

Pojęcie i kryteria „całkowitej niezależności" są obecnie wyraźnie określone w RODO, które uwzględnia zasady ustanowione w opisanych orzeczeniach TSUE. Zgodnie z rozporządzeniem[504] całkowita niezależność w toku wypełniania swoich zadań i wykonywania swoich uprawnień oznacza, że:

- członkowie każdego organu nadzorczego pozostają wolni od bezpośrednich i pośrednich wpływów zewnętrznych, nie zwracają się do nikogo o instrukcje ani od nikogo ich nie przyjmują;
- członkowie każdego organu nadzorczego powstrzymują się od wszelkich czynności sprzecznych ze swoimi obowiązkami, aby zapobiegać konfliktom interesów;
- państwa członkowskie zapewniają, by każdy organ nadzorczy dysponował zasobami kadrowymi, technicznymi i finansowymi i infrastrukturą niezbędnymi do skutecznego wypełniania swoich zadań;
- państwa członkowskie zapewniają, by każdy organ nadzorczy wybierał własny personel;
- kontrola finansowa, której podlega każdy organ nadzorczy zgodnie z prawem krajowym nie może naruszać jego niezależności. Organy nadzorcze muszą dysponować odrębnym, publicznym budżetem rocznym, który umożliwia im właściwe funkcjonowanie.

Niezależność organów nadzorczych jest również uznawana za zasadniczy wymóg w prawie RE. Zaktualizowana konwencja nr 108 wymaga, aby organy nadzorcze „działały w sposób całkowicie niezależny i bezstronny przy wypełnianiu swoich zadań i wykonywaniu swoich uprawnień", nie zwracając się o instrukcje ani ich nie przyjmując[505]. W ten sposób w konwencji uznano, że organy te nie mogą skutecznie chronić praw i wolności osób fizycznych związanych z przetwarzaniem danych, jeżeli nie pełnią swoich funkcji w sposób całkowicie niezależny. W sprawozdaniu

504 Ogólne rozporządzenie o ochronie danych, art. 52.

505 Zaktualizowana konwencja nr 108, art. 15 ust. 5.

wyjaśniającym do zaktualizowanej konwencji nr 108 określono szereg elementów, które przyczyniają się do ochrony tej niezależności. Elementy te obejmują możliwość zatrudniania własnego personelu przez organy nadzorcze oraz podejmowania decyzji bez ingerencji z zewnątrz, a także czynniki związane z czasem sprawowania przez nie funkcji i warunkami, na jakich mogą one zaprzestać pełnienia swoich funkcji[506].

5.2. Właściwość i uprawnienia

W prawie UE w RODO przedstawiono zarys właściwości i struktury organizacyjnej organów nadzorczych i przewidziano ich właściwość i uprawnienia do pełnienia funkcji wymaganych na mocy rozporządzenia.

Organ nadzorczy jest głównym organem w prawie krajowym, który zapewnia zgodność z unijnym prawem o ochronie danych. Organy nadzorcze dysponują kompleksowym katalogiem zadań i uprawnień wykraczających poza monitorowanie, które obejmują proaktywne i zapobiegawcze działania nadzorcze. W celu wykonywania tych zadań organy nadzorcze muszą posiadać odpowiednie uprawnienia w zakresie prowadzonych postępowań, uprawnienia naprawcze i doradcze, wymienione w art. 58 RODO, takie jak uprawnienia do[507]:

- udzielania porad administratorom i osobom, których dane dotyczą we wszelkich kwestiach związanych z ochroną danych;
- zatwierdzania standardowych klauzul umownych, wiążących reguł korporacyjnych lub uzgodnień administracyjnych;
- badania operacji przetwarzania i odpowiedniej interwencji;
- żądania przedłożenia wszelkich informacji wymaganych w celu nadzorowania czynności administratora;
- ostrzeżenia lub udzielenia upomnienia i nakazania przesłania zgłoszeń o naruszeniach ochrony danych osobom, których dane dotyczą;

506 Explanatory Report of Modernised Convention 108.

507 Ogólne rozporządzenie o ochronie danych, art. 58. Zob. także konwencja nr 108, protokół dodatkowy, art. 1.

- nakazania sprostowania, zablokowania, usunięcia lub zniszczenia tych danych;
- nałożenia czasowego lub całkowitego zakazu przetwarzania lub nałożenia administracyjnych kar finansowych;
- skierowania sprawy do sądu.

W celu pełnienia swoich funkcji, organ nadzorczy musi mieć dostęp do wszystkich danych osobowych i informacji niezbędnych do przeprowadzenia dochodzenia, jak również do wszelkich pomieszczeń, w których administrator przechowuje istotne informacje. Zdaniem TSUE uprawnienia organu nadzorczego należy interpretować szeroko, aby zapewnić pełną skuteczność ochrony danych osób, których dane dotyczą, w UE.

Przykład: W sprawie *Schrems* TSUE rozważał, czy przekazywanie danych osobowych Stanom Zjednoczonym (USA) w ramach pierwszego porozumienia UE–USA w sprawie „bezpiecznej przystani" było zgodne z prawem UE dotyczącym ochrony danych w świetle doniesień Edwarda Snowdena. W swoim toku rozumowania TSUE stwierdził, że krajowe organy nadzorcze – działając jako niezależni kontrolerzy przetwarzania danych przez administratorów – mogą uniemożliwić przekazanie danych osobowych do państwa trzeciego pomimo istnienia decyzji w sprawie adekwatności, jeżeli istnieją uzasadnione dowody na to, że w państwie trzecim nie ma już gwarancji odpowiedniej ochrony[508].

Każdy organ nadzorczy jest właściwy do wykonywania uprawnień w zakresie prowadzonych postępowań oraz uprawnień w zakresie interwencji na terytorium objętym zakresem swojego działania. Ponieważ jednak działalność administratorów i podmiotów przetwarzających ma często charakter transgraniczny, a przetwarzanie danych ma wpływ na osoby, których dane dotyczą, znajdujące się w wielu państwach członkowskich, pojawia się pytanie o podział właściwości między różnymi organami nadzorczymi. Trybunał Sprawiedliwości Unii Europejskiej miał okazję zbadać tę kwestię w sprawie *Weltimmo*.

508 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r., pkt 26–36 i 40–41.

Przykład: W sprawie *Weltimmo*[509] przedmiotem rozważań TSUE była właściwość krajowych organów nadzorczych do rozpatrywania kwestii dotyczących organizacji niemających siedziby w ramach ich jurysdykcji. Weltimmo było spółką zarejestrowaną na Słowacji, prowadzącą stronę internetową z ogłoszeniami dotyczącymi nieruchomości położonych na Węgrzech. Ogłoszeniodawcy złożyli skargi do węgierskiego organu nadzorczego w zakresie ochrony danych w związku z naruszeniem węgierskiego prawa o ochronie danych, a organ nałożył na Weltimmo grzywnę. Spółka zaskarżyła grzywnę do sądów krajowych, a sprawę skierowano do TSUE w celu ustalenia, czy dyrektywa UE o ochronie danych zezwalała na zastosowanie przez organy nadzorcze państwa członkowskiego swoich krajowych przepisów o ochronie danych w odniesieniu do spółki zarejestrowanej w innym państwie członkowskim.

Zgodnie z wykładnią zaproponowaną przez TSUE, art. 4 ust. 1 lit. a) dyrektywy o ochronie danych zezwala na zastosowanie przepisów prawnych dotyczących ochrony danych państwa członkowskiego innego niż państwo, w którym zarejestrowany jest administrator tych danych, „o ile prowadzi on poprzez stabilne rozwiązanie organizacyjne na terytorium tego państwa członkowskiego faktyczną i rzeczywistą działalność, choćby nawet drobną, w której kontekście dokonuje się rozpatrywanego przetwarzania". Trybunał zauważył, że z informacji przedstawionych w sprawie wynika, iż Weltimmo prowadziło rzeczywistą i faktyczną działalność na Węgrzech, ponieważ spółka miała na Węgrzech swojego przedstawiciela wpisanego do słowackiego rejestru spółek pod adresem węgierskim, a także węgierski rachunek bankowy i skrzynkę pocztową, a także prowadziła działalność na Węgrzech na piśmie w języku węgierskim. Informacje te wskazywały na istnienie działalności gospodarczej i powodowały, że działalność Weltimmo podlegałaby węgierskiej ustawie o ochronie danych oraz jurysdykcji węgierskiego organu nadzorczego. Trybunał pozostawił jednak do rozstrzygnięcia sądowi krajowemu weryfikację tych informacji i ustalenie, czy Weltimmo prowadziło działalność gospodarczą na Węgrzech.

Gdyby sąd odsyłający uznał, że Weltimmo prowadziło działalność gospodarczą na Węgrzech, węgierski organ nadzorczy miałby prawo nałożyć grzywnę. Niemniej jednak, gdyby sąd krajowy orzekł inaczej, tj.

509 TSUE, C-230/14, *Weltimmo s.r.o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 października 2015 r.

gdyby Weltimmo nie prowadziło działalności gospodarczej na Węgrzech, prawem właściwym byłoby prawo państwa członkowskiego (państw członkowskich), w którym (których) spółka była zarejestrowana. W tym przypadku, ponieważ uprawnienia organów nadzorczych muszą być wykonywane zgodnie z suwerennością terytorialną innych państw członkowskich, organy węgierskie nie miałyby możliwości nakładania grzywien. Ponieważ dyrektywa o ochronie danych nałożyła na organy nadzorcze obowiązek współpracy, organ węgierski mogły jednak zwrócić się do słowackiego odpowiednika o zbadanie sprawy, stwierdzenie naruszenia prawa słowackiego i nałożenie grzywien przewidzianych w słowackim ustawodawstwie.

Wraz z przyjęciem RODO wprowadzono szczegółowe przepisy dotyczące właściwości organów nadzorczych w sprawach transgranicznych. Rozporządzenie ustanawia „mechanizm kompleksowej współpracy" i zawiera przepisy nakładające obowiązek współpracy między różnymi organami nadzorczymi. Aby zapewnić skuteczną współpracę w sprawach transgranicznych RODO wymaga, by wiodący organ nadzorczy był właściwy do podejmowania działań jako organ nadzorczy głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego[510]. Wiodący organ nadzorczy jest odpowiedzialny za sprawy transgraniczne, a inne organy nadzorcze komunikują się jedynie z wiodącym organem nadzorczym, który też koordynuje współpracę z nimi. Współpraca obejmuje wymianę informacji, wzajemną pomoc w zakresie monitorowania, prowadzenia postępowań i podejmowania wiążących decyzji[511].

W prawie RE właściwość i uprawnienia organów nadzorczych zostały określone w art. 15 zaktualizowanej konwencji nr 108. Uprawnienia te odpowiadają uprawnieniom nadanym organom nadzorczym na mocy prawa UE, w tym uprawnieniom do prowadzenia postępowań i interweniowania, uprawnieniom do wydawania decyzji i nakładania sankcji administracyjnych w przypadku naruszenia postanowień konwencji oraz uprawnieniom do udziału w postępowaniach sądowych. Niezależne organy nadzorcze są również uprawnione do rozpatrywania wniosków i skarg składanych przez osoby, których dane dotyczą, do podnoszenia świadomości społecznej w zakresie prawa o ochronie danych oraz do doradzania krajowym decydentom w zakresie aktów prawnych i administracyjnych środków przewidujących przetwarzanie danych osobowych.

510 Ogólne rozporządzenie o ochronie danych, art. 56 ust. 1.

511 Tamże, art. 60.

5.3. Współpraca

Ogólne rozporządzenie o ochronie danych ustanawia ogólne ramy współpracy między organami nadzorczymi i określa bardziej szczegółowe zasady współpracy między organami nadzorczymi w zakresie transgranicznej działalności związanej z przetwarzaniem danych.

Zgodnie z RODO organy nadzorcze świadczą sobie wzajemną pomoc i przekazują sobie stosowne informacje w celu spójnego wdrażania i stosowania rozporządzenia[512]. Pomoc ta obejmuje konsultacje, kontrole i postępowania prowadzone przez organ nadzorczy, do którego zwrócono się z wnioskiem. Organy nadzorcze prowadzą wspólne operacje, w tym wspólne postępowania i wspólne działania egzekucyjne, w których uczestniczy personel wszystkich zaangażowanych organów nadzorczych[513].

W UE administratorzy i podmioty przetwarzające w coraz większym stopniu działają na poziomie ponadnarodowym. Wymaga to ścisłej współpracy między właściwymi organami nadzorczymi w państwach członkowskich w celu zapewnienia zgodności przetwarzania danych osobowych z wymogami RODO. Zgodnie z „mechanizmem kompleksowej współpracy" ustanowionym w rozporządzeniu, jeżeli administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w kilku państwach członkowskich lub jeżeli mają pojedynczą jednostkę organizacyjną, ale operacje przetwarzania znacznie wpływają na osoby, których dane dotyczą w więcej niż jednym państwie członkowskim, organem nadzorczym głównej (lub pojedynczej) jednostki organizacyjnej jest organ wiodący w odniesieniu do działalności transgranicznej administratora lub podmiotu przetwarzającego. Organy wiodące mają uprawnienia do podejmowania działań w zakresie egzekwowania prawa względem administratora lub podmiotu przetwarzającego. Mechanizm kompleksowej współpracy ma na celu poprawę harmonizacji i jednolitego stosowania unijnego prawa o ochronie danych we wszystkich państwach członkowskich. Jest to również korzystne dla przedsiębiorstw, ponieważ muszą one jedynie współpracować z organem wiodącym, a nie z kilkoma organami nadzorczymi. Zwiększa to pewność prawa dla przedsiębiorstw, a w praktyce powinno również oznaczać szybsze podejmowanie decyzji oraz to, że przedsiębiorstwa nie mają do czynienia z różnymi organami nadzorczymi nakładającymi na nie sprzeczne ze sobą wymogi.

512 Tamże, art. 61 ust. 1–3 i art. 62 ust. 1.

513 Tamże, art. 62 ust. 1.

Określenie organu wiodącego wiąże się z określeniem lokalizacji głównej jednostki organizacyjnej przedsiębiorstwa w UE. Termin „główna jednostka organizacyjna" zdefiniowano w RODO. Ponadto Grupa Robocza Art. 29 wydała wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego, które obejmują kryteria identyfikacji głównej jednostki organizacyjnej[514].

Aby zapewnić wysoki poziom ochrony danych w całej UE, wiodący organ nadzorczy nie działa w pojedynkę. Musi on współpracować z innymi organami nadzorczymi, których sprawa dotyczy, w celu podejmowania decyzji w sprawie przetwarzania danych osobowych przez administratorów i podmioty przetwarzające, dążąc do osiągnięcia porozumienia i zapewnienia spójności. Współpraca między właściwymi organami nadzorczymi obejmuje wymianę informacji, wzajemną pomoc, prowadzenie wspólnych postępowań i działań monitorujących[515]. Udzielając sobie wzajemnej pomocy, organy nadzorcze muszą dokładnie rozpatrywać wnioski o udzielenie informacji złożone przez inne organy nadzorcze i stosować środki nadzorcze, takie jak na przykład uprzednie zezwolenia i konsultacje z administratorem danych w sprawie jego działalności w zakresie przetwarzania danych, przeprowadzania kontroli lub postępowań wyjaśniających. Wzajemna pomoc dla organów nadzorczych w innych państwach członkowskich musi być udzielana na wniosek bez zbędnej zwłoki i nie później niż w terminie jednego miesiąca od otrzymania wniosku[516].

Jeżeli administrator posiada jednostki organizacyjne w kilku państwach członkowskich, organy nadzorcze mogą prowadzić wspólne operacje, w tym postępowania i działania egzekucyjne, w których uczestniczy personel organów nadzorczych z innego państwa członkowskiego[517].

Współpraca między różnymi organami nadzorczymi jest również ważnym wymogiem w prawie RE. Zaktualizowana konwencja nr 108 stanowi, że organy nadzorcze muszą współpracować ze sobą w zakresie niezbędnym do wykonywania swoich zadań[518]. Powinno się to odbywać na przykład poprzez wzajemne dostarczanie

514 Grupa Robocza Art. 29 (2016), *Guidelines for identifying a controller or processor's lead supervisory authority*, WP 244, Bruksela, 13 grudnia 2016 r., zmienione w dniu 5 kwietnia 2017 r.

515 Ogólne rozporządzenie o ochronie danych, art. 60 ust. 1–3.

516 Tamże, art. 61 ust. 1 i 2.

517 Tamże, art. 62 ust. 1.

518 Zaktualizowana konwencja nr 108, art. 16 ust. 7 i art. 17.

sobie istotnych i użytecznych informacji oraz poprzez koordynację postępowań i prowadzenie wspólnych działań[519].

5.4. Europejska Rada Ochrony Danych

W niniejszym rozdziale opisano już znaczenie niezależnych organów nadzorczych i główne właściwości, jakie przysługują im na mocy europejskich przepisów o ochronie danych. Europejska Rada Ochrony Danych (EROD) jest kolejnym ważnym podmiotem w zapewnianiu skutecznego i spójnego stosowania przepisów o ochronie danych w całej UE.

Na gruncie ogólnego rozporządzenia o ochronie danych ustanowiono EROD jako organ UE posiadający osobowość prawną[520]. Rada jest następcą Grupy Roboczej Art. 29[521], którą dyrektywa o ochronie danych ustanowiła w celu doradzania Komisji w sprawie wszelkich środków UE mających wpływ na prawa osób fizycznych w odniesieniu do przetwarzania danych osobowych i prywatności, wspierania jednolitego stosowania dyrektywy oraz służenia Komisji wiedzą ekspercką w sprawach związanych z ochroną danych. Grupa Robocza Art. 29 składała się z przedstawicieli organów nadzorczych państw członkowskich UE oraz przedstawicieli Komisji i EIOD.

Podobnie jak Grupa Robocza, w skład EROD wchodzą szefowie organów nadzorczych z każdego państwa członkowskiego oraz EIOD lub ich przedstawiciele[522]. Europejski Inspektor Ochrony Danych korzysta z równego prawa głosu, z wyjątkiem przypadków związanych z rozstrzyganiem sporów, w których może głosować jedynie nad decyzjami dotyczącymi zasad i przepisów mających zastosowanie do instytucji UE, które zasadniczo odpowiadają zasadom i przepisom RODO. Komisja ma prawo uczestniczyć w działaniach i posiedzeniach EROD, ale bez prawa głosu[523]. Rada wybiera przewodniczącego (któremu powierza się jej reprezentowanie) i dwóch wiceprzewodniczących spośród swoich członków zwykłą większością głosów na pięcioletnią kadencję. Ponadto EROD dysponuje również sekretariatem,

519 Tamże, art. 17 (1).

520 Ogólne rozporządzenie o ochronie danych, art. 68.

521 Zgodnie z dyrektywą 95/46/WE Grupa Robocza Art. 29 miała służyć Komisji radą w sprawie wszelkich środków UE mających wpływ na prawa osób fizycznych w odniesieniu do przetwarzania danych osobowych i prywatności, promować jednolite stosowanie dyrektywy oraz służyć Komisji wiedzą ekspercką w sprawach związanych z ochroną danych. Grupa Robocza Art. 29 składała się z przedstawicieli organów nadzorczych państw członkowskich UE oraz Komisji i EIOD.

522 Ogólne rozporządzenie o ochronie danych, art. 68 ust. 3.

523 Tamże, art. 68 ust. 4 i 5.

który zapewnia EIOD, aby Rada dysponowała wsparciem analitycznym, administracyjnym i logistycznym[524].

Zadania EROD są szczegółowo określone w art. 64, 65 i 70 RODO i obejmują kompleksowe obowiązki, które można podzielić na trzy główne obszary działalności:

- **Spójność:** Europejska Rada Ochrony Danych może wydawać wiążące decyzje dotyczące przypadków, w których organ nadzorczy wniósł mający znaczenie dla sprawy i uzasadniony sprzeciw w przypadku mechanizmów kompleksowej współpracy w sprawach, w których występują sprzeczne opinie co do tego, który z organów nadzorczych jest wiodącym organem, oraz w których właściwy organ nadzorczy nie zwraca się o opinię lub nie stosuje się do opinii EROD[525]. Głównym zadaniem EROD jest zapewnienie spójnego stosowania RODO w całej UE; odgrywa ona również kluczową rolę w mechanizmie spójności opisanym w sekcji 5.5.

- **Konsultacje:** Do zadań EROD należy doradzanie Komisji we wszelkich kwestiach związanych z ochroną danych osobowych w Unii, takich jak zmiany RODO, zmiany przepisów UE, które wiążą się z przetwarzaniem danych i mogą być sprzeczne z unijnymi przepisami o ochronie danych, lub wydawanie decyzji Komisji stwierdzających odpowiedni poziom ochrony, które umożliwiają przekazywanie danych osobowych państwu trzeciemu lub organizacji międzynarodowej.

- **Wskazówki:** Rada wydaje także wytyczne, zalecenia i określa najlepsze praktyki, by zachęcić do spójnego stosowania rozporządzenia, a także upowszechnia współpracę i wymianę wiedzy między organami nadzorczymi. Ponadto musi ona zachęcać stowarzyszenia administratorów lub podmiotów przetwarzających do opracowania kodeksów postępowania, a także do ustanawiania mechanizmów certyfikacji i znaków jakości.

Decyzje EROD można zaskarżyć przed TSUE.

524 Tamże, art. 73 i 75.

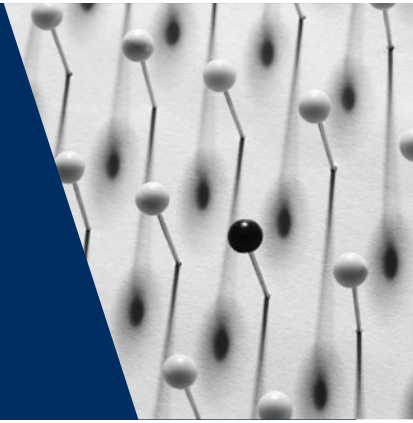
525 Tamże, art. 65.

5.5. Mechanizm spójności RODO

Ogólne rozporządzenie o ochronie danych ustanawia mechanizm spójności w celu zapewnienia spójnego stosowania rozporządzenia we wszystkich państwach członkowskich, w ramach którego organy nadzorcze współpracują ze sobą oraz, w stosownych przypadkach, z Komisją. Mechanizm spójności stosowany jest w dwóch sytuacjach. Pierwsza z nich dotyczy opinii EROD w przypadkach, w których właściwy organ nadzorczy zamierza przyjąć środki, takie jak wykaz operacji przetwarzania danych wymagających oceny skutków dla ochrony danych lub określić standardowe klauzule umowne. Druga dotyczy wiążących decyzji podejmowanych przez EROD na rzecz organów nadzorczych w sprawach dotyczących mechanizmu kompleksowej współpracy, w których organ nadzorczy nie śledzi sprawy, lub nie zwraca się o opinię do EROD.

6

Prawa osób, których dane dotyczą, i ich egzekwowanie



UE	Omówione zagadnienia	RE
Prawo do informacji		
Artykuł 12 ogólnego rozporządzenia o ochronie danych TSUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) przeciwko Geoffreyowi Englebertowi i in.*, 2013 TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 2015	**Przejrzystość informacji**	Artykuł 8 zaktualizowanej konwencji nr 108
Artykuł 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 ogólnego rozporządzenia o ochronie danych	**Treść informacji**	Artykuł 8 ust. 1 zaktualizowanej konwencji nr 108
Artykuł 13 ust. 1 i art. 14 ust. 3 ogólnego rozporządzenia o ochronie danych	**Czas przekazania informacji**	Artykuł 9 ust. 1 lit. b) zaktualizowanej konwencji nr 108
Artykuł 12 ust. 1, 5 i 7 ogólnego rozporządzenia o ochronie danych	**Sposób przekazania informacji**	Artykuł 9 ust. 1 lit. b) zaktualizowanej konwencji nr 108
Artykuł 13 ust. 2 lit. d) i art. 14 ust. 2 lit. e) oraz art. 77, 78 i 79 ogólnego rozporządzenia o ochronie danych	**Prawo wniesienia skargi**	Artykuł 9 ust. 1 lit. f) zaktualizowanej konwencji nr 108

UE	Omówione zagadnienia	RE
Prawo dostępu		
Artykuł 15 ust. 1 ogólnego rozporządzenia o ochronie danych TSUE, C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M. E. E. Rijkeboerowi*, 2009 TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 2014 TSUE, C-434/16, *Peter Nowak przeciwko Data Protection Commissioner*, 2017	**Prawo dostępu do własnych danych osobowych**	Artykuł 9 ust. 1 lit. b) zaktualizowanej konwencji nr 108 ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 1987
Prawo do sprostowania danych		
Artykuł 16 ogólnego rozporządzenia o ochronie danych	**Prawo do sprostowania nieprawidłowych danych osobowych**	**Artykuł 9 ust. 1 lit. e) zaktualizowanej konwencji nr 108** ETPC, *Cemalettin Canli przeciwko Turcji*, nr 22427/04, 2008 r. ETPC, *Ciubotaru przeciwko Mołdawii*, nr 27138/04, 2010
Prawo do usunięcia danych		
Artykuł 17 ust. 1 ogólnego rozporządzenia o ochronie danych	**Usunięcie danych osobowych**	Artykuł 9 ust. 1 lit. e) zaktualizowanej konwencji nr 108 ETPC, *Segerstedt-Wiberg i in. przeciwko Szwecji*, nr 62332/00, 2006
TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 2014 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 2017	**Prawo do bycia zapomnianym**	

UE	Omówione zagadnienia	RE
Prawo do ograniczenia przetwarzania		
Artykuł 18 ust. 1 ogólnego rozporządzenia o ochronie danych	Prawo do ograniczenia wykorzystywania danych osobowych	
Artykuł 19 ogólnego rozporządzenia o ochronie danych	Obowiązek powiadomienia	
Prawo do przenoszenia danych		
Artykuł 20 ogólnego rozporządzenia o ochronie danych	Prawo do przenoszenia danych	
Prawo do sprzeciwu		
Artykuł 21 ust. 1 ogólnego rozporządzenia o ochronie danych TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 2017	Prawo do sprzeciwu z uwagi na szczególną sytuację osoby, której dane dotyczą	Artykuł 5 ust. 3 zalecenia w sprawie profilowania Artykuł 9 ust. 1 lit. d) zaktualizowanej konwencji nr 108
Artykuł 21 ust. 2 ogólnego rozporządzenia o ochronie danych	Prawo do sprzeciwu wobec wykorzystywania danych do celów marketingu	Artykuł 4 ust. 1 zalecenia w sprawie marketingu bezpośredniego
Artykuł 21 ust. 5 ogólnego rozporządzenia o ochronie danych	Prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków	
Prawa związane ze zautomatyzowanym podejmowaniem decyzji i z profilowaniem		
Artykuł 22 ogólnego rozporządzenia o ochronie danych	Prawa związane ze zautomatyzowanym podejmowaniem decyzji i z profilowaniem	Artykuł 9 ust. 1 lit. a) zaktualizowanej konwencji nr 108
Artykuł 21 ogólnego rozporządzenia o ochronie danych	Prawo do sprzeciwu oraz zautomatyzowane podejmowanie decyzji	
Artykuł 13 ust. 2 lit. f) ogólnego rozporządzenia o ochronie danych	Prawo do rzeczowego wyjaśnienia	Artykuł 9 ust. 1 lit. c) zaktualizowanej konwencji nr 108

UE	Omówione zagadnienia	RE
Środki prawne, odpowiedzialność, sankcje i odszkodowanie		
Artykuł 47 karty praw podstawowych TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 2015 Artykuły 77–84 ogólnego rozporządzenia o ochronie danych	**Z tytułu naruszenia krajowego prawa o ochronie danych**	Artykuł 13 EKPC (tylko w przypadku państw członkowskich RE) Artykuł 9 ust. 1 lit. f) oraz art. 12, 15, 16-21 zaktualizowanej konwencji nr 108 ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2008 ETPC, *Biriuk przeciwko Litwie*, nr 23373/03, 2008
Artykuły 34 i 49 ogólnego rozporządzenia o ochronie danych przez instytucje UE TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.* [WI], 2010	**Z tytułu naruszenia prawa UE przez instytucje i organy UE**	

Skuteczność norm prawnych w ujęciu ogólnym – i praw osób, których dane dotyczą, w ujęciu szczegółowym – zależy w dużym stopniu od istnienia odpowiednich mechanizmów ich egzekwowania. W epoce cyfrowej przetwarzanie danych osobowych stało się praktyką powszechną, a dla jednostek – coraz bardziej niezrozumiałą. Aby wyrównać układ sił między osobami, których dane dotyczą, a administratorami danych, osobom fizycznym nadano określone prawa, by zapewnić im większą kontrolę nad przetwarzaniem ich danych osobowych. Prawo dostępu do własnych danych i prawo do dokonania ich sprostowania zapisano w art. 8 ust. 2 Karty praw podstawowych UE – dokumencie, który stanowi źródło prawa pierwotnego UE i odgrywa zasadniczą rolę w porządku prawnym Unii. Prawo wtórne UE – zwłaszcza ogólne rozporządzenie o ochronie danych – ustanawia spójne ramy prawne nadające osobom, których dane dotyczą, uprawnienia względem administratorów danych. Oprócz prawa dostępu do danych i ich sprostowania RODO przyznaje szereg innych praw, takich jak prawo do usunięcia danych („prawo do bycia zapomnianym"), prawo sprzeciwu lub ograniczenia przetwarzania danych osobowych oraz prawa związane ze zautomatyzowanym podejmowaniem decyzji i z profilowaniem. Podobne zabezpieczenia, mające na celu umożliwienie osobom, których dane dotyczą, sprawowania skutecznej kontroli nad swoimi danymi, zostały również uwzględnione w zaktualizowanej konwencji nr 108. W art. 9 wymieniono prawa, z których osoby fizyczne powinny móc korzystać w odniesieniu do przetwarzania ich danych

osobowych. Umawiające się strony muszą zagwarantować, że prawa te są dostępne dla wszystkich osób, których dane dotyczą, w ich jurysdykcji oraz że towarzyszą im skuteczne środki prawne i praktyczne sposoby umożliwiające takim osobom ich wykonywanie.

Oprócz zapewnienia osobom fizycznym praw równie ważne jest stworzenie mechanizmów umożliwiających osobom, których dane dotyczą, zaskarżanie naruszeń ich praw, pociąganie administratorów danych do odpowiedzialności i dochodzenie odszkodowań. Zagwarantowane na mocy EKPC i karty prawo do skutecznego środka prawnego wymaga udostępnienia każdej osobie środków sądowych.

6.1. Prawa osób, których dane dotyczą

Najważniejsze kwestie

- Każda osoba, której dane dotyczą, ma prawo do informacji o przetwarzaniu jej danych osobowych przez jakiegokolwiek administratora, z kilkoma wyjątkami.
- Osoby, których dane dotyczą, mają prawo:
  - dostępu do swoich danych i do otrzymania określonych informacji na temat ich przetwarzania;
  - żądać, aby ich dane zostały sprostowane przez przetwarzającego je administratora, jeżeli są one nieprawidłowe;
  - żądać usunięcia swoich danych przez administratora, w stosownych przypadkach, jeżeli ten przetwarza ich dane niezgodnie z prawem;
  - tymczasowo ograniczyć przetwarzanie;
  - w określonych okolicznościach żądać przeniesienia danych do innego administratora.
- Ponadto osoby, których dane dotyczą, mają prawo do sprzeciwu wobec przetwarzania danych:
  - z uwagi na ich szczególną sytuację,
  - na potrzeby wykorzystywania do celów marketingu bezpośredniego.

- Osoby, których dane dotyczą, mają prawo do tego, by nie podlegać decyzjom, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują wobec tych osób skutki prawne lub istotnie na nie wpływają. Ponadto osoby, których dane dotyczą, mają prawo do:
  - uzyskania interwencji ludzkiej ze strony administratora,
  - wyrażenia własnego stanowiska i do zakwestionowania decyzji opartej na zautomatyzowanym przetwarzaniu.

6.1.1. Prawo do informacji

Zgodnie zarówno z **prawem RE**, jak i **prawem UE** podczas pozyskiwania danych administratorzy wykonujący czynność przetwarzania danych mają obowiązek poinformować osobę, której dane dotyczą, o zamierzonym przetwarzaniu. Obowiązek ten nie zależy od złożenia wniosku przez osobę, której dane dotyczą; administrator musi podjąć aktywne działania bez względu na to, czy osoba, której dane dotyczą, wykazuje zainteresowanie tymi informacjami, czy też nie.

W myśl prawa RE, zgodnie z art. 8 zaktualizowanej konwencji nr 108, umawiające się strony muszą zadbać o to, by administratorzy informowali osoby, których dane dotyczą, o swojej tożsamości, miejscu zwykłego pobytu, podstawie prawnej i celu przetwarzania, kategoriach przetwarzanych danych osobowych, odbiorcach takich danych osobowych (w stosownych przypadkach) oraz o tym, w jaki sposób takie osoby mogą skorzystać ze swoich praw wynikających z art. 9, w tym prawa dostępu, prawa do sprostowania danych oraz prawa do środka prawnego. Osobom, których dane dotyczą, należy przekazać również wszelkie inne, dodatkowe informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania danych osobowych. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 wyjaśniono, że informacje przedstawiane osobom, których dane dotyczą, „powinny być łatwo dostępne, czytelne, zrozumiałe i dostosowane do osób, których dane dotyczą”[526].

Zasada przejrzystości zapisana w prawie UE wymaga, by wszelkie przypadki przetwarzania danych osobowych były co do zasady przejrzyste dla osób fizycznych. Osoby fizyczne mają prawo wiedzieć, dlaczego i w jaki sposób ich dane osobowe są zbierane, wykorzystywane lub w inny sposób przetwarzane, jak również mieć świadomość ryzyka, zabezpieczeń i przysługujących im praw związanych

526 Explanatory Report of Modernised Convention 108, pkt 68.

z przetwarzaniem danych[527]. Z tego względu w art. 12 ogólnego rozporządzenia o ochronie danych nałożono na administratorów danych szeroki i kompleksowy obowiązek przekazywania przejrzystych informacji lub informowania o tym, jak osoby, których dane dotyczą, mogą skorzystać ze swoich praw[528]. Informacje te muszą być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne oraz sformułowane jasnym i prostym językiem. Muszą być przekazywane w formie pisemnej, w tym w stosownych przypadkach w formie elektronicznej, a nawet ustnie, jeżeli osoba, której dane dotyczą, tego zażąda, a jej tożsamość zostanie ustalona ponad wątpliwość. Informacje takie należy przekazywać bez zbędnej zwłoki czy nadmiernych kosztów[529].

Artykuły 13 i 14 RODO poświęcono prawu osób, których dane dotyczą, do informacji – odpowiednio w sytuacjach, gdy dane osobowe są zbierane bezpośrednio od takich osób, lub w przypadkach gdy dane nie zostały uzyskane od nich.

Zakres prawa do informacji oraz jego ograniczenia wynikające z prawa UE wyjaśniono w orzecznictwie TSUE.

Przykład: W sprawie *Institut professionnel des agents immobiliers (IPI) przeciwko Geoffreyowi Englebertowi i in.*[530] zwrócono się do TSUE o wykładnię art. 13 ust. 1 dyrektywy 95/46. Przedmiotowy artykuł daje państwom członkowskim możliwość wyboru, czy chcą przyjąć środki ustawodawcze w celu ograniczenia zakresu praw osoby, której dane dotyczą, do informacji, kiedy ograniczenie takie stanowi środek konieczny do ochrony, między innymi, praw i wolności innych osób, oraz do prowadzenia działań prewencyjnych i czynności dochodzeniowych w sprawach karnych i sprawach o naruszenie zasad etyki w zawodach podlegających regulacji. IPI jest organizacją zawodową zrzeszającą agentów nieruchomości w Belgii, odpowiedzialną za czuwanie nad właściwym wykonywaniem tego zawodu. Organizacja ta zwróciła się do sądu krajowego o stwierdzenie, że pozwani dopuścili się działań sprzecznych z zasadami wykonywania zawodu, oraz

527 Ogólne rozporządzenie o ochronie danych, motyw 39.

528 Tamże, art. 13 i 14; zaktualizowana konwencja nr 108, art. 8 ust. 1 lit. b).

529 Ogólne rozporządzenie o ochronie danych, art. 12 ust. 5; zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. b).

530 TSUE, C-473/12, *Institut professionnel des agents immobiliers (IPI) przeciwko Geoffreyowi Englebertowi i in.*, 7 listopada 2013 r.

nakazanie im zaprzestania prowadzenia określonych czynności na rynku nieruchomości. Powództwo opierało się na materiale dowodowym zebranym przez prywatnych detektywów, z których usług IPI korzystała.

Sąd krajowy powziął wątpliwość co do wartości dowodów zgromadzonych przez detektywów, biorąc pod uwagę to, że mogły one zostać uzyskane przy braku przestrzegania wymogów w zakresie ochrony danych przewidzianych w belgijskim prawie, zwłaszcza obowiązku poinformowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych przed zebraniem tych informacji. Trybunał zauważył, że art. 13 ust. 1 stanowi, że państwa członkowskie „mogą", lecz nie mają obowiązku wprowadzać w swoich przepisach krajowych wyjątków od obowiązku informowania osób, których dane dotyczą, o przetwarzaniu ich danych osobowych. Z uwagi na to, że w art. 13 ust. 1 wymieniono działania prewencyjne, prowadzone czynności dochodzeniowo-śledcze i prokuratorskie w sprawach karnych lub sprawach o naruszenie zasad etyki jako podstawy ewentualnego ograniczenia praw osób fizycznych przez państwa członkowskie, działanie organizacji takiej jak IPI i działających w jej imieniu prywatnych detektywów mogłoby opierać się na tym zapisie. Jeżeli jednak państwo członkowskie nie przewidziało takiego wyjątku, osoby, których dane dotyczą, muszą zostać poinformowane.

Przykład: W sprawie *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*[531] TSUE wyjaśnił, czy prawo UE uniemożliwia krajowemu organowi administracji publicznej przekazanie danych osobowych innemu organowi administracji publicznej w celu ich dalszego przetwarzania bez informowania osoby, której dane dotyczą, o tymże przekazaniu i przetwarzaniu. W przedmiotowej sprawie krajowa agencja administracyjna przekazała dane skarżących krajowej kasie ubezpieczeń zdrowotnych bez wcześniejszego poinformowania ich o tym.

Trybunał zważył, że wynikający z prawa UE wymóg informowania osoby, której dane dotyczą, o przetwarzaniu jej danych osobowych „jest tym ważniejszy, iż stanowi warunek konieczny wykonywania przez te osoby ich prawa dostępu do przetwarzanych danych i sprostowania ich [...] oraz ich prawa sprzeciwu wobec przetwarzania tych danych". Zasada rzetelnego przetwarzania danych wymaga informowania osób, których dane dotyczą,

531 TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 1 października 2015 r.

o przekazaniu ich danych innemu organowi publicznemu w celu ich dalszego przetwarzania przez ów organ. W myśl art. 13 ust. 1 dyrektywy 95/46 państwa członkowskie mogą ograniczyć prawo do informacji, jeżeli jest to konieczne do zabezpieczenia ważnego interesu ekonomicznego państwa, łącznie z kwestiami podatkowymi. Takie ograniczenia muszą jednak być przyjmowane w drodze środków ustawodawczych. Ponieważ ani definicja danych, które mają zostać przekazane, ani szczegółowe zasady, według których odbywało się przekazanie, nie zostały określone w drodze środka ustawodawczego, a jedynie w protokole zawartym między dwoma organami publicznymi, przesłanki odstępstwa przewidziane w prawie UE nie zostały spełnione. Należało poinformować skarżących o przekazaniu ich danych osobowych krajowej kasie ubezpieczeń zdrowotnych oraz o późniejszym przetwarzaniu tych danych przez ten organ, zanim doszło do przekazania i przetwarzania.

Treść informacji

Na mocy art. 8 ust. 1 zaktualizowanej konwencji nr 108 administrator danych ma obowiązek przekazać osobie, której dotyczą dane, wszelkie informacje zapewniające rzetelność i przejrzystość przetwarzania danych osobowych, do których należą:

- tożsamość i miejsce zwykłego pobytu lub jednostka organizacyjna;
- podstawa prawna i cele planowanego przetwarzania;
- kategorie przetwarzanych danych osobowych;
- odbiorcy lub kategorie odbiorców danych osobowych, o ile tacy istnieją;
- sposoby wykonywania praw przez osoby, których dane dotyczą.

Zgodnie z RODO w przypadku zbierania danych od osoby, której dane dotyczą, administrator podczas pozyskiwania danych osobowych jest zobowiązany podać jej następujące informacje[532]:

532 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 1.

- tożsamość i dane kontaktowe administratora danych oraz, gdy ma to zastosowanie, dane inspektora ochrony danych;
- cel oraz podstawa prawna przetwarzania, tj. umowa bądź zobowiązanie prawne;
- prawnie uzasadnione interesy realizowane przez administratora, jeżeli na tej podstawie odbywa się przetwarzanie;
- dane osobowe ewentualnych odbiorców lub kategorie odbiorców;
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia odpowiedniego stopnia ochrony lub wzmiankę o odpowiednich zabezpieczeniach;
- okres, przez który dane osobowe będą przechowywane, a gdy ustalenie tego okresu nie jest możliwe, kryteria wyznaczenia okresu przechowywania danych;
- prawa osób, których dane dotyczą, w odniesieniu do przetwarzania, takie jak prawo dostępu, sprostowania, usunięcia i ograniczenia bądź sprzeciwu wobec przetwarzania;
- informacje, czy podanie danych osobowych jest wymogiem ustawowym lub umownym oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są konsekwencje niepodania danych;
- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- informacje o prawie wycofania zgody na przetwarzanie danych.

W przypadkach zautomatyzowanego podejmowania decyzji, w tym profilowania, osoby, których dane dotyczą, muszą otrzymać istotne informacje o zasadach profilowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

W przypadku pozyskiwania danych osobowych w sposób inny niż bezpośrednio od osoby, której dane dotyczą, administrator danych musi powiadomić daną osobę o źródle pochodzenia danych osobowych. W każdym przyypadku administrator

musi poinformować osobę, której dane dotyczą, między innymi o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu[533]. Ponadto jeżeli administrator zamierza przetwarzać dane osobowe do celów innych niż pierwotnie wskazany osobie, której dane dotyczą, zasady ograniczenia celu i przejrzystości wymagają, by administrator danych podał takiej osobie informacje o nowym celu. Administratorzy danych muszą dostarczać informacje przed przystąpieniem do jakiegokolwiek dalszego przetwarzania. Innymi słowy w przypadku gdy osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie danych osobowych, administrator musi otrzymać ponowną zgodę takiej osoby, jeżeli cel przetwarzania danych się zmieni lub zostaną dodane kolejne cele.

Czas przekazania informacji

W RODO dokonano rozróżnienia między dwoma scenariuszami i określonymi punktami w czasie, gdy administrator danych musi przekazać informacje osobie, której dane dotyczą:

- Jeżeli dane osobowe są zbierane bezpośrednio od osoby, której dotyczą, administrator musi podczas pozyskiwania danych osobowych powiadomić ją o wszystkich związanych z nią informacjach oraz o wszystkich prawach przysługujących jej na mocy rozporządzenia[534].

  Jeżeli administrator zamierza podejmować się dalszego przetwarzania danych osobowych do innych celów, przekazuje wszystkie stosowne informacje, zanim przystąpi do przetwarzania.

- Jeżeli dane osobowe nie zostały pozyskane bezpośrednio od osoby, której dane dotyczą, administrator jest zobowiązany do przekazania takiej osobie informacji o przetwarzaniu „w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca" lub przed ujawnieniem danych osobie trzeciej[535].

Sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108 stanowi, że jeżeli nie jest możliwe poinformowanie osób, których dane dotyczą, przy rozpoczynaniu przetwarzania, można takie informacje przekazać na późniejszym etapie, na

533 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 2 i art. 14 ust. 2 lit. f).

534 Tamże, art. 13 ust. 1 i 2, formuła wprowadzająca, w której RODO odnosi się do informacji na temat obowiązku, który należy wypełnić „podczas pozyskiwania danych osobowych".

535 Tamże, art. 13 ust. 3 i art. 14 ust. 3; zob. także odniesienie do koncepcji „rozsądnych odstępów czasu" i „bez zbędnej zwłoki", o których mowa w zaktualizowanej konwencji nr 108, art. 8 ust. 1 lit. b).

przykład przy okazji kontaktu administratora danych z osobą, której dane dotyczą, z dowolnego powodu[536].

Różne sposoby przekazywania informacji

Zarówno na mocy prawa RE, jak i prawa UE informacje, jakie administrator musi przekazać osobom, których dane dotyczą, muszą być zwięzłe, przejrzyste, zrozumiałe i łatwo dostępne. Muszą być przekazywane na piśmie lub w inny sposób, w tym w formie elektronicznej, oraz być sformułowane jasnym, prostym i zrozumiałym językiem. Przy przekazywaniu informacji administrator może korzystać ze standardowych znaków graficznych, które umożliwiają przekazanie informacji w widoczny i zrozumiały sposób[537]. Przykładowo znak graficzny przedstawiający kłódkę mógłby posłużyć do zasygnalizowania, że dane są gromadzone w sposób bezpieczny lub szyfrowane. Osoby, których dane dotyczą, mogą zwrócić się o przekazanie im informacji ustnie. Informacje te muszą być wolne od opłat, chyba że żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne (np. ze względu na swój ustawiczny charakter)[538]. Łatwy dostęp do przekazywanych informacji ma znaczenie nadrzędne względem możliwości wykonywania przez osobę, której dane dotyczą, praw zagwarantowanych jej na mocy unijnych przepisów o ochronie danych.

Zasada rzetelnego przetwarzania danych wymaga, by informacje były zrozumiałe dla osób, których dane dotyczą. Należy je formułować językiem dostosowanym do odbiorców. Poziom trudności i rodzaj użytego języka muszą się różnić w zależności od tego, czy zamierzonymi odbiorcami są na przykład dorośli czy dzieci, ogół społeczeństwa czy eksperci z kręgów akademickich. Wyważone podejście do tego aspektu zrozumiałego informowania opisano w opinii Grupy Roboczej Art. 29 w sprawie dalszej harmonizacji zasad informowania. W opinii proponuje się tzw. warstwowe noty informacyjne[539] pozwalające osobie, której dane dotyczą, wybrać pożądany poziom szczegółowości. Ten sposób prezentacji informacji nie zwalnia jednak administratora z jego obowiązku wynikającego z art. 13 i 14

536 Sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108, pkt 70.

537 Komisja Europejska będzie dalej rozwijać kwestię informacji przedstawianych za pomocą znaków graficznych oraz procedur ustanowienia standardowych znaków graficznych w drodze aktów delegowanych; zob. ogólne rozporządzenie o ochronie danych, art. 12 ust. 8.

538 Ogólne rozporządzenie o ochronie danych, art. 12 ust. 1, 5 i 7 oraz zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. b).

539 Grupa Robocza Art. 29 (2004), *Opinion 10/2004 on More Harmonised Information Provisions,* WP 100, Bruksela, 25 listopada 2004 r.

RODO. Administrator i tak musi dostarczyć osobie, której dane dotyczą, wszystkie informacje.

Jednym z najskuteczniejszych sposobów przekazania informacji jest zamieszczenie odpowiednich klauzul informacyjnych, na przykład polityki prywatności serwisu internetowego, na stronie głównej administratora. Znaczna część społeczeństwa nie korzysta jednak z Internetu, co należy wziąć pod uwagę w polityce informacyjnej spółki lub organu władzy publicznej.

Oświadczenie o ochronie prywatności dotyczące przetwarzania danych osobowych zamieszczone w witrynie internetowej mogłoby wyglądać następująco:

Kim jesteśmy?

„Administratorem" przetwarzającym dane jest spółka Bed and Breakfast C&U z siedzibą w [adres: xxx], tel.: xxx; faks: xxx; adres e-mail info@c&u.com; dane kontaktowe inspektora ochrony danych: [xxx].

Oświadczenie dotyczące danych osobowych stanowi część warunków regulujących świadczenie przez nas usług hotelarskich.

Jakie dane o Tobie zbieramy?

Zbieramy następujące dane osobowe na Twój temat: imię i nazwisko, adres pocztowy, numer telefonu, adres e-mail, informacje o pobycie, numer karty kredytowej i debetowej oraz adresy IP lub nazwy domen komputerów, z których korzystasz w celu połączenia z naszą witryną.

Dlaczego zbieramy Twoje dane?

Twoje dane przetwarzamy na podstawie wyrażonej przez Ciebie zgody na potrzeby realizacji rezerwacji, zawierania i wykonywania umów związanych z oferowanymi usługami oraz przestrzegania wymogów prawnych, na przykład ustawy o opłatach klimatycznych, która wymaga od nas zbierania danych osobowych w celu zapłaty podatku miejskiego od zakwaterowania.

Jak przetwarzamy Twoje dane?

Twoje dane osobowe będziemy przechowywać przez okres trzech miesięcy. Dane nie będą poddawane procedurom automatycznego podejmowania decyzji.

Spółka Bed and Breakfast C&U stosuje rygorystyczne procedury bezpieczeństwa, mające zapewnić, że dane osobowe nie zostaną uszkodzone, zniszczone ani ujawnione osobom trzecim bez Twojej zgody oraz zapobiec nieuprawnionemu dostępowi do takich danych. Komputery, na których informacje są przechowywane, znajdują się w bezpiecznym miejscu, a fizyczny dostęp do nich jest ograniczony. Aby ograniczyć dostęp elektroniczny, korzystamy z bezpiecznych zapór i innych środków zabezpieczających. Gdy konieczne jest przekazanie danych osobie trzeciej, wymagamy od niej stosowania podobnych środków ochrony Twoich danych osobowych.

Żadne informacje, które gromadzimy lub rejestrujemy, nie są udostępniane osobom spoza naszych biur. Dostęp do danych osobowych uzyskują wyłącznie osoby, którym dane te są niezbędne do realizacji ich obowiązków wynikających z umowy. Za każdym razem gdy będziemy potrzebować informacji o Twojej tożsamości, zwrócimy się do Ciebie z wyraźną prośbą. Zanim ujawnimy Ci informacje, możemy od Ciebie wymagać przejścia kontroli bezpieczeństwa. Możesz w dowolnej chwili zaktualizować przekazane nam dane osobowe, kontaktując się z nami bezpośrednio.

Jakie prawa Ci przysługują?

Przysługuje Ci prawo dostępu do danych, otrzymania ich kopii, zażądania ich usunięcia, sprostowania lub przekazania innemu administratorowi.

Swoje żądania możesz kierować do nas na adres info@c&u.com. Mamy obowiązek odpowiedzieć na Twoje żądanie w ciągu jednego miesiąca, jeśli jednak jest ono zbyt złożone bądź otrzymamy zbyt wiele innych żądań, poinformujemy Cię, że okres ten może wydłużyć się o kolejne dwa miesiące.

Dostęp do danych osobowych

Masz prawo dostępu do swoich danych, do otrzymania na żądanie informacji o powodach przetwarzania danych, żądania usunięcia lub sprostowania danych oraz prawo do niepodlegania całkowicie zautomatyzowanemu podejmowaniu decyzji bez uwzględnienia Twoich uwag. Swoje żądania możesz kierować do nas na adres info@c&u.com. Ponadto przysługuje Ci prawo sprzeciwu wobec przetwarzania danych, wycofania zgody na przetwarzanie danych i wniesienia skargi do krajowego organu nadzorczego, jeśli uznasz, że przetwarzanie danych odbywa się wbrew prawu, jak również prawo do dochodzenia odszkodowania z tytułu szkód poniesionych w wyniku niezgodnego z prawem przetwarzania.

Prawo wniesienia skargi

Na mocy RODO administrator ma obowiązek poinformować osoby, których dane dotyczą, o mechanizmach egzekwowania ich praw, przewidzianych w prawie krajowym i prawie UE w przypadku stwierdzenia naruszenia ochrony danych osobowych. Administrator musi poinformować osoby, których dane dotyczą, o przysługującym im prawie wniesienia skargi na naruszenie ochrony danych osobowych do organu nadzorczego oraz, w razie potrzeby, sądu krajowego[540]. Prawo RE również przewiduje prawo przysługujące osobom, których dane dotyczą, do bycia poinformowanymi o sposobach wykonywania ich praw, w tym prawa do środka ochrony określonego w artykule 9 ust. 1 lit. f).

Wyjątki od obowiązku informowania

W RODO przewidziano wyjątek od obowiązku informowania. Zgodnie z art. 13 ust. 4 i art. 14 ust. 5 rozporządzenia obowiązek informowania osób, których dane dotyczą, nie obowiązuje, jeżeli dana osoba dysponuje już wszystkimi niezbędnymi informacjami[541]. Ponadto w przypadku gdy dane osobowe nie zostały pozyskane od osoby, której dotyczą, obowiązek informowania nie będzie miał zastosowania, jeżeli przekazanie informacji jest niemożliwe bądź wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów

540 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 2 lit. d) i art. 14 ust. 2 lit. e); zaktualizowana konwencja nr 108 art. 8 ust. 1 lit. f).

541 Tamże, art. 13 ust. 4 oraz art. 14 ust. 5 lit. a).

archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych[542].

Co więcej, na mocy RODO państwa członkowskie mogą w pewnym zakresie ograniczyć obowiązki i prawa jednostek wynikające z rozporządzenia, o ile takie ograniczenie jest w demokratycznym społeczeństwie niezbędnym i proporcjonalnym środkiem służącym na przykład bezpieczeństwu narodowemu i publicznemu, obronie, ochronie dochodzeń i postępowań sądowych lub interesów gospodarczych i finansowych, jak również prywatnych interesów, które są ważniejsze niż interesy ochrony danych[543].

Wszelkie wyjątki lub ograniczenia muszą stanowić środek niezbędny w demokratycznym społeczeństwie i proporcjonalny do zamierzonego celu. W bardzo wyjątkowych przypadkach, na przykład ze względu na wskazania medyczne, ochrona osoby, której dane dotyczą, może sama w sobie wymagać ograniczenia przejrzystości. Odnosi się to w szczególności do ograniczenia prawa dostępu każdej osoby, której dane dotyczą[544]. Prawo krajowe musi jednak zapewniać poszanowanie przynajmniej istoty podstawowych praw i wolności chronionych prawem UE[545]. W związku z tym prawo krajowe musi zawierać konkretne przepisy wyjaśniające cel przetwarzania, kategorie odnośnych danych osobowych, zabezpieczenia oraz inne wymogi proceduralne[546].

W przypadku gromadzenia danych do celów badań naukowych bądź historycznych, do celów statystycznych lub do celów archiwalnych w interesie publicznym, prawo Unii lub państw członkowskich może przewidywać odstępstwa od obowiązku informowania, jeżeli obowiązek ten może uniemożliwić lub poważnie utrudnić osiągnięcie tych celów[547].

Podobne ograniczenia istnieją na mocy prawa Rady Europy, gdy prawa przyznane osobom, których dane dotyczą, na mocy artykułu 9 zaktualizowanej konwencji nr 108 mogą podlegać możliwym ograniczeniom na mocy artykułu 11 zaktualizowanej konwencji nr 108, pod ścisłymi warunkami. Ponadto zgodnie z artykułem 8 ust. 2

542 Tamże, art. 14 ust. 5 lit. b)–e).

543 Ogólne rozporządzenie o ochronie danych, art. 23 ust. 1.

544 Ogólne rozporządzenie o ochronie danych, art. 15.

545 Ogólne rozporządzenie o ochronie danych, art. 23 ust. 1.

546 Tamże, art. 23 ust. 2.

547 Tamże, art. 89 ust. 2 i 3.

zaktualizowanej konwencji nr 108 obowiązek przejrzystości przetwarzania nałożony na administratorów nie ma zastosowania, gdy osoba, której dane dotyczą, już posiada informacje.

Prawo dostępu do własnych danych osobowych

Zgodnie z prawem RE prawo dostępu do własnych danych wyraźnie potwierdzono w art. 9 zaktualizowanej konwencji nr 108. Przepis ten stanowi, że każda osoba ma prawo do otrzymania na żądanie informacji o przetwarzaniu dotyczących jej danych osobowych, która to informacja jest jej przekazywana w sposób zrozumiały. Prawo dostępu zostało uznane nie tylko w przepisach zaktualizowanej konwencji nr 108, lecz także w orzecznictwie ETPC. Trybunał wielokrotnie uznawał, że osobom przysługuje prawo dostępu do informacji o ich danych osobowych i że to prawo wynika z potrzeby poszanowania życia prywatnego[548]. Prawo dostępu do danych osobowych przechowywanych przez publiczne bądź prywatne organizacje może jednak być w określonych przypadkach ograniczone[549].

W prawie UE prawo dostępu do własnych danych osobowych potwierdzono wprost w art. 15 RODO, a ponadto uznano za element podstawowego prawa do ochrony danych osobowych, zapisanego w art. 8 ust. 2 Karty praw podstawowych UE[550]. Prawo do uzyskania dostępu do własnych danych osobowych to kluczowy element europejskiego prawa o ochronie danych[551].

W RODO zagwarantowano każdej osobie, której dane dotyczą, prawo dostępu do swoich danych osobowych oraz określonych informacji o przetwarzaniu, które administratorzy mają obowiązek jej przekazać[552]. W szczególności każda osoba, której dane dotyczą, ma prawo uzyskać od administratora potwierdzenie, czy są przetwarzane dotyczące jej dane, oraz informacje obejmujące co najmniej:

548 ETPC, *Gaskin przeciwko Zjednoczonemu Królestwu*, nr 10454/83, 7 lipca 1989 r.; ETPC, *Odièvre przeciwko Francji* [WI], nr 42326/98, 13 lutego 2003 r.; ETPC, *K.H. i in. przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.; ETPC, *Godelli przeciwko Włochom*, nr 33783/09, 25 września 2012 r.

549 ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.

550 Zob. także TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 17 lipca 2014 r.; TSUE, C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) przeciwko Europejskiemu Urzędowi ds. Bezpieczeństwa Żywności (EFSA), Komisji Europejskiej*, 16 lipca 2015 r.

551 TSUE, sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 17 lipca 2014 r.

552 Ogólne rozporządzenie o ochronie danych, art. 15 ust. 1.

- cele przetwarzania;
- kategorie odnośnych danych osobowych;
- informacje o odbiorcach lub kategoriach odbiorców, którym dane są ujawniane;
- planowany okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o prawie do sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
- informacje o prawie wniesienia skargi do organu nadzorczego;
- wszelkie dostępne informacje o źródle przetwarzanych danych, jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą;
- w przypadku zautomatyzowanych decyzji informacje o zasadach jakiegokolwiek zautomatyzowanego przetwarzania danych.

Administrator danych musi dostarczyć osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Wszelkie informacje przekazywane osobie, której dane dotyczą, muszą być przygotowane w zrozumiałej formie, co oznacza, że administrator musi zagwarantować, by ta osoba była w stanie je zrozumieć. Przykładowo podanie w odpowiedzi na żądanie dostępu skrótów technicznych, pojęć zakodowanych lub akronimów co do zasady nie jest wystarczające, chyba że znaczenie tych pojęć zostanie wyjaśnione. W przypadku zautomatyzowanego podejmowania decyzji, w tym profilowania, konieczne będzie wyjaśnienie ogólnych zasad zautomatyzowanego podejmowania decyzji, w tym kryteriów uwzględnionych przy ocenie osoby, której dane dotyczą. Podobne wymogi przewidziano w **prawie RE**[553].

Przykład: Uzyskanie dostępu do swoich danych osobowych ułatwi osobie, której dane dotyczą, ustalenie, czy dane te są prawidłowe. W związku z tym niezbędne jest poinformowanie osoby, której dane dotyczą, w zrozumiały sposób nie tylko o samych przetwarzanych danych osobowych, lecz

553 Zob. zaktualizowana konwencja nr 108, art. 8 ust. 1 lit. c).

także o kategoriach, w ramach których takie przetwarzanie się odbywa, takich jak nazwisko, adres IP, współrzędne geolokalizacyjne, numer karty kredytowej itp.

Jeżeli dane nie są zbierane od osoby, której dotyczą, w odpowiedzi na żądanie dostępu muszą zostać podane informacje o źródle danych – o ile są dostępne. Przepis ten należy rozumieć w świetle zasad rzetelności, przejrzystości i rozliczalności. Administrator nie może zniszczyć informacji o źródle danych, aby zwolnić się z ich ujawnienia – chyba że usunięcie takich informacji miałoby miejsce pomimo otrzymania żądania dostępu – i mimo to musi przestrzegać ogólnych wymogów w zakresie „rozliczalności".

Jak podkreślono w orzecznictwie TSUE, prawo dostępu do własnych danych nie może być w nadmierny sposób ograniczane terminami. Osobom, których dane dotyczą, należy zapewnić rozsądną możliwość uzyskania informacji o czynności przetwarzania, których dokonywano w przeszłości.

Przykład: W sprawie *Rijkeboer*[554] TSUE miał rozstrzygnąć, czy prawo osoby do dostępu do informacji o odbiorcach lub kategoriach odbiorców danych osobowych i treści przekazanych danych może zostać ograniczone do roku poprzedzającego złożenie wniosku o dostęp.

Aby rozstrzygnąć, czy w przepisach UE dopuszcza się takie ograniczenie czasowe, TSUE postanowił dokonać wykładni art. 12 w świetle celów dyrektywy. Trybunał stwierdził po pierwsze, że prawo dostępu jest niezbędne, aby umożliwić osobie, której dane dotyczą, wykonanie prawa do żądania, aby administrator sprostował, usunął lub zablokował jej dane bądź zawiadomił osoby trzecie, którym ujawniono dane, o takim sprostowaniu, usunięciu lub zablokowaniu. Skuteczne prawo dostępu jest również niezbędne, aby umożliwić osobie, której dane dotyczą, wykonanie prawa sprzeciwu wobec przetwarzania jej danych osobowych bądź prawa do wniesienia skargi i dochodzenia odszkodowania[555].

554 TSUE, C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M. E. E. Rijkeboerowi*, 7 maja 2009 r.

555 Ogólne rozporządzenie o ochronie danych, art. 15 ust. 1 lit. c) i f), art. 16, art. 17 ust. 2 i art. 21 oraz rozdział VIII.

Aby zapewnić w praktyce skuteczność praw nadanych osobom, których dane dotyczą, TSUE uznał, że „prawo to musi koniecznie odnosić się do przeszłości. Gdyby tak nie było, zainteresowana osoba nie byłaby w stanie efektywnie wykonać swojego prawa do sprostowania, usunięcia lub zablokowania dotyczących jej danych potencjalnie nielegalnych lub nieprawidłowych, ani też do wniesienia środków prawnych i uzyskania naprawienia poniesionej szkody".

6.1.2. Prawo do sprostowania danych

Na mocy prawa Unii i **prawa RE** osoby, których dane dotyczą, mają prawo żądać, by ich dane osobowe zostały sprostowane. Prawidłowość danych osobowych jest niezbędna do zapewnienia wysokiego poziomu ochrony danych osób, których dane dotyczą[556].

Przykład: W sprawie *Ciubotaru przeciwko Mołdawii*[557] skarżący nie był w stanie zmienić pochodzenia etnicznego zapisanego w dokumentach urzędowych z mołdawskiego na rumuńskie, rzekomo ze względu na brak uzasadnienia przedłożonego wniosku. ETPC uznał, że państwa mogą wymagać obiektywnych dowodów, odnotowując przynależność etniczną danej osoby. Gdy taki wniosek oparty jest na czysto subiektywnych i nieuzasadnionych przesłankach, władze mogą odmówić. Wniosek skarżącego opierał się jednak nie tylko na subiektywnym postrzeganiu własnej grupy etnicznej, przedstawił on bowiem możliwe do obiektywnej weryfikacji powiązania z rumuńską grupą etniczną, takie jak język, nazwisko, więzy emocjonalne i inne. Na mocy prawa krajowego skarżący musiał jednak udowodnić, że jego rodzice należeli do rumuńskiej grupy etnicznej. Ze względu na realia historyczne Mołdawii taki wymóg skutkował niemożliwymi do przezwyciężenia przeszkodami w rejestracji tożsamości etnicznej innej niż odnotowana w przypadku jego rodziców przez władze sowieckie. Uniemożliwiając skarżącemu rozpatrzenie jego wniosku w świetle możliwych do obiektywnej weryfikacji dowodów, państwo nie wypełniło pozytywnego obowiązku zapewnienia skarżącemu rzeczywistego poszanowania jego życia prywatnego. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

556 Tamże, art. 16 i motyw 65; zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. e).

557 ETPC, *Ciubotaru przeciwko Mołdawii*, nr 27138/04, 27 kwietnia 2010 r., pkt 51 i 59.

W niektórych przypadkach wystarczy, aby osoba, której dane dotyczą, po prostu zażądała sprostowania, na przykład pisowni nazwiska, zmiany adresu lub numeru telefonu. Zgodnie z **prawem Unii** i **prawem RE** nieprawidłowe dane osobowe należy poprawić bez zbędnej i nadmiernej zwłoki[558]. Jeżeli jednak takie wnioski dotyczą zagadnień istotnych z prawnego punktu widzenia, na przykład tożsamości prawnej osoby, której dane dotyczą, bądź prawidłowego miejsca zamieszkania do celów doręczeń dokumentów prawnych, wnioski o sprostowanie danych mogą nie być wystarczające i administrator może mieć prawo żądać wykazania rzekomych nieprawidłowości. Takie żądania nie mogą nakładać na osobę, której dane dotyczą, nadmiernego ciężaru dowodu, a tym samym uniemożliwiać osobom, których dane dotyczą, poprawienia swoich danych. ETPC stwierdził naruszenie art. 8 EKPC w kilku przypadkach, gdy skarżący nie był w stanie zakwestionować nieprawidłowości informacji przechowywanych w tajnych rejestrach[559].

Przykład: W sprawie *Cemalettin Canli przeciwko Turcji*[560] ETPC stwierdził naruszenie art. 8 EKPC w związku z błędnymi danymi podanymi przez policję w postępowaniu karnym.

Przeciwko skarżącemu dwukrotnie wszczęto postępowanie karne z powodu domniemanego członkostwa w nielegalnych organizacjach, ale nigdy go nie skazano. Gdy skarżącego ponownie aresztowano i oskarżono o inne przestępstwo, policja przedłożyła sądowi karnemu raport zatytułowany „formularz informacyjny o dodatkowych przestępstwach", w którym skarżący figurował jako członek dwóch nielegalnych organizacji. Wniosek skarżącego o poprawienie raportu i dokumentacji policyjnej oddalono. Trybunał uznał, że informacje zawarte w raporcie policyjnym wchodziły w zakres art. 8 EKPC, gdyż systematycznie gromadzone informacje publiczne przechowywane w aktach będących w posiadaniu organów władz mogą również dotyczyć „życia prywatnego". Ponadto raport policyjny był błędnie sporządzony, a sposób jego przedłożenia sądowi karnemu nie był zgodny z prawem krajowym. Trybunał stwierdził, że doszło do naruszenia art. 8.

558 Ogólne rozporządzenie o ochronie danych, art. 16; zaktualizowana konwencja nr 108, art. 9 ust. 1.

559 ETPC, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, 4 maja 2000 r.

560 ETPC, *Cemalettin Canli przeciwko Turcji*, nr 22427/04, 18 listopada 2008 r., pkt 33 i 42–43; ETPC, *Dalea przeciwko Francji*, nr 964/07, 2 lutego 2010 r.

Podczas postępowania cywilnego lub postępowania przed organem władzy publicznej prowadzonego w celu ustalenia, czy dane są prawidłowe, czy też nie, osoba, której dane dotyczą, może wnioskować o zamieszczenie w jej aktach wpisu lub adnotacji wskazującej, że ich dokładność jest kwestionowana, a decyzja urzędowa nie została jeszcze podjęta[561]. W tym okresie administrator danych nie może twierdzić, że dane są prawidłowe lub że nie są zmieniane, zwłaszcza w stosunku do osób trzecich.

6.1.3. Prawo do usunięcia danych („prawo do bycia zapomnianym")

Zagwarantowanie osobom, których dane dotyczą, prawa żądania usunięcia ich danych, ma szczególne znaczenie dla skutecznego stosowania zasad ochrony danych, zwłaszcza zasady minimalizacji danych (dane osobowe muszą być ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane). Prawo usunięcia danych jest zatem zapisane w instrumentach prawnych zarówno RE, jak i UE[562].

Przykład: W sprawie *Segerstedt-Wiberg i in. przeciwko Szwecji*[563] skarżący należeli do liberalnych i komunistycznych partii politycznych. Podejrzewali oni, że informacje na ich temat znalazły się w aktach policyjnych, i zażądali ich usunięcia. ETPC stwierdził, że przechowywanie tych danych miało podstawę prawną i służyło uzasadnionemu celowi. W odniesieniu do niektórych skarżących ETPC uznał jednak, że dalsze zatrzymywanie danych stanowiło nieproporcjonalną ingerencję w ich życie prywatne. Na przykład w przypadku jednego ze skarżących władze przechowywały informacje o tym, jakoby w 1969 r. miał on namawiać do przemocy w reakcji na działania policji podczas demonstracji. Trybunał stwierdził, że ta informacja nie mogła służyć żadnemu istotnemu interesowi bezpieczeństwa narodowego, zwłaszcza ze względu na jej historyczny charakter. ETPC stwierdził, że w odniesieniu do czterech spośród pięciu skarżących doszło do naruszenia art. 8 EKPC, ponieważ zważywszy na długi czas, jaki upłynął od czynów, jakich rzekomo dopuścili się skarżący, dalsze przechowywanie ich danych było bezzasadne.

561 Ogólne rozporządzenie o ochronie danych, art. 18 i motyw 67.

562 Tamże, art. 17.

563 ETPC, *Segerstedt-Wiberg i in. przeciwko Szwecji*, nr 62332/00, 6 czerwca 2006 r., pkt 89 i 90; zob. także na przykład ETPC, *M.K. przeciwko Francji*, nr 19522/09, 18 kwietnia 2013 r.

Przykład: W sprawie *Brunet przeciwko Francji*[564] skarżący zaskarżył przechowywanie jego danych osobowych w policyjnej bazie danych zawierającej informacje o skazanych, oskarżonych i ofiarach przestępstw. Choć postępowanie karne przeciwko skarżącemu umorzono, jego dane w dalszym ciągu widniały w bazie danych. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC. Trybunał zważył, że skarżący nie miał w praktyce możliwości doprowadzenia do usunięcia swoich danych osobowych z przedmiotowej bazy. Ponadto ETPC uwzględnił charakter informacji ujętych w bazie danych i uznał, że ingerowały one w prywatność skarżącego, ponieważ zawierały informacje o jego tożsamości i osobowości. Co więcej, Trybunał stwierdził, że okres zatrzymania danych osobowych w bazie danych, który wynosił 20 lat, był zbyt długi, zwłaszcza w świetle faktu, że skarżący nigdy nie został skazany przez żaden sąd.

W zaktualizowanej konwencji nr 108 wyraźnie uznano, że każda osoba ma prawo usunięcia swoich danych, które są nieprawidłowe, fałszywe lub przetwarzane z naruszeniem prawa[565].

W prawie UE art. 17 RODO umożliwia osobom, których dane dotyczą, żądanie usunięcia lub skasowania ich danych. Prawo żądania niezwłocznego usunięcia swoich danych osobowych ma zastosowanie, gdy:

- dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub były w inny sposób przetwarzane;
- osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie, i nie ma innej podstawy prawnej przetwarzania;
- osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania;
- dane osobowe były przetwarzane niezgodnie z prawem;
- dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

564 ETPC, *Brunet przeciwko Francji*, nr 21010/10, 18 września 2014 r.

565 Zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. e).

- dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 RODO, dzieciom[566].

Ciężar udowodnienia, że przetwarzanie danych jest zgodne z prawem, spoczywa na administratorach danych, gdyż to oni są odpowiedzialni za zgodność przetwarzania z prawem[567]. Zgodnie z zasadą rozliczalności administrator musi zawsze być w stanie wykazać, że przetwarzanie danych opiera się na solidnej podstawie prawnej – w przeciwnym przypadku musi zaprzestać przetwarzania danych[568]. W RODO przewidziano wyjątki od prawa do bycia zapomnianym, obejmujące przypadki, gdy przetwarzanie danych osobowych jest niezbędne:

- do korzystania z prawa do wolności wypowiedzi i informacji;
- do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego;
- do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych;
- do ustalenia, dochodzenia lub obrony roszczeń[569].

TSUE potwierdził, że prawo usunięcia danych jest istotne dla zapewnienia wysokiego poziomu ochrony danych.

Przykład: W sprawie *Google Spain*[570] TSUE rozpatrywał, czy spółka Google miała obowiązek usunąć nieaktualne informacje dotyczące trudności finansowych skarżącego z wyników wyszukiwania. Spółka Google zakwestionowała między innymi swoją odpowiedzialność, podnosząc, że

566 Ogólne rozporządzenie o ochronie danych, art. 17 ust. 1.

567 Tamże.

568 Tamże, art. 5 ust. 2.

569 Tamże, art. 17 ust. 3.

570 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 55–58.

udostępnia jedynie hiperłącze do strony internetowej wydawcy, na której znajdowały się te informacje – w tym przypadku gazety, która poinformowała o problemach skarżącego związanych z niewypłacalnością[571]. Spółka Google twierdziła, że wniosek o usunięcie nieaktualnych informacji ze strony internetowej należało złożyć do dostawcy strony internetowej, nie do spółki Google, gdyż ta zaledwie udostępnia łącze do strony, na której informacje te zostały pierwotnie opublikowane. Trybunał stwierdził, że spółka Google, przeszukując sieć pod kątem informacji i stron internetowych oraz indeksując treści w celu udostępniania wyników wyszukiwania, przyjmuje rolę administratora danych, który podlega obowiązkom i zobowiązaniom wynikającym z prawa UE.

Trybunał wyjaśnił, że wyszukiwarki internetowe i wyniki wyszukiwania zawierające dane osobowe mogą umożliwiać sporządzenie szczegółowego profilu danej osoby[572]. Wyszukiwarki sprawiają, że informacje ujęte na takiej liście wyników są powszechnie dostępne. Biorąc pod uwagę potencjalną wagę tej ingerencji, nie może być ona uzasadniona jedynie interesem, jaki ma w tym przetwarzaniu danych operator wyszukiwarki internetowej. Należy dążyć do znalezienia punktu równowagi pomiędzy uzasadnionym interesem internautów zainteresowanych uzyskaniem dostępu do tej informacji a prawami podstawowymi przysługującymi osobie, której dane dotyczą, na podstawie art. 7 i 8 Karty praw podstawowych UE. W coraz bardziej zdigitalizowanym społeczeństwie wymóg, by dane osobowe były dokładne i nie wykraczały poza to, co niezbędne (tj. do celów informowania społeczeństwa), ma zasadnicze znaczenie dla zapewnienia wysokiego poziomu ochrony danych osób. [Operator wyszukiwarki] „winien w ramach spoczywającej na nim odpowiedzialności, przysługujących mu uprawnień i posiadanych możliwości zapewnić, iż działalność ta spełnia określone w dyrektywie 95/46 wymogi, tak aby przewidziane w niej gwarancje były

571 Ponadto spółka Google zakwestionowała zastosowanie unijnych przepisów z zakresu ochrony danych na tej podstawie, że siedziba spółki Google Inc. mieści się w Stanach Zjednoczonych i przetwarzanie przedmiotowych danych osobowych również odbywało się w tym kraju. Kolejny argument przemawiający za brakiem możliwości zastosowania prawa UE o ochronie danych był związany z twierdzeniem, że wyszukiwarek nie można uznać za „administratorów" danych wyświetlanych w wynikach wyszukiwania, gdyż nie posiadają one o nich żadnej wiedzy i nie sprawują nad nimi kontroli. Trybunał oddalił oba argumenty, uznając że dyrektywa 95/46/WE miała w przedmiotowej sprawie zastosowanie, i przystąpił do przeanalizowania zakresu praw nadanych na mocy tego aktu, zwłaszcza prawa usunięcia danych osobowych.

572 Tamże, pkt 36, 38, 80–81 i 97.

w pełni skuteczne”[573]. Oznacza to, że prawo żądania usunięcia swoich danych osobowych w przypadku, gdy są one nieaktualne bądź gdy przetwarzanie nie jest już niezbędne, obejmuje również administratorów danych, którzy je powielają[574].

Analizując, czy spółka Google była zobowiązana do usunięcia łączy dotyczących skarżącego czy też nie, TSUE uznał, że w określonych okolicznościach osoby mają prawo żądać usunięcia swoich danych osobowych. Na prawo to można się powołać, gdy informacje odnoszące się do danej osoby są nieprawidłowe, niewłaściwe, niestosowne bądź nadmierne ilościowo w stosunku do celów, do których są przetwarzane. Trybunał uznał, że prawo to nie jest bezwzględne – wymaga wyważenia względem innych praw i interesów, zwłaszcza interesu szerokiego grona odbiorców w dostępie do określonych informacji. Każdy wniosek o usunięcie należy oceniać indywidualnie, by znaleźć równowagę między podstawowymi prawami do ochrony danych osobowych i życia prywatnego osoby, której dane dotyczą, z jednej strony, a uzasadnionymi interesami wszystkich internautów, w tym wydawców, z drugiej. Trybunał przedstawił zalecenia dotyczące czynników, jakie należy w takim kontekście uwzględnić. Szczególnie istotnym czynnikiem jest charakter przedmiotowych informacji. Jeśli odnoszą się one do życia prywatnego danej osoby, a dostępność tych informacji nie leży w interesie publicznym, względy ochrony danych i prywatności są nadrzędne wobec prawa szerokiego grona odbiorców do dostępu do tych informacji. Z drugiej zaś strony, jeśli osoba, której dane dotyczą, jest osobą publiczną, bądź jeżeli charakter informacji uzasadnia udostępnienie ich szerokiemu gronu odbiorców, wówczas nadrzędny interes ogółu w dostępie do tych informacji może uzasadniać ingerencję w podstawowe prawa osoby, której dane dotyczą, do ochrony danych i prywatności.

573 Tamże, pkt 81–83.

574 TSUE, C-131/12 *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 88. Zob. także Grupa Robocza Art. 29 (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, Bruksela, 26 listopada 2014 r. oraz Recommendation CM/Rec 2012(3) of the Committee of Ministers to member states on the protection of human rights with regard to search engines, 4 kwietnia 2012 r.

W następstwie tego wyroku Grupa Robocza Art. 29 przyjęła wytyczne dotyczące wykonania orzeczenia TSUE[575]. Wytyczne te zawierają wykaz wspólnych kryteriów, z których organy nadzorcze mają korzystać podczas rozpatrywania skarg dotyczących wniosków osób fizycznych o usunięcie danych, a także wyjaśnienie, co prawo usunięcia danych obejmuje oraz wskazówki dotyczące osiągania równowagi między prawami poszczególnych stron. W wytycznych tych podkreślono, że oceny tych okoliczności należy dokonywać w każdym przypadku indywidualnie. Jako że prawo do bycia zapomnianym nie jest bezwzględne, wynik rozpatrzenia wniosku może się różnić w zależności od sprawy. Odzwierciedla to również orzecznictwo TSUE w sprawach rozpatrywanych po sprawie Google.

Przykład: W sprawie *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*[576] TSUE rozpatrywał, czy po rozwiązaniu spółki osobie przysługuje prawo żądania usunięcia danych osobowych opublikowanych w rejestrze spółek. S. Manni zażądał od izby handlowej w Lecce usunięcia jego danych osobowych z tego rejestru, gdy zdał sobie sprawę, że potencjalni klienci mogli zasięgnąć informacji z rejestru i dowiedzieć się, że zarządzał on wcześniej spółką, która ponad dekadę wcześniej zbankrutowała. Zdaniem skarżącego informacja ta mogłaby zniechęcić potencjalnych klientów.

Dokonując wyważenia przysługującego S. Manniemu prawa do ochrony jego danych osobowych na tle interesu szerokiego grona odbiorców w dostępie do tych informacji, TSUE wziął pod uwagę przede wszystkim cel tego publicznego rejestru. Trybunał zwrócił uwagę na fakt, że jawność tych informacji przewidziano w przepisach, zwłaszcza w dyrektywie UE mającej na celu ułatwienie osobom trzecim dostępu do informacji o spółkach. Osobom trzecim powinno się zatem udostępnić i zapewnić wgląd w podstawowe dokumenty spółki oraz inne informacje na jej temat, „w szczególności dane szczegółowe dotyczące osób, które są uprawnione do nabywania praw i zaciągania zobowiązań w imieniu spółki". Celem ujawnienia było

575 Grupa Robocza Art. 29 (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, Bruksela, 26 listopada 2014 r.

576 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 9 marca 2017 r.

ponadto zapewnienie pewności prawa w przypadku wzmocnienia wymiany handlowej między państwami członkowskimi poprzez zagwarantowanie osobom trzecim dostępu do wszystkich istotnych informacji o spółkach w UE.

Trybunał zauważył ponadto, że nawet wraz z upływem czasu i po rozwiązaniu spółki przysługujące jej prawa i spoczywające na niej zobowiązania nadal pozostają w mocy. Spory związane z rozwiązaniem spółki mogą toczyć się bardzo długo, a kwestie dotyczące spółki, jej kierowników i likwidatorów mogą wyniknąć nawet lata po zakończeniu działalności. Trybunał stwierdził, że ze względu na dużą liczbę możliwych sytuacji oraz różnice w zakresie terminów przedawnienia obowiązujących w poszczególnych państwach członkowskich „wydaje się, że nie jest możliwe ustalenie jednolitego terminu, biegnącego od dnia rozwiązania spółki, po upływie którego wpis rzeczonych danych w rejestrze i ich jawność nie byłyby już konieczne". W świetle prawnie uzasadnionego celu ujawnienia oraz trudności w ustaleniu okresu, po upływie którego byłoby możliwe usunięcie danych osobowych z rejestru bez szkody dla interesów osób trzecich, TSUE uznał, że unijne przepisy z zakresu ochrony danych nie gwarantują prawa usunięcia danych osobowych osobom, które znalazły się w podobnej sytuacji, co S. Manni.

Jeżeli administrator upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to jest zobowiązany i musi podjąć „rozsądne" działania, by poinformować innych administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda ich usunięcia. Podejmując działania, administrator musi uwzględniać dostępną technologię i koszt ich realizacji[577].

6.1.4. Prawo do ograniczenia przetwarzania

Artykuł 18 RODO nadaje osobom, których dane dotyczą, prawo do tymczasowego ograniczenia przetwarzania ich danych osobowych przez administratora. Osoby, których dane dotyczą, mają prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:

- osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych;

577 Ogólne rozporządzenie o ochronie danych, art. 17 ust. 2 i motyw 66.

- przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, żąda ograniczenia wykorzystywania danych zamiast ich usunięcia;
- dane muszą zostać zachowane do celów dochodzenia lub obrony roszczeń;
- oczekuje się na wydanie decyzji w kwestii prawnie uzasadnionych interesów administratora danych nadrzędnych wobec interesów osoby, której dane dotyczą[578].

Wśród metod pozwalających administratorowi ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych lub czasowe usunięcie opublikowanych danych[579]. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą[580].

Obowiązek powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

Administrator musi informować o sprostowaniu lub usunięciu danych osobowych lub wszelkim ograniczeniu przetwarzania każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku[581]. Jeżeli osoba, której dane dotyczą, zażąda informacji o tych odbiorcach, administrator jej ich udziela[582].

6.1.5. Prawo do przenoszenia danych

Na mocy RODO osoby, których dane dotyczą, mają prawo do przenoszenia danych w przypadkach, gdy dane osobowe, które dostarczyły administratorowi, są przetwarzane w sposób zautomatyzowany na podstawie zgody lub gdy przetwarzanie danych osobowych jest niezbędne do wykonania umowy i odbywa się w sposób zautomatyzowany. Oznacza to, że prawo do przenoszenia danych nie ma

578 Tamże, art. 18 ust. 1.
579 Tamże, motyw 67.
580 Tamże, art. 18 ust. 3.
581 Tamże, art. 19.
582 Tamże.

zastosowania wówczas, gdy przetwarzanie danych osobowych opiera się na podstawie prawnej innej niż zgoda lub umowa[583].

Jeżeli prawo do przenoszenia danych ma zastosowanie, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe[584]. W tym celu administrator powinien opracować interoperacyjne formaty, które umożliwiają osobom, których dane dotyczą, przenoszenie danych[585]. Rozporządzenie określa, że aby umożliwić interoperacyjność, dane te muszą być przekazywane w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego[586]. Interoperacyjność można w szerokim rozumieniu zdefiniować jako zdolność systemów informacyjnych do wymiany danych oraz do umożliwienia dzielenia się informacjami[587]. Choć celem stosowanych formatów jest osiągnięcie interoperacyjności, RODO nie nakłada szczególnych zaleceń dotyczących konkretnych formatów: mogą się one różnić w poszczególnych sektorach[588].

Zgodnie z wytycznymi Grupy Roboczej Art. 29 prawo do przenoszenia danych „wspiera możliwość dokonywania wyboru i sprawowania kontroli przez użytkownika oraz uprawnienia użytkownika", co ma na celu zwiększenie kontroli osób, których dane dotyczą, nad ich własnymi danymi[589]. W wytycznych wyjaśniono najważniejsze elementy przenoszenia danych, do których należą:

- prawo osób, których dane dotyczą, do otrzymywania w ustrukturyzowanym, powszechnie używanym, interoperacyjnym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyły administratorowi;

- prawo przesłania danych osobowych przez jednego administratora danych innemu administratorowi bez przeszkód, o ile jest to technicznie możliwe;

583 Tamże, motyw 68 i art. 20 ust. 1.

584 Tamże, art. 20 ust. 2.

585 Tamże, motyw 68 i art. 20 ust. 1.

586 Tamże, motyw 68.

587 Komunikat Komisji z dnia 2 kwietnia 2016 r. „Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa", COM(2016) 205 final.

588 Grupa Robocza Art. 29 (2016), *Guidelines on the right to data portability*, WP 242, 13 grudnia 2016 r., zmienione 5 kwietnia 2017 r., s. 13.

589 Tamże.

- system sprawowania kontroli – gdy administrator odpowiada na wniosek o przeniesienie danych, działa w imieniu osoby, której dane dotyczą, co oznacza, że nie jest odpowiedzialny za zapewnienie zgodności z prawem ochrony danych przez odbiorcę, zważywszy że to osoba, której dane dotyczą, wybiera, do kogo dane są przenoszone;

- wykonanie prawa do przenoszenia danych odbywa się bez uszczerbku dla jakiegokolwiek innego prawa, tak jak w przypadku wszelkich innych praw w ramach RODO.

6.1.6. Prawo do sprzeciwu

Osoby, których dane dotyczą, mogą skorzystać z prawa sprzeciwu wobec przetwarzania danych osobowych z uwagi na swoją szczególną sytuację oraz wobec przetwarzania danych do celów marketingu bezpośredniego. Prawo sprzeciwu można wykonać za pośrednictwem zautomatyzowanych środków.

Prawo sprzeciwu z uwagi na szczególną sytuację osób, których dane dotyczą

Osobom, których dane dotyczą, nie przysługuje ogólne prawo sprzeciwu wobec przetwarzania ich danych[590]. W artykule 21 ust. 1 RODO przyznaje się osobie, której dane dotyczą, prawo wniesienia sprzeciwu z przyczyn związanych z jej szczególną sytuacją, jeżeli podstawą prawną przetwarzania jest wykonanie przez administratora zadania realizowanego w interesie publicznym lub gdy przetwarzanie opiera się na prawnie uzasadnionym interesie administratora[591]. Prawo sprzeciwu odnosi się do profilowania. Podobne prawo zapisano w zaktualizowanej konwencji nr 108[592].

Prawo sprzeciwu z uwagi na szczególną sytuację osoby, której dane dotyczą, ma na celu zapewnienie właściwej równowagi między prawami osoby, której dane dotyczą, do ochrony danych osobowych a uzasadnionymi prawami innych osób w związku z przetwarzaniem takich danych. TSUE wyjaśnił jednak, że prawa osoby, której dane dotyczą, są „co do zasady" nadrzędne wobec interesów gospodarczych administratora danych, w zależności od „charakteru rozpatrywanych informacji i od

590 Zob. także ETPC, *M.S. przeciwko Szwecji*, nr 20837/92, 27 sierpnia 1997 r. [gdziebez zgody lub możliwości sprzeciwu przekazano dane medyczne]; ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.; ETPC, *Mosley przeciwko Zjednoczonemu Królestwu*, nr 48009/08, 10 maja 2011 r.

591 Ogólne rozporządzenie o ochronie danych, motyw 69; art. 6 ust. 1 lit. e) i f).

592 Zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. d); zalecenie w sprawie profilowania, art. 5 ust. 3.

tego, jak istotne są one dla prywatności osoby, której dane dotyczą, oraz dla publicznego interesu w dysponowaniu tą informacją"[593]. Zgodnie z RODO ciężar udowodnienia spoczywa na administratorach, którzy muszą wykazać przekonujące podstawy uzasadniające dalsze przetwarzanie[594]. Podobnie sprawozdanie wyjaśniające do zaktualizowanej konwencji nr 108 wyjaśnia, że uzasadnione podstawy przetwarzania danych (które mogą być nadrzędne wobec prawa sprzeciwu przysługującego osobie, której dane dotyczą) muszą być wykazywane indywidualnie w każdym przypadku[595].

Przykład: W sprawie *Manni*[596] TSUE uznał, że z uwagi na zgodny z prawem cel ujawnienia danych osobowych w rejestrze spółek, zwłaszcza potrzebę ochrony interesów osób trzecich i zapewnienia pewności prawa, co do zasady S. Manni nie miał prawa żądać usunięcia swoich danych osobowych z tego rejestru. Trybunał potwierdził jednak istnienie prawa sprzeciwu wobec przetwarzania, stwierdzając, że „nie można wykluczyć ewentualności zaistnienia sytuacji szczególnych, w których przeważające i uzasadnione względy dotyczące konkretnego przypadku osoby, której dane dotyczą, uzasadniają wyjątkowo, aby dostęp do figurujących w rejestrze danych osobowych dotyczących tej osoby został ograniczony, po upływie wystarczająco długiego okresu [...] do kręgu osób trzecich mających konkretny, uzasadniony interes w uzyskaniu wglądu do tych danych".

Trybunał uznał, że to na sądach krajowych spoczywa obowiązek przeanalizowania każdej sprawy w świetle wszystkich istotnych okoliczności sytuacji danej osoby oraz tego, czy istnieją uzasadnione i przeważające względy, które mogłyby wyjątkowo usprawiedliwić ograniczenie dostępu osób trzecich do danych osobowych figurujących w rejestrach spółek. Trybunał wyjaśnił jednak, że w przypadku S. Manniego sama okoliczność, iż ujawnienie jego danych osobowych w rejestrze rzekomo wpłynęło na

593 TSUE, C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r., pkt 81.

594 Zob. także zaktualizowana konwencja nr 108, art. 98 ust. 1 lit. d), który stanowi, że osoba, której dane dotyczą, może wyrazić sprzeciw wobec przetwarzania swoich danych, „chyba że administrator wykaże uzasadnione podstawy przetwarzania, nadrzędne wobec interesów lub praw i podstawowych wolności danej osoby".

595 Explanatory Report of Modernised Convention 108, pkt 78.

596 TSUE, C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 9 marca 2017 r., pkt 47 i 60.

jego klientów, nie może stanowić takiego uprawnionego i przeważającego względu. Potencjalni klienci S. Manniego mają uzasadniony interes w tym, by mieć dostęp do informacji o bankructwie jego poprzedniej firmy.

W wyniku skutecznego sprzeciwu administrator nie może dalej przetwarzać przedmiotowych danych. Operacje przetwarzania wykonywane na danych osoby, której dane dotyczą, przed wniesieniem sprzeciwu pozostają jednak zgodne z prawem.

Prawo do sprzeciwu wobec przetwarzania danych do celów marketingu bezpośredniego

W art. 21 ust. 2 RODO zapisano konkretne prawo do sprzeciwu wobec wykorzystania danych osobowych do celów marketingu bezpośredniego, wyjaśniając tym samym bardziej szczegółowo art. 13 dyrektywy o prywatności i łączności elektronicznej. Prawo takie zawarto również w zaktualizowanej konwencji nr 108 oraz w zaleceniu w sprawie marketingu bezpośredniego RE[597]. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 wyjaśniono, że sprzeciw wobec przetwarzania danych osobowych do celów marketingu bezpośredniego powinien skutkować bezwarunkowym usunięciem bądź skasowaniem przedmiotowych danych osobowych[598].

Osoba, której dane dotyczą, ma prawo wnieść sprzeciw wobec wykorzystania jej danych osobowych do celów marketingu bezpośredniego w dowolnym momencie i bezpłatnie. Osoby, których dane dotyczą, należy o tym poinformować jasno i oddzielnie od wszelkich innych informacji.

Prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków

Jeżeli dane osobowe są wykorzystywane i przetwarzane do celów usług społeczeństwa informacyjnego, osoba, której dane dotyczą, może wykonać swoje sprawo do sprzeciwu wobec przetwarzania swoich danych za pośrednictwem zautomatyzowanych środków.

597 Rada Europy, Komitet Ministrów (1985), zalecenie Rec(85)20 dla państw członkowskich w sprawie ochrony danych osobowych wykorzystywanych do celów marketingu bezpośredniego, 25 października 1985 r., art. 4 ust. 1.

598 Explanatory Report of Modernised Convention 108, pkt 79.

Definicja usług społeczeństwa informacyjnego obejmuje każdą usługę normalnie świadczoną za wynagrodzeniem, na odległość, drogą elektroniczną i na indywidualne żądanie odbiorcy usług[599].

Administratorzy danych oferujący usługi społeczeństwa informatycznego muszą dysponować odpowiednimi ustaleniami i procedurami technicznymi, by zapewnić możliwość skutecznego wykonywania prawa sprzeciwu za pośrednictwem zautomatyzowanych środków[600]. Może to być na przykład blokowanie plików cookie w witrynach lub wyłączenie śledzenia przeglądania Internetu.

Prawo do sprzeciwu wobec przetwarzania do celów badań naukowych lub historycznych lub do celów statystycznych

Zgodnie z prawem UE badania naukowe należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych[601]. Do badań historycznych należą też badania do celów genealogicznych; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do osób zmarłych[602]. Wyrażenie „cele statystyczne" oznacza każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych[603]. Również w tym przypadku podstawą prawną prawa sprzeciwu wobec przetwarzania danych osobowych do celów badań naukowych jest szczególna sytuacja takiej osoby[604]. Wyjątek stanowi sytuacja, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym. Prawo do usunięcia nie ma jednak zastosowania w sytuacji, gdy przetwarzanie danych jest niezbędne (czy to w interesie publicznym, czy też nie) do celów badań naukowych lub historycznych lub do celów statystycznych[605].

Rozporządzenie zapewnia równowagę między wymogami związanymi z badaniami naukowymi, statystycznymi lub historycznymi oraz prawami osób, których dane dotyczą, za pomocą konkretnych zabezpieczeń i odstępstw zapisanych w art. 89.

599 Dyrektywa 98/34/WE zmieniona dyrektywą 98/48/WE ustanawiającą procedurę udzielania informacji w zakresie norm i przepisów technicznych, art. 1 ust. 1.

600 Ogólne rozporządzenie o ochronie danych, art. 21 ust. 5.

601 Tamże, motyw 159.

602 Tamże, motyw 160.

603 Tamże, motyw 162.

604 Tamże, art. 21 ust. 6.

605 Tamże, art. 17 ust. 3 lit. d).

Zatem prawo Unii lub prawo państw członkowskich może przewidywać odstępstwa od prawa do sprzeciwu, jeżeli prawo to może uniemożliwić bądź znacznie utrudnić osiągnięcie celów badawczych, oraz gdy takie odstępstwa są niezbędne do realizacji tych celów.

W **prawie RE** art. 9 ust. 2 zaktualizowanej konwencji nr 108 stanowi, że prawo może przewidywać ograniczenia praw osób, których dane dotyczą, w tym prawa do sprzeciwu, w odniesieniu do przetwarzania danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, jeżeli w oczywisty sposób brak jest ryzyka naruszenia praw i podstawowych wolności osób, których dane dotyczą.

Niemniej w sprawozdaniu wyjaśniającym (pkt 41) uznano również, że osoby, których dane dotyczą, powinny mieć możliwość wyrażenia zgody wyłącznie w odniesieniu do określonych dziedzin badań lub części projektów badawczych – w zakresie, w jakim zamierzony cel to umożliwia – oraz wniesienia sprzeciwu, gdy ich zdaniem przetwarzanie bez uzasadnionych podstaw nadmiernie ingeruje w ich prawa i wolności.

Innymi słowy, takie przetwarzanie byłoby zatem z założenia uznawane za zgodne z prawem, pod warunkiem że istniałyby inne zabezpieczenia oraz że te operacje co do zasady wyłączałyby wykorzystanie pozyskanych informacji w jakikolwiek sposób na potrzeby decyzji lub środków dotyczących danej osoby.

6.1.7. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie

Decyzje zautomatyzowane to decyzje podejmowane z wykorzystaniem danych osobowych przetwarzanych wyłącznie w sposób automatyczny, bez jakiejkolwiek interwencji ludzkiej. **Zgodnie z prawem UE** osoby, których dane dotyczą, nie mogą podlegać zautomatyzowanemu podejmowaniu decyzji wywołujących wobec nich skutki prawne lub w podobny sposób znacząco na nie wpływające. Jeżeli takie decyzje mogą wywierać znaczny wpływ na życie jednostek ze względu na to, że dotyczą na przykład zdolności kredytowej, elektronicznej rekrutacji, wyników osiąganych w pracy lub analizy sposobu zachowania lub wiarygodności, niezbędna jest specjalna ochrona, aby uniknąć niepożądanych konsekwencji. Do zautomatyzowanego podejmowania decyzji zalicza się profilowanie, które obejmuje dowolne

zautomatyzowane przetwarzanie pozwalające ocenić „czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się"[606].

Przykład: Aby szybko ocenić zdolność kredytową przyszłego klienta, biura informacji kredytowej (BIK) zbierają określone dane, na przykład informacje o jego historii kredytowej lub zobowiązaniach za usługi/media, dane o poprzednich adresach klienta, jak również informacje pochodzące ze źródeł publicznych, takie jak spis wyborców, rejestry publiczne (w tym wyroki sądowe) lub dane dotyczące bankructwa i niewypłacalności. Te dane osobowe są następnie wprowadzane do algorytmu oceny, który oblicza ogólną wartość odzwierciedlającą zdolność kredytową potencjalnego klienta.

Zdaniem Grupy Roboczej Art. 29 prawo do niepodlegania decyzjom opartym wyłącznie na zautomatyzowanym przetwarzaniu, wywołującym wobec osób, których dane dotyczą, skutki prawne lub w podobny sposób istotnie na nie wpływające, jest równoznaczne z ogólnym zakazem i nie wymaga aktywnego wyrażenia sprzeciwu wobec takiej decyzji przez osobę, której dane dotyczą[607].

Niemniej na mocy RODO zautomatyzowane podejmowanie decyzji wywołujące skutki prawne bądź istotnie wpływające na osoby fizyczne może być dopuszczalne, jeśli jest niezbędne do zawarcia lub wykonania umowy między administratorem danych a osobą, której dane dotyczą, lub w przypadku gdy osoba, której dane dotyczą, udzieli na to wyraźnej zgody. Zautomatyzowane podejmowanie decyzji jest ponadto dopuszczalne, gdy jest dozwolone prawem, a prawa, wolności i prawnie uzasadnione interesy osoby, której dane dotyczą, są właściwie zabezpieczone[608].

Wśród obowiązków administratora dotyczących informacji, które należy przekazać w sytuacji, gdy dochodzi do zbierania danych, RODO przewiduje obowiązek informowania osób, których dane dotyczą, o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu[609]. Nie ma to wpływu na prawo dostępu do danych

606 Tamże, motyw 71, art. 4 ust. 4 i art. 22.

607 Grupa Robocza Art. 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 października 2017 r., s. 15.

608 Ogólne rozporządzenie o ochronie danych, art. 22 ust. 2.

609 Tamże, art. 12.

osobowych przetwarzanych przez administratora[610]. W informacjach tych należy nie tylko wskazać fakt, że będzie realizowane profilowanie, lecz także zawrzeć istotne informacje na temat zasad profilowania oraz o przewidywanych konsekwencjach dla osoby, której przetwarzane dane dotyczą[611]. Przykładowo zakład ubezpieczeń zdrowotnych przetwarzający wnioski z wykorzystaniem zautomatyzowanego podejmowania decyzji powinien przekazać osobom, których dane dotyczą, ogólne informacje o tym, jak działa algorytm oraz które czynniki bierze pod uwagę przy obliczaniu składek na ubezpieczenie. Również wykonując „prawo dostępu", osoby, których dane dotyczą, mogą zwrócić się do administratora o informacje o zautomatyzowanym podejmowaniu decyzji oraz istotne informacje o zasadach ich podejmowania[612].

Informacje podawane osobom, których dane dotyczą, mają na celu zapewnienie przejrzystości oraz umożliwienie takim osobom wyrażenia świadomej zgody (w stosownych przypadkach) lub uzyskanie interwencji ludzkiej. Administrator danych jest zobowiązany do wdrażania właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Obejmuje to co najmniej prawo do uzyskania interwencji ludzkiej ze strony administratora, możliwość wyrażenia przez osobę, której dane dotyczą, własnego stanowiska oraz zakwestionowania decyzji opartej na zautomatyzowanym przetwarzaniu jej danych osobowych[613].

Grupa Robocza Art. 29 przedstawiła dodatkowe wytyczne na temat korzystania ze zautomatyzowanego podejmowania decyzji na mocy RODO[614].

Zgodnie z prawem RE osoby fizyczne mają prawo do niepodlegania decyzji, która istotnie na nie wpłynie i która opiera się wyłącznie na zautomatyzowanym przetwarzaniu danych bez uwzględnienia jej stanowiska[615]. Wymóg uwzględnienia stanowiska osoby, której dane dotyczą, w przypadku, gdy decyzje opierają się wyłącznie na zautomatyzowanym przetwarzaniu, oznacza, że osoba taka ma prawo zakwestionować takie decyzje i powinna mieć prawo zakwestionować nieścisłości w wykorzystywanych przez administratora danych osobowych, jak również

610 Tamże, art. 15.

611 Tamże, art. 13 ust. 2 lit. f).

612 Tamże, art. 15 ust. 1 lit. h).

613 Tamże, art. 22 ust. 3.

614 Grupa Robocza Art. 29 (2017), *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, WP 251, 3 października 2017 r.

615 Zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. a).

zasadność jakiegokolwiek profilu zastosowanego w odniesieniu do takiej osoby[616]. Osoba fizyczna nie może jednak skorzystać z tego prawa, jeżeli zautomatyzowana decyzja jest dozwolona prawem, któremu administrator podlega i w którym przewidziano odpowiednie środki zabezpieczające prawa, wolności i uzasadnione interesy osoby, której dane dotyczą. Ponadto osoby, których dane dotyczą, mają prawo otrzymać, na żądanie, informacje o powodach przetwarzania danych osobowych[617]. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 przedstawiono przykład punktowej oceny kredytowej. Osoby fizyczne powinny mieć prawo wiedzieć nie tylko o pozytywnej lub negatywnej decyzji podjętej w wyniku oceny, lecz także o *zasadach* przetwarzania ich danych osobowych, które doprowadziły do podjęcia takiej, a nie innej decyzji. „Zrozumienie tych elementów przyczynia się do skutecznego wykonywania innych podstawowych zabezpieczeń, takich jak prawo do sprzeciwu i prawo do wniesienia skargi do właściwego organu"[618].

Zalecenie w sprawie profilowania, choć nie jest prawnie wiążące, określa warunki zbierania i przetwarzania danych osobowych w kontekście profilowania[619]. Zawarto w nim zapisy dotyczące potrzeby zapewnienia, by przetwarzanie w kontekście profilowania było rzetelne, zgodne z prawem, proporcjonalne oraz by służyło konkretnym, zgodnym z prawem celom. Ujęto w nim zapisy o informacjach, jakie administratorzy danych powinni przekazywać osobom, których dane dotyczą. W zaleceniu tym zapisano również zasadę jakości danych – wymagającą od administratorów podejmowania środków w celu poprawy czynników wpływających na nieprawidłowość danych, ograniczenia ryzyka lub błędów związanych z profilowaniem oraz okresowego przeglądu jakości wykorzystanych danych i algorytmów.

616 Projekt sprawozdania wyjaśniającego do zaktualizowanej konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108), pkt 75.

617 Zaktualizowana konwencja nr 108, art. 9 ust. 1 lit. c).

618 Explanatory Report of Modernised Convention 108, pkt 73.

619 Rada Europy, Recommendation CM/Rec(2010)13 of the Committee of Ministers to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling, art. 5 ust. 5.

6.2. Środki prawne, odpowiedzialność, sankcje i odszkodowanie

Najważniejsze kwestie

- Zgodnie ze zaktualizowaną konwencją nr 108 w prawie krajowym umawiających się stron trzeba określić odpowiednie środki prawne i sankcje w przypadku naruszenia prawa do ochrony danych.
- W prawie UE RODO przewiduje środki prawne, z których osoby, których dane dotyczą, mogą korzystać w przypadku naruszenia ich praw, jak również sankcje nakładane na administratorów i podmioty przetwarzające, którzy nie przestrzegają przepisów rozporządzenia. W rozporządzeniu przewidziano ponadto prawo do odszkodowania i odpowiedzialność.
  - Osoby, których dane dotyczą, mają prawo do wniesienia skargi do organu nadzorczego w związku z rzekomym naruszeniem rozporządzenia, jak również prawo do skutecznego środka ochrony prawnej przed sądem oraz do uzyskania odszkodowania.
  - Podczas wykonywania swojego prawa do skutecznego środka prawnego osoby mogą być reprezentowane przez organizacje pożytku publicznego działające w obszarze ochrony danych.
  - Administrator lub podmiot przetwarzający odpowiada za wszelkie szkody majątkowe i niemajątkowe powstałe wskutek naruszenia.
  - Za naruszenia rozporządzenia organy nadzorcze mogą nakładać administracyjne kary pieniężne w wysokości do 20 000 000 EUR lub w przypadku przedsiębiorstw – 4% całkowitego rocznego światowego obrotu, przy czym zastosowanie ma kwota wyższa.
- Osoby, których dane dotyczą, mogą kierować sprawy dotyczące naruszenia prawa o ochronie danych do ETPC – po wyczerpaniu wszystkich innych środków i pod pewnymi warunkami.
- Każda osoba fizyczna lub prawna ma prawo wnieść do TSUE skargę o unieważnienie każdej decyzji Europejskiej Rady Ochrony Danych na warunkach przewidzianych w traktatach.

Przyjęcie instrumentów prawnych nie jest wystarczające do zagwarantowania ochrony danych osobowych w Europie. Aby zwiększyć skuteczność europejskich przepisów w zakresie ochrony danych, konieczne jest ustanowienie mechanizmów umożliwiających osobom przeciwstawienie się naruszaniu ich praw oraz

dochodzenie odszkodowań z tytułu poniesionych szkód. Ponadto ważne jest, by organy nadzorcze dysponowały uprawnieniami do nakładania sankcji, które są skuteczne, odstraszające i proporcjonalne w stosunku do danego naruszenia.

Prawa wynikające z przepisów o ochronie danych może wykonywać osoba, której prawa są zagrożone – czyli osoba, której dane dotyczą. Niemniej w imieniu osób, których dane dotyczą, mogą podczas wykonywania ich praw występować również inne osoby – spełniające niezbędne wymogi przewidziane w prawie krajowym. Zgodnie z ustawodawstwem krajowym dzieci i osoby z niepełnosprawnościami umysłowymi muszą być reprezentowane przez ich opiekunów[620]. Zgodnie z prawem UE o ochronie danych zrzeszenie, którego zgodnym z prawem celem jest promowanie praw ochrony danych, może reprezentować osoby, których dane dotyczą, przed organem nadzorczym lub sądem[621].

6.2.1. Prawo do wniesienia skargi do organu nadzorczego

Zarówno zgodnie z prawem **RE**, jak i **UE** osoby fizyczne mają prawo do wnoszenia wniosków i skarg do właściwego organu nadzorczego, jeżeli ich zdaniem przetwarzanie ich danych osobowych przebiega z naruszeniem prawa.

W zaktualizowanej konwencji nr 108 uznano prawo osób, których dane dotyczą, do skorzystania z pomocy organu nadzorczego przy wykonywaniu ich praw wynikających z konwencji, niezależnie od ich narodowości i miejsca pobytu[622]. Wniosek o wsparcie może zostać odrzucony wyłącznie w szczególnych okolicznościach, a osoby, których dane dotyczą, nie powinny ponosić kosztów i opłat wynikających z udzielenia pomocy[623].

Podobne przepisy można znaleźć w systemie prawnym UE. Rozporządzenie nakłada na organy nadzorcze wymóg stosowania środków ułatwiających wnoszenie skarg, takich jak utworzenie elektronicznego formularza skargi[624]. Osoba, której dane

620 FRA (2015), Podręcznik prawa europejskiego dotyczącego praw dziecka, Luksemburg, Urząd Publikacji; FRA (2013), Legal capacity of persons with intellectual disabilities and persons with mental health problems, Luksemburg, Urząd Publikacji.

621 Ogólne rozporządzenie o ochronie danych, art. 80.

622 Zaktualizowana konwencja nr 108, art. 18.

623 Tamże, art. 16–17.

624 Ogólne rozporządzenie o ochronie danych, art. 57 ust. 2.

dotyczą, ma prawo wnieść skargę do organu nadzorczego w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia[625]. Skargi muszą zostać rozpatrzone, a organ nadzorczy musi poinformować daną osobę o wyniku rozpatrzenia skargi[626].

Potencjalne naruszenia po stronie instytucji lub organów UE można zgłaszać do Europejskiego Inspektora Ochrony Danych[627]. W przypadku braku odpowiedzi EIOD w ciągu sześciu miesięcy skargę uznaje się za odrzuconą. Odwołania od decyzji EIOD można zgłaszać do TSUE w ramach rozporządzenia (WE) nr 45/2001, w którym nałożono na instytucje i organy UE obowiązek przestrzegania przepisów z zakresu ochrony danych.

Musi istnieć możliwość wniesienia odwołania od decyzji krajowego organu nadzorczego do sądów. Odnosi się to do osoby, której dane dotyczą, jak również administratorów i podmiotów przetwarzających, które były stroną postępowania przed organem nadzorczym.

Przykład: We wrześniu 2017 r. hiszpański organ ochrony danych nałożył na spółkę Facebook grzywnę za naruszenie szeregu regulacji z zakresu ochrony danych. Organ nadzorczy potępił sieć społecznościową za zbieranie, przechowywanie i przetwarzanie danych osobowych, w tym szczególnych kategorii danych osobowych, do celów reklamowych i bez uzyskania zgody osoby, której dane dotyczą. Decyzję wydano w wyniku dochodzenia przeprowadzonego z inicjatywy własnej organu nadzorczego.

6.2.2. Prawo do skutecznego środka ochrony prawnej przed sądem

Oprócz prawa wniesienia skargi do organu nadzorczego osoby fizyczne muszą mieć prawo do skutecznego środka ochrony prawnej przed sądem oraz do wystąpienia ze sprawą na drogę sądową. Prawo do środka ochrony prawnej jest wyraźnie

625 Tamże, art. 77 ust. 1.

626 Tamże, art. 77 ust. 2.

627 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

wpisane w europejską tradycję prawną i jest uznawane za prawo podstawowe, zarówno na mocy art. 47 Karty praw podstawowych UE, jak i art. 13 EKPC[628].

Jeśli chodzi o prawo UE, znaczenie zagwarantowania osobom, których dane dotyczą, skutecznych środków prawnych w przypadku naruszenia ich praw jasno wynika zarówno z przepisów RODO – które ustanawia prawo do skutecznego środka ochrony prawnej przed sądem przeciwko organom nadzorczym, administratorom i podmiotom przetwarzającym – jak i z orzecznictwa TSUE.

Przykład: W sprawie *Maximillian Schrems przeciwko Data Protection Commissioner*[629] TSUE stwierdził nieważność decyzji o prawidłowości ochrony przewidzianej przez zasady „bezpiecznej przystani". Decyzja ta dopuszczała międzynarodowe przekazywanie danych z UE do organizacji w USA, które dokonały samocertyfikacji w ramach programu „bezpiecznej przystani". Trybunał zidentyfikował w programie szereg braków, które naruszały podstawowe prawa obywateli Unii do ochrony prywatności, danych osobowych oraz prawo do skutecznego środka ochrony prawnej.

W kwestii naruszenia prawa do prywatności i ochrony danych TSUE podkreślił, że ustawodawstwo USA dopuszcza dostęp określonych organów publicznych do danych osobowych przekazywanych z państw członkowskich do USA oraz przetwarzanie ich w sposób niezgodny z celami, dla których dane te zostały pierwotnie przekazane, oraz w zakresie wykraczającym poza to, co ściśle niezbędne i proporcjonalne do ochrony bezpieczeństwa narodowego. W kwestii prawa do skutecznego środka prawnego Trybunał stwierdził, że osobom, których dane dotyczą, nie przysługiwała droga administracyjna ani sądowa umożliwiająca im uzyskanie dostępu do dotyczących ich danych i, w odpowiednim przypadku, dokonania ich sprostowania lub usunięcia. Trybunał stwierdził, że uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych „nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty". Trybunał podkreślił, że

628 Zob. na przykład ETPC, *Karabeyoğlu przeciwko Turcji*, nr 30083/10, 7 czerwca 2016 r.; ETPC, *Mustafa Sezgin Tanrıkulu przeciwko Turcji*, nr 27473/06, 18 lipca 2017 r.

629 TSUE, sprawa C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

istnienie środków ochrony prawnej przed sądem służącej zapewnieniu poszanowania przepisów prawa jest nierozerwalnie związane z istnieniem państwa prawa.

Osoby fizyczne, administratorzy i podmioty przetwarzające chcące zakwestionować prawnie wiążącą decyzję organu nadzorczego mogą wszcząć postępowanie przed sądem[630]. Pojęcie „decyzja" należy interpretować szeroko jako obejmujące wykonywanie przez organy nadzorcze uprawnień do prowadzenia postępowań wyjaśniających, nakładania kar i do wydawania zezwoleń oraz oddalania lub odrzucania skarg. Niemniej niemające wiążącej mocy prawnej środki przyjęte przez organy nadzorcze, takie jak wydawane przez nie opinie czy zalecenia nie mogą być przedmiotem sprawy wniesionej do sądu[631]. Sprawy sądowe należy wszczynać przed sądami państwa członkowskiego, w którym dany organ nadzorczy ma siedzibę[632].

W przypadku naruszenia praw osoby, której dane dotyczą, przez administratora lub podmiot przetwarzający, taka osoba ma prawo wnieść skargę do sądu[633]. W przypadku postępowań przeciwko administratorowi lub podmiotowi przetwarzającemu szczególne znaczenie ma umożliwienie osobom fizycznym wyboru miejsca wszczęcia postępowania. Osoba taka może wnieść skargę w państwie członkowskim, w którym administrator lub podmiot przetwarzający ma jednostkę organizacyjną, albo w państwie członkowskim, w którym dana osoba, której dane dotyczą, ma miejsce zwykłego pobytu[634]. Druga z wymienionych możliwości znacznie ułatwia osobom fizycznym wykonywanie przysługujących im praw, ponieważ pozwala im wnosić skargi w państwie, w którym zamieszkują, w znanej im jurysdykcji. Ograniczenie miejsca postępowań przeciwko administratorom i podmiotom przetwarzającym do państwa członkowskiego, w którym mają jednostkę organizacyjną, mogłoby zniechęcać osoby, których dane dotyczą, zamieszkujące w innych państwa członkowskich do występowania na drogę sądową, jako że wymagałoby podróży i dodatkowych kosztów, a postępowanie mogłoby toczyć się w obcym języku i w nieznanej jurysdykcji. Jedyny wyjątek dotyczy spraw, w których administrator lub podmiot przetwarzający są organami publicznymi, a przetwarzanie odbywa się w ramach wykonywania ich uprawnień publicznych. W takim przypadku wyłącznie

630 Ogólne rozporządzenie o ochronie danych, art. 78.

631 Tamże, motyw 143.

632 Tamże, art. 78 ust. 3.

633 Tamże, art. 79.

634 Tamże, art. 79 ust. 2.

sądy państwa, w którym mieści się dany organ publiczny, są właściwe do rozpatrywania roszczenia[635].

Choć w większości przypadków sprawy dotyczące zasad ochrony danych będą rozpatrywane przez sądy państw członkowskich, niektóre można wnieść do TSUE. Jest to możliwe po pierwsze w sytuacji, gdy osoba, której dane dotyczą, administrator, podmiot przetwarzający lub organ nadzorczy dążą do unieważnienia decyzji Europejskiej Rady Ochrony Danych. Skarga podlega jednak warunkom art. 263 TFUE, co oznacza, że aby była dopuszczalna, takie osoby i podmioty muszą wykazać, że decyzja Rady dotyczy ich bezpośrednio i indywidualnie.

Druga możliwość dotyczy spraw niezgodnego z prawem przetwarzania danych osobowych przez instytucje lub organy UE. W przypadkach naruszenia prawa o ochronie danych przez instytucje UE osoby, których dane dotyczą, mogą wnieść skargę bezpośrednio do Sądu Unii Europejskiej (Sąd wchodzi w skład TSUE). Sąd odpowiada za rozpatrywanie, w pierwszej instancji, skarg na naruszenia prawa UE przez instytucje Unii. Z tego względu skargi przeciwko Europejskiemu Inspektorowi Ochrony Danych – będącemu instytucją UE – również można wnosić do Sądu[636].

Przykład: W sprawie *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*.[637] spółka zwróciła się do Komisji Europejskiej z wnioskiem o dostęp do pełnego protokołu spotkania zorganizowanego przez Komisję, które rzekomo dotyczyło kwestii prawnych istotnych dla spółki. Komisja odrzuciła wniosek spółki o dostęp ze względu na nadrzędny interes ochrony danych[638]. Na podstawie art. 32 rozporządzenia o ochronie danych przez instytucje UE spółka Bavarian Lager wniosła na tę decyzję skargę do Sądu Pierwszej Instancji (poprzednika Sądu). Wyrokiem w sprawie T-194/04 *The Bavarian Lager Co. Ltd przeciwko Komisji Wspólnot Europejskich* Sąd Pierwszej Instancji stwierdził nieważność decyzji Komisji o odrzuceniu wniosku o dostęp. Komisja Europejska odwołała się od tego wyroku do TSUE.

635 Tamże.

636 Rozporządzenie (WE) nr 45/2001, art. 32 ust. 3.

637 TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd* [WI], 2010.

638 Analizę sprawy można znaleźć w dokumencie: EIOD (2011), *Public access to documents containing personal data after the Bavarian Lager ruling,* Bruksela, EIOD.

Zasiadając jako Wielka Izba, Trybunał Sprawiedliwości UE uchylił wyrok Sądu Pierwszej Instancji i potwierdził odmowę Komisji Europejskiej dotyczącą wniosku o dostęp do pełnego protokołu spotkania, aby ochronić dane osobowe osób, które w nim uczestniczyły. Trybunał przyznał, że decyzja Komisji o odmowie ujawnienia tych informacji była słuszna, zważywszy że uczestnicy spotkania nie wyrazili zgody na ujawnienie ich danych osobowych. Ponadto spółka Bavarian Lager nie zdołała wykazać, że dostęp do informacji jest jej niezbędny.

Ponadto osoby, których dane dotyczą, organy nadzorcze, administratorzy lub podmioty przetwarzające mogą podczas postępowania krajowego zwrócić się do sądu krajowego z wnioskiem, aby ten zwrócił się do TSUE o wyjaśnienie w sprawie wykładni i ważności aktów instytucji, organów, urzędów lub agencji UE. Takie wyjaśnienia noszą nazwę orzeczeń w trybie prejudycjalnym. Nie dają one skarżącemu bezpośredniego środka prawnego, ale umożliwiają sądom krajowym upewnienie się, że dokonują prawidłowej wykładni prawa UE. To właśnie przez mechanizm orzeczeń w trybie prejudycjalnym takie znaczące sprawy jak *Digital Rights Ireland* i Kärntner Landesregierung i in.[639] oraz *Schrems*[640], które w ogromnej mierze przyczyniły się do rozwoju prawa UE w zakresie ochrony danych, trafiły do rozpatrzenia przez TSUE.

Przykład: Sprawy *Digital Rights Ireland* i *Kärntner Landesregierung i in.*[641] to sprawy połączone wszczęte przez irlandzki wysoki trybunał i austriacki trybunał konstytucyjny w przedmiocie zgodności dyrektywy 2006/24/WE (dyrektywy retencyjnej) z prawem UE w zakresie ochrony danych. Austriacki trybunał konstytucyjny przedłożył do TSUE pytania dotyczące ważności art. 3–9 dyrektywy 2006/24/WE w świetle art. 7, 9 i 11 Karty praw podstawowych UE. W pytaniach tych trybunał zwrócił się między innymi o rozstrzygnięcie, czy określone przepisy austriackiej ustawy federalnej

639 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

640 Sprawa C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

641 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

o telekomunikacji transponującej dyrektywę retencyjną są niezgodne z określonymi aspektami poprzedniej dyrektywy o ochronie danych i rozporządzeniem w sprawie ochrony danych przez instytucje UE.

Jeden ze skarżących w postępowaniu w sprawie *Kärntner Landesregierung i in.*, M. Seitlinger, stwierdził, że używa telefonu, Internetu oraz poczty elektronicznej zarówno w celach zawodowych, jak i w życiu prywatnym. W związku z tym informacje, które wysyła i odbiera, są przekazywane za pośrednictwem publicznych sieci telekomunikacyjnych. Na mocy austriackiej ustawy o telekomunikacji z 2003 r. jego operator telekomunikacyjny jest zobowiązany prawem do gromadzenia i przechowywania danych na temat korzystania przez niego z sieci. Zdaniem M. Seitlingera takie gromadzenie i przechowywanie jego danych osobowych nie jest konieczne do celów technicznych związanych z przesłaniem i odbieraniem informacji w sieci. Gromadzenie i przechowywanie tych danych nie jest też niezbędne do celów rozliczeń. M. Seitlinger oświadczył, że nie wyraził zgody na takie wykorzystanie jego danych osobowych, a jedynym powodem ich gromadzenia i przechowywania była austriacka ustawa o telekomunikacji z 2003 r.

M. Seitlinger wniósł w związku z tym do austriackiego trybunału konstytucyjnego skargę, w której zarzucił, że obowiązki ustawowe jego operatora telekomunikacyjnego naruszają jego prawa podstawowe na mocy art. 8 Karty praw podstawowych UE. Zważywszy że przedmiotowe austriackie przepisy wdrażały prawo UE (ówczesną dyrektywę retencyjną), austriacki trybunał konstytucyjny skierował sprawę do TSUE, by ten rozpatrzył czy dyrektywa jest zgodna z prawem do poszanowania życia prywatnego i prawem do ochrony danych zapisanymi w Karcie praw podstawowych UE.

Wielka Izba TSUE wydała w tej sprawie orzeczenie, w wyniku którego stwierdzono nieważność dyrektywy retencyjnej UE. Trybunał stwierdził, że dyrektywa wyjątkowo mocno ingeruje w podstawowe prawa do poszanowania życia prywatnego i ochrony danych, a ingerencja ta nie ogranicza się do tego, co ściśle niezbędne. Przedmiotowa dyrektywa służyła uzasadnionemu celowi, ponieważ umożliwiała organom krajowym skorzystanie z dodatkowych możliwości dochodzenia i ścigania poważnych przestępstw i z tego względu stanowiła cenne narzędzie przy prowadzeniu czynności dochodzeniowo-śledczych. Trybunał stwierdził jednak, że ograniczenia praw podstawowych powinny ograniczać się do

tego, co absolutnie konieczne, oraz że powinny im towarzyszyć jasne i dokładne reguły dotyczące ich zakresu, jak również zapewnione osobom zabezpieczenia.

Zdaniem TSUE dyrektywa nie spełniła kryteriów konieczności. Po pierwsze, nie ustanowiono w niej jasnych i dokładnych reguł ograniczających zakres ingerencji w prawa. Zamiast wymagać istnienia związku między zatrzymanymi danymi i poważnym przestępstwem, dyrektywa odnosiła się do wszystkich metadanych wszystkich użytkowników wszystkich środków łączności elektronicznej. Dyrektywa stanowi zatem ingerencję w prawa do poszanowania życia prywatnego i ochrony danych prawie wszystkich mieszkańców UE, co może być uznawane za nieproporcjonalne. W dyrektywie brak było warunków ograniczających grono osób upoważnionych do dostępu do danych osobowych, a ponadto taki dostęp nie podlegał warunkom proceduralnym, takim jak wymóg uzyskania uprzedniej zgody organu administracyjnego lub sądu. Co więcej, w dyrektywie nie przewidziano jasnych zabezpieczeń umożliwiających ochronę zatrzymanych danych. Z tego względu nie zapewniała skutecznej ochrony danych przed ryzykiem nadużycia oraz przed jakimkolwiek nieuprawnionym dostępem i wykorzystaniem[642].

Co do zasady TSUE musi odpowiedzieć na zadane mu pytania i nie może odmówić wydania orzeczenia w trybie prejudycjalnym, twierdząc, że nie byłoby ono istotne ani wydane w terminie w odniesieniu do pierwotnej sprawy. Może jednak odmówić, jeżeli pytanie nie wchodzi w zakres jego właściwości[643]. TSUE orzeka jedynie w przedmiocie elementów skierowanego do niego wniosku o wydanie orzeczenia w trybie prejudycjalnym, pierwotną sprawę rozstrzyga natomiast sąd krajowy[644].

Zgodnie z prawem RE umawiające się strony mają obowiązek ustanowić odpowiednie środki ochrony przed sądem i pozasądowe środki ochrony dostępne w przypadku naruszenia postanowień zaktualizowanej konwencji nr 108[645]. Zarzuty doty-

642 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r., pkt 69.

643 TSUE, C-244/80, *Pasquale Foglia przeciwko Marielli Novello* (nr 2), 16 grudnia 1981 r.; TSUE, C-467/04, *Postępowanie karne przeciwko Giuseppemu Francescowi Gasparinniemu i innym*, 28 września 2006 r.

644 TSUE, C-438/05, *International Transport Workers' Federation, Finnish Seamen's Union przeciwko Viking Line ABP, OÜ Viking Line Eesti* [WI], 11 grudnia 2007 r., pkt 85.

645 Zaktualizowana konwencja nr 108, art. 12.

czące naruszeń praw do ochrony danych stanowiących naruszenie art. 8 EKPC przez umawiającą się stronę EKPC można dodatkowo kierować do ETPC po wyczerpaniu wszystkich dostępnych krajowych środków ochrony prawnej. Skarga na naruszenie art. 8 EKPC kierowana do ETPC musi także spełniać inne kryteria dopuszczalności (art. 34–35 EKPC)[646].

Chociaż skargi do ETPC mogą być kierowane tylko przeciwko umawiającym się stronom, mogą one też wynikać pośrednio z działań lub zaniechań osób prywatnych w zakresie, w jakim umawiająca się strona nie dopełniła swoich pozytywnych zobowiązań wynikających z EKPC i nie zapewniła wystarczającej ochrony przed naruszeniami prawa do ochrony danych w swoim prawie krajowym.

Przykład: W sprawie *K.U. przeciwko Finlandii*[647] małoletni skarżący zarzucił, że w internetowym serwisie randkowym zamieszczono dotyczący go anons o charakterze seksualnym. Usługodawca odmówił ujawnienia tożsamości osoby, która opublikowała informacje, z powodu obowiązków w zakresie poufności wynikających z prawa fińskiego. Skarżący twierdził, że prawo krajowe nie zapewnia wystarczającej ochrony przed działaniami osoby prywatnej umieszczającej w Internecie obciążające dane dotyczące skarżącego. ETPC uznał, że państwa mają nie tylko obowiązek powstrzymania się od arbitralnej ingerencji w prywatne życie osób, ale mogą także spoczywać na nich pozytywne obowiązki, które obejmują „przyjęcie środków mających na celu zapewnienie poszanowania życia prywatnego nawet w sferze relacji między osobami prywatnymi". W przypadku skarżącego praktyczna i skuteczna ochrona wymagała podjęcia skutecznych działań w celu zidentyfikowania i ścigania sprawcy. Państwo nie zapewniło jednak takiej ochrony, więc Trybunał uznał, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Köpke przeciwko Niemcom*[648] skarżącą podejrzewano o kradzież w miejscu pracy, w związku z czym poddano ją ukrytemu nadzorowi wideo. ETPC stwierdził, że „nic nie wskazuje, aby władze krajowe nie wyważyły we właściwy sposób, w ramach swojej swobody uznania, z jednej strony prawa skarżącej do poszanowania jej życia prywatnego na

646 EKPC, art. 34–37.

647 ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2 grudnia 2008 r.

648 ETPC, *Köpke przeciwko Niemcom* [dec.], nr 420/07, 5 października 2010 r.

mocy art. 8, a z drugiej strony interesu jej pracodawcy do ochrony swojego prawa własności i interesu publicznego we właściwym sprawowaniu wymiaru sprawiedliwości". Skargę uznano zatem za niedopuszczalną.

Jeżeli ETPC ustali, że umawiająca się strona naruszyła którekolwiek z praw chronionych na mocy EKPC, taka umawiająca się strona jest zobowiązana wykonać wyrok Trybunału (art. 46 EKPC). Środki wykonawcze muszą w pierwszej kolejności usunąć naruszenie i naprawić, jeżeli jest to możliwe, jego negatywne skutki dla skarżącego. Wykonanie wyroków może też wymagać zastosowania ogólnych środków w celu zapobieżenia naruszeniom podobnym do ustalonych przez Trybunał – przez zmiany w ustawodawstwie, orzecznictwie lub inne środki.

W przypadku gdy ETPC stwierdzi naruszenie EKPC, może zgodnie z art. 41 EKPC przyznać skarżącemu „słuszne zadośćuczynienie" na koszt umawiającej się strony.

Prawo umocowania podmiotu, organizacji lub zrzeszenia, które nie mają charakteru zarobkowego

RODO umożliwia osobom wnoszącym skargi do organu nadzorczego lub wszczynającym postępowanie przed sądem umocowanie podmiotu, organizacji lub zrzeszenia, które nie mają charakteru zarobkowego, do występowania w ich imieniu[649]. Takie podmioty muszą mieć statutowo na celu interes publiczny i działać w dziedzinie ochrony danych osobowych. Mogą one wówczas wnieść skargę lub wykonać prawo do środka ochrony prawnej przed sądem w imieniu osoby, której dane dotyczą. W rozporządzeniu pozostawiono państwom członkowskim swobodę zadecydowania – zgodnie z prawem krajowym – czy organ może wnosić skargi w imieniu osób, których dane dotyczą, bez uzyskania od nich upoważnienia.

To prawo do reprezentacji daje osobom fizycznym możliwość skorzystania z wiedzy fachowej i możliwości organizacyjnych i finansowych takich podmiotów, co znacznie ułatwia takim osobom wykonywanie swoich praw. RODO umożliwia tym podmiotom wnoszenie powództw zbiorowych w imieniu wielu osób, których dane dotyczą. Ma to dodatkowo korzystny wpływ na funkcjonowanie i wydajność systemu sądowego, ponieważ podobne roszczenia są grupowane i rozpatrywane łącznie.

649 Ogólne rozporządzenie o ochronie danych, art. 80.

6.2.3. Odpowiedzialność i prawo do odszkodowania

Prawo do skutecznego środka ochrony prawnej musi umożliwiać osobom fizycznym dochodzenie odszkodowania z tytułu wszelkich szkód poniesionych w wyniku przetwarzania ich danych osobowych z naruszeniem obowiązujących przepisów. Odpowiedzialność administratorów i podmiotów przetwarzających z tytułu niezgodnego z prawem przetwarzania została wyraźnie przewidziana w RODO[650]. Rozporządzenie daje osobom fizycznym prawo do otrzymania od administratora lub podmiotu przetwarzającego odszkodowania zarówno z tytułu szkód majątkowych, jak i niemajątkowych, a w motywach wskazano, że „pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia"[651]. W przypadku niedopełnienia swoich zobowiązań wynikających z rozporządzenia administratorzy ponoszą odpowiedzialność i mogą być przeciwko nim kierowane roszczenia odszkodowawcze. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie wtedy, gdy nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Administrator lub podmiot przetwarzający, który zapłacił odszkodowanie za całą wyrządzoną szkodę, ma na mocy RODO prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność[652]. Stosowanie wyjątków od odpowiedzialności jest obwarowane surowymi warunkami i wymaga dowiedzenia, że administrator lub podmiot przetwarzający w żaden sposób nie odpowiada za zdarzenie będące przyczyną szkody.

Odszkodowanie musi być „pełne i skuteczne" w odniesieniu do poniesionej szkody. W sytuacji gdy szkoda jest spowodowana przetwarzaniem przez kilku administratorów i podmioty przetwarzające, każdy z administratorów i podmiotów przetwarzających musi odpowiadać za całość szkody. Ta zasada ma na celu zagwarantowanie osobom, których dane dotyczą, skutecznego odszkodowania oraz zapewnienie skoordynowanego podejścia do przestrzegania przepisów przez administratorów i podmioty przetwarzające zaangażowanych w przetwarzanie.

650 Tamże, art. 82.

651 Tamże, motyw 146.

652 Tamże, art. 82 ust. 2 i 5.

Przykład: Podmioty, których dane dotyczą, nie muszą występować ze skargą i dochodzić odszkodowania od wszystkich podmiotów odpowiedzialnych za szkodę, gdyż może się to wiązać z kosztownymi i długotrwałymi postępowaniami. Wystarczy wnieść skargę przeciwko jednemu ze współadministratorów, który może wówczas zostać pociągnięty do odpowiedzialności za całość szkody. W takich przypadkach administrator lub podmiot przetwarzający, który zapłaci za szkodę, może następnie dochodzić od innych podmiotów uczestniczących w przetwarzaniu i odpowiedzialnych za naruszenie zwrotu zapłaconej kwoty w części odpowiadającej odpowiedzialności tych podmiotów za przedmiotową szkodę. Takie postępowania między współadministratorami i podmiotami przetwarzającymi rozpoczynają się po otrzymaniu przez osobę, której dane dotyczą, odszkodowania i osoba ta w nich nie uczestniczy.

W ramach prawnych RE art. 12 zmodernizowanej konwencji nr 108 wymaga od umawiających się stron ustanowienia odpowiednich środków ochrony prawnej w przypadku naruszenia przepisów krajowych wdrażających wymogi konwencji. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 wskazano, że środki ochrony prawnej muszą umożliwiać zaskarżenie decyzji lub praktyki na drodze sądowej, przy czym należy też zagwarantować pozasądowe środki ochrony[653]. Tryb korzystania z dostępu do tych środków ochrony, jak również zasady i procedury korzystania z nich pozostają w gestii poszczególnych umawiających się stron. Umawiające się strony oraz sądy krajowe powinny ponadto rozważyć wprowadzenie przepisów dotyczących odszkodowania z tytułu szkód majątkowych i niemajątkowych wynikłych z przetwarzania, jak również możliwość wnoszenia powództw zbiorowych[654].

6.2.4. Sankcje

Jeżeli chodzi o prawo RE, zgodnie z art. 12 zaktualizowanej konwencji nr 108 każda z umawiających się stron ma obowiązek wprowadzić odpowiednie sankcje i środki ochrony prawnej w przypadku naruszenia przepisów prawa krajowego wprowadzających w życie podstawowe zasady ochrony danych ustanowione w konwencji nr 108. Konwencja nie ustanawia ani nie narzuca konkretnego zbioru sankcji. Wręcz przeciwnie – wyraźnie wskazuje, że każda z umawiających się stron może według własnego uznania określać charakter sankcji sądowych lub pozasądowych,

653 Explanatory Report of Modernised Convention 108, pkt 100.

654 Tamże.

do których mogą należeć sankcje karne, administracyjne bądź cywilne. W sprawozdaniu wyjaśniającym do zaktualizowanej konwencji nr 108 przewidziano, że sankcje muszą być skuteczne, proporcjonalne i odstraszające[655]. Umawiające się strony mają obowiązek przestrzegać tej zasady podczas określania charakteru i dotkliwości sankcji przewidzianych w krajowym porządku prawnym.

Jeżeli chodzi o prawo UE, zgodnie z art. 83 RODO organy nadzorcze państw członkowskich są uprawnione do nakładania administracyjnych kar pieniężnych za naruszenie przepisów rozporządzenia. Wysokość takich kar pieniężnych oraz okoliczności, jakie organy krajowe muszą wziąć uwagę podczas podejmowania decyzji o ich ewentualnym nałożeniu, jak również maksymalna wysokość kary są przewidziane w art. 83. System sankcji jest zatem w UE zharmonizowany.

RODO przewiduje wielopoziomowe podejście do kar pieniężnych. Za naruszenia rozporządzenia organy nadzorcze mogą nakładać administracyjne kary pieniężne w wysokości do 20 000 000 EUR lub w przypadku przedsiębiorstw – 4% całkowitego rocznego światowego obrotu, przy czym zastosowanie ma kwota wyższa. Do naruszeń, za które można nałożyć karę pieniężną w takiej wysokości, należą naruszenia podstawowych zasad przetwarzania i warunków zgody, naruszenia praw osób, których dane dotyczą, oraz przepisów rozporządzenia regulujących przekazywanie danych osobowych odbiorcom w państwach trzecich. Za inne naruszenia organy nadzorcze mogą nakładać kary pieniężne w wysokości do 10 000 000 EUR lub w przypadku przedsiębiorstw – 2% całkowitego rocznego światowego obrotu, przy czym zastosowanie ma kwota wyższa.

Przy ustalaniu rodzaju i wysokości kary pieniężnej organy nadzorcze muszą wziąć pod uwagę szereg czynników[656]. Przykładowo muszą zwrócić należytą uwagę na charakter, wagę i czas trwania naruszenia, kategorie danych osobowych, których ono dotyczy, oraz to, czy naruszenie było umyślne czy też nie. W przypadku gdy administrator lub podmiot przetwarzający podjął działania w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą, taką okoliczność również należy uwzględnić. Stopień współpracy z organem nadzorczym po wystąpieniu naruszenia oraz sposób, w jaki organ nadzorczy się o nim dowiedział (na przykład czy zostało ono zgłoszone przez podmiot odpowiedzialny za przetwarzanie czy

655 Tamże.

656 Ogólne rozporządzenie o ochronie danych, art. 83 ust. 2.

przez osobę, której dane dotyczą, której prawa naruszono) również należą do istotnych czynników wpływających na decyzje organów nadzorczych[657].

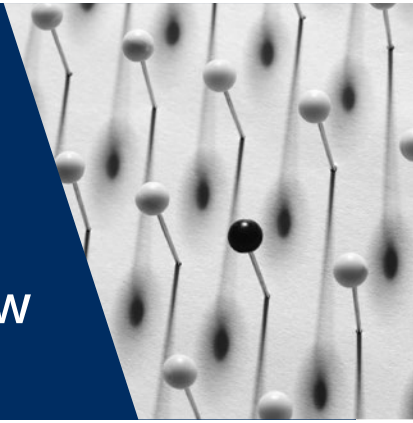
Oprócz możliwości nakładania administracyjnych kar pieniężnych organom nadzorczym przysługuje szereg uprawnień naprawczych. Tak zwane „uprawnienia naprawcze" organów nadzorczych określono w art. 58 RODO. Obejmują one różne środki – od wydawania nakazów i ostrzeżeń oraz udzielania upomnień administratorom i podmiotom przetwarzającym po wprowadzanie czasowych, a nawet stałych zakazów przetwarzania.

W odniesieniu do sankcji z tytułu naruszenia prawa UE przez instytucje lub organy unijne, ze względu na szczególny zakres rozporządzenia o ochronie danych przez instytucje UE, przewiduje się jedynie sankcje w postaci postępowania dyscyplinarnego. Zgodnie z art. 49 rozporządzenia „niedopełnienie zobowiązań wynikających z niniejszego rozporządzenia, niezależnie od tego, czy celowe czy przez zaniedbanie, powoduje, że urzędnik lub inny funkcjonariusz Wspólnot Europejskich podlega karze dyscyplinarnej […]".

657 Grupa Robocza Art. 29 (2017), *Guidelines on the application and setting of administrative fines for the purpose of the Regulation 2016/679*, WP 253, 3 października 2017 r.

7

Międzynarodowe przekazywanie i przepływ danych osobowych



UE	Omówione zagadnienia	RE
Przekazywanie danych osobowych		
Artykuł 44 ogólnego rozporządzenia o ochronie danych	Pojęcie	Artykuł 14 ust. 1 i 2 zaktualizowanej konwencji nr 108
Swobodny przepływ danych osobowych		
Artykuł 1 ust. 3 i motyw 170 ogólnego rozporządzenia o ochronie danych	Między państwami członkowskimi UE	
	Między umawiającymi się stronami konwencji nr 108	Artykuł 14 ust. 1 zaktualizowanej konwencji nr 108
Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych		
Artykuł 45 ogólnego rozporządzenia o ochronie danych C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 2015	Decyzja stwierdzająca odpowiedni poziom ochrony/państwa trzecie lub organizacje międzynarodowe zapewniające odpowiedni poziom ochrony	Artykuł 14 ust. 2 zaktualizowanej konwencji nr 108
Artykuł 46 ust. 1 i art. 46 ust. 2 ogólnego rozporządzenia o ochronie danych	Odpowiednie zabezpieczenia, w tym egzekwowalne prawa osób, których dane dotyczą, i środki ochrony prawnej, zapewniane za pomocą standardowych klauzul umownych, wiążących reguł korporacyjnych, kodeksów postępowania i mechanizmów certyfikacji	Artykuł 14 ust. 2, 3, 5 i 6 zaktualizowanej konwencji nr 108

UE	Omówione zagadnienia	RE
Artykuł 46 ust. 3 ogólnego rozporządzenia o ochronie danych Artykuł 46 ust. 5 ogólnego rozporządzenia o ochronie danych	Z zastrzeżeniem zezwolenia właściwego organu nadzorczego: klauzule umowne i postanowienia uzgodnień administracyjnych między organami publicznymi Istniejące zezwolenia wydane na podstawie dyrektywy 95/46/WE	
Artykuł 47 ogólnego rozporządzenia o ochronie danych	Wiążące reguły korporacyjne	
Artykuł 49 ogólnego rozporządzenia o ochronie danych	Wyjątki w szczególnych sytuacjach	Artykuł 14 ust. 4 zaktualizowanej konwencji nr 108
Przykłady: Umowa PNR UE–USA Umowa SWIFT UE–USA	Umowy międzynarodowe	Artykuł 14 ust. 3 lit. a) zaktualizowanej konwencji nr 108

W ramach prawa UE ogólne rozporządzenie o ochronie danych zapewnia swobodny przepływ danych w granicach Unii Europejskiej. Przewidziano w nim jednak szczególne wymogi dotyczące przekazywania danych osobowych do państw trzecich poza UE i do organizacji międzynarodowych. W rozporządzeniu uznano znaczenie takiego przekazywania danych, zwłaszcza w kontekście handlu międzynarodowego i współpracy międzynarodowej, zwrócono też jednak uwagę na zwiększone ryzyko naruszenia ochrony danych osobowych. W związku z tym rozporządzenie ma na celu zapewnienie takiego samego poziomu ochrony danych osobowych przekazywanych do państw trzecich, jaki jest zagwarantowany w UE[658]. RE również uznała znaczenie przepisów wykonawczych dotyczących transgranicznego przepływu danych, przewidujących swobodny przepływ między stronami konwencji oraz szczególne wymogi obowiązujące w przypadku przekazywania danych do państw niebędących stronami.

658 Ogólne rozporządzenie o ochronie danych, motywy 101 i 116.

7.1. Charakter przekazywania danych osobowych

Najważniejsze kwestie

- Zarówno prawo UE, jak i prawo RE obejmuje przepisy regulujące przekazywanie danych osobowych do odbiorców w państwach trzecich lub do organizacji międzynarodowych.
- Zagwarantowanie zabezpieczenia praw osoby, której dane dotyczą, w sytuacji przekazywania danych poza UE umożliwia obejmowanie danych osobowych pochodzących z UE ochroną zapewnioną na mocy prawa UE, gdziekolwiek zostaną przekazane.

Prawo RE definiuje transgraniczny przepływ danych jako przekazywanie danych osobowych do odbiorców, którzy podlegają jurysdykcji zagranicznej[659]. Transgraniczny przepływ danych do odbiorcy, który nie podlega jurysdykcji umawiającej się strony, dopuszcza się wyłącznie pod warunkiem zapewnienia odpowiedniego poziomu ochrony[660].

Prawo UE reguluje przekazywanie „danych osobowych, które są przetwarzane lub mają być przetwarzane po przekazaniu do państwa trzeciego lub organizacji międzynarodowej [...]"[661]. Taki przepływ danych jest możliwy wyłącznie wówczas, gdy takie państwa lub organizacje przestrzegają zasad określonych w rozdziale V RODO.

Na mocy prawa RE bądź UE jest możliwy transgraniczny przepływ danych osobowych do odbiorcy podlegającego jurysdykcji odpowiednio umawiającej się strony lub państwa członkowskiego. Ponadto oba systemy prawne dopuszczają przekazywanie danych do państwa niebędącego umawiającą się stroną bądź państwem członkowskim z zastrzeżeniem spełnienia określonych warunków.

659 Zaktualizowana konwencja nr 108, pkt 102.

660 Zaktualizowana konwencja nr 108, art. 14 ust. 2.

661 Ogólne rozporządzenie o ochronie danych, art. 44.

7.2. Swobodny przepływ danych osobowych między państwami członkowskimi lub między umawiającymi się stronami

Najważniejsze kwestie

- Przepływ danych osobowych w UE, jak również przekazywanie danych osobowych między umawiającymi się stronami zaktualizowanej konwencji nr 108 muszą być wolne od ograniczeń. Tym niemniej, jako że nie wszystkie umawiające się strony zaktualizowanej konwencji nr 108 są państwami członkowskimi UE, przekazywanie danych z państwa członkowskiego UE do państwa trzeciego, będącego wszakże umawiającą się stroną konwencji nr 108, nie jest możliwe, o ile państwo to nie spełni warunków określonych w RODO.

Zgodnie z prawem RE musi istnieć swobodny przepływ danych osobowych między umawiającymi się stronami konwencji nr 108. Można jednak zakazać przekazywania danych osobowych, jeżeli istnieje „rzeczywiste i poważne ryzyko, że przekazanie innej stronie doprowadzi do obchodzenia przepisów konwencji" lub gdy stronę zobowiązują do tego „zharmonizowane zasady ochrony obowiązujące państwa należące do regionalnej organizacji międzynarodowej"[662].

Na mocy prawa UE ograniczenia lub zakazy dotyczące swobodnego przepływu danych osobowych między państwami członkowskimi UE z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych są zabronione[663]. Obszar swobodnego przepływu danych poszerzono na mocy Porozumienia o Europejskim Obszarze Gospodarczym (EOG)[664], które włączyło do rynku wewnętrznego Islandię, Liechtenstein i Norwegię.

Przykład: Jeżeli podmiot stowarzyszony międzynarodowej grupy mającej jednostki organizacyjne w kilku państwach członkowskich, w tym w Słowenii i we Francji, przesyła dane osobowe ze Słowenii do Francji, krajowe prawo słoweńskie nie może ograniczać ani zakazywać takiego przepływu danych z powodów odnoszących się do ochrony danych osobowych.

662 Zaktualizowana konwencja nr 108, art. 12 ust. 1

663 Ogólne rozporządzenie o ochronie danych, art. 1 ust. 3.

664 Decyzja Rady i Komisji z dnia 13 grudnia 1993 r. w sprawie zawarcia Porozumienia o Europejskim Obszarze Gospodarczym, między Wspólnotami Europejskimi, ich Państwami Członkowskimi a Republiką Austrii, Republiką Finlandii, Republiką Islandii, Księstwem Liechtensteinu, Królestwem Norwegii, Królestwem Szwecji i Konfederacją Szwajcarską, Dz.U. L 1 z 3.1.1994.

Jeżeli jednak ten sam słoweński podmiot stowarzyszony pragnie przekazać te same dane osobowe spółce dominującej w Malezji, słoweński podmiot przekazujący dane musi uwzględnić zasady przewidziane w rozdziale V RODO. Zawarte w nim przepisy mają na celu zabezpieczenie danych osobowych osób, których dane dotyczą, podlegających jurysdykcji UE.

Jeżeli chodzi o prawo UE, przepływ danych osobowych do państw członkowskich EOG do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar reguluje dyrektywa (UE) 2016/680[665] . Przepisy te gwarantują dodatkowo, że wymiana danych osobowych między właściwymi organami w Unii nie jest ograniczona ani zakazana ze względu na ochronę danych. Jeżeli chodzi o prawo RE, przetwarzanie wszystkich danych osobowych (w tym transgraniczny przepływ danych do innych stron konwencji nr 108), bez ograniczeń co do celu lub obszarów działania, ujęto w konwencji nr 108, przy czym umawiające się strony mogą przewidywać wyjątki od tych zasad. Wszystkie państwa członkowskie EOG są również stronami konwencji nr 108.

7.3. Przekazywanie danych osobowych do państw trzecich/państw niebędących stronami lub organizacji międzynarodowych

Najważniejsze kwestie

- Zarówno **RE**, jak i **UE** dopuszczają przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych pod warunkiem spełnienia określonych warunków ochrony danych osobowych.
    - **Zgodnie z prawem RE** odpowiedni poziom ochrony można osiągnąć za pomocą prawa danego państwa lub organizacji międzynarodowej bądź poprzez wdrożenie odpowiednich standardów.

665 Dyrektywa (UE) 2016/80 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016.

- **Zgodnie z prawem UE** przekazywanie danych jest dopuszczone, gdy państwo trzecie zapewnia odpowiedni poziom ochrony bądź gdy administrator danych lub podmiot przetwarzający ustanowi odpowiednie zabezpieczenia – w tym egzekwowalne prawa osób, których dane dotyczą, i środki ochrony prawnej – za pomocą takich środków, jak standardowe klauzule ochrony danych lub wiążące reguły korporacyjne.

- **Zarówno w prawie RE, jak i w prawie UE** przewidziano odstępstwa dopuszczające przekazywanie danych osobowych w określonych okolicznościach, nawet gdy nie są zapewnione ani odpowiedni poziom ochrony, ani stosowne zabezpieczenia.

Choć i prawo RE, i prawo UE umożliwiają przepływ danych do państw trzecich lub organizacji międzynarodowych, przewidują odmienne warunki w tym zakresie. Każdy ze zbiorów warunków uwzględnia strukturę i cele danej organizacji.

Prawo UE przewiduje co do zasady dwa sposoby umożliwienia przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Przekazanie danych osobowych może opierać się na: decyzji stwierdzającej odpowiedni poziom ochrony wydanej przez Komisję Europejską[666]; lub, w przypadku braku takiej decyzji, na zapewnieniu przez administratora lub podmiot przetwarzający odpowiednich zabezpieczeń, w tym egzekwowalnych praw osób, których dane dotyczą, i środków ochrony prawnej[667]. Gdy brak jest decyzji stwierdzającej odpowiedni poziom ochrony lub odpowiednich zabezpieczeń, można skorzystać z szeregu wyjątków.

Zgodnie z prawem **RE** swobodne przekazywanie danych do państw niebędących stronami konwencji jest jednak możliwe wyłącznie na podstawie:

- prawa danego państwa lub danej organizacji międzynarodowej, w tym stosownych traktatów międzynarodowych lub porozumień gwarantujących odpowiednie zabezpieczenia;

- doraźnych lub zatwierdzonych ustandaryzowanych zabezpieczeń zagwarantowanych prawnie wiążącymi i egzekwowalnymi instrumentami przyjętymi i wdrożonymi przez osoby uczestniczące w przekazywaniu danych i ich dalszym przetwarzaniu[668].

666 Ogólne rozporządzenie o ochronie danych, art. 45.

667 Tamże, art. 46.

668 Zaktualizowana konwencja nr 108, art. 14 ust. 3 lit. a) i b).

Podobnie jak w przypadku prawa UE, gdy brak jest odpowiedniego poziomu ochrony danych, dostępnych jest szereg wyjątków.

7.3.1. Przekazywanie danych na podstawie decyzji stwierdzającej odpowiedni poziom ochrony

Jeżeli chodzi o **prawo UE**, swobodny przepływ danych osobowych do państw trzecich zapewniających odpowiedni poziom ochrony przewidziano w art. 45 RODO. Trybunał Sprawiedliwości Unii Europejskiej wyjaśnił, że aby można było mówić o „odpowiednim stopniu ochrony", państwo trzecie powinno zapewnić taki poziom ochrony praw podstawowych i wolności, który jest „merytorycznie równoważny" poziomowi gwarantowanemu w prawie UE[669]. Jednocześnie środki, z jakich państwo trzecie korzysta dla zapewnienia takiego poziomu ochrony, mogą różnić się od środków wprowadzonych w Unii, a odpowiedni standard ochrony można osiągnąć bez konieczności dokładnego powielenia przepisów unijnych[670].

Komisja Europejska ocenia poziom ochrony danych w państwach trzecich, analizując ich prawo krajowe i stosowne zobowiązania międzynarodowe. Do elementów uwzględnianych przy ocenie należy też udział danego państwa w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych. Jeżeli Komisja Europejska uzna, że dane państwo trzecie lub dana organizacja międzynarodowa zapewnia odpowiedni poziom ochrony, może wydać decyzję o prawidłowości, która to decyzja ma moc wiążącą[671]. Niemniej TSUE stwierdził, że krajowe organy nadzorcze w dalszym ciągu są właściwe do rozpatrywania skarg jednostek odnoszących się do ochrony dotyczących ich danych osobowych, które zostały przeniesione do państwa trzeciego uznanego przez Komisję za zapewniające odpowiedni poziom ochrony, w sytuacji gdy dana osoba podniesie, że prawo i praktyki przyjęte w takim państwie trzecim nie zapewniają odpowiedniego poziomu ochrony[672].

669 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r., pkt 96.

670 Tamże, pkt 74. Zob. także Komisja Europejska (2017), Komunikat Komisji do Parlamentu Europejskiego i Rady „Wymiana i ochrona danych osobowych w zglobalizowanym świecie", COM(2017)7 final z dnia 10 stycznia 2017 r., s. 6.

671 Stale aktualizowana lista krajów, w odniesieniu do których dokonano ustalenia odpowiedniego poziomu ochrony, znajduje się na stronie Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej.

672 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r., pkt 63 i 65–66.

Komisja Europejska może również ocenić poziom ochrony w odniesieniu do określonego terytorium w granicach państwa trzeciego bądź ograniczyć się do konkretnych sektorów, jak miało to miejsce w przypadku prywatnego prawa handlowego Kanady[673]. Wydała także kilka ustaleń odpowiedniego poziomu ochrony odnoszących się do przekazywania danych na podstawie umów między UE a innymi państwami. Decyzje te odnoszą się wyłącznie do jednego rodzaju przekazywania danych, na przykład przekazywania danych dotyczących przelotu pasażera (PNR) przez linie lotnicze zagranicznym organom kontroli granicznej przy lotach z UE na niektóre lotniska zagraniczne (zob. sekcja 7.3.4).

Decyzje stwierdzające odpowiedni poziom ochrony są na bieżąco monitorowane. Komisja Europejska dokonuje regularnego przeglądu takich decyzji z myślą o śledzeniu zmian mogących wpłynąć na ich status. Zatem jeżeli Komisja Europejska stwierdzi, że państwo trzecie bądź organizacja międzynarodowa przestały spełniać warunki uzasadniające wydanie decyzji stwierdzającej odpowiedni poziom ochrony, może uchylić, zmienić lub zawiesić decyzję. Komisja może również podjąć negocjacje z państwem trzecim lub organizacją międzynarodową w celu zaradzenia sytuacji będącej przyczyną decyzji.

Decyzje przyjęte przez Komisję Europejską na mocy dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia decyzją Komisji przyjętą zgodnie z przepisami art. 45 RODO.

Do tej pory Komisja Europejska uznała, że odpowiedni poziom ochrony zapewniają Andora, Argentyna, Guernsey, Izrael, Jersey, Kanada (organizacje handlowe objęte zakresem kanadyjskiej ustawy o ochronie informacji osobowych i dokumentów elektronicznych), Nowa Zelandia, Szwajcaria, Urugwaj, Wyspa Man i Wyspy Owcze. Jeśli chodzi o przekazywanie danych do Stanów Zjednoczonych, w 2000 r. Komisja Europejska przyjęła decyzję w sprawie odpowiedniego poziomu ochrony dopuszczającą przekazywanie danych do spółek, które zadeklarowały, że chronią dane osobowe przenoszone z UE oraz przestrzegają tak zwanych „zasad bezpiecznej

673 Komisja Europejska (2002), Decyzja 2002/2/WE z dnia 20 grudnia 2001 r. na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie odpowiedniej ochrony danych osobowych zapewnionej w ustawie kanadyjskiej o ochronie informacji osobowych i dokumentów elektronicznych, Dz.U. L 2 z 4.1.2002.

przystani"[674]. W 2015 r. TSUE unieważnił tę decyzję, a w lipcu 2016 r. przyjęto nową, umożliwiającą spółkom przystąpienie z dniem 1 sierpnia 2016 r.

Przykład: W sprawie *Schrems*[675] Maximillian Schrems, obywatel Austrii, przez kilka lat był użytkownikiem Facebooka. Dane udostępnione przez M. Schremsa Facebookowi zostały, w całości lub częściowo, przekazane przez irlandzki podmiot zależny spółki Facebook na serwery położone na terytorium Stanów Zjednoczonych, gdzie dane te były przetwarzane. M. Schrems wniósł skargę do irlandzkiego organu ochrony danych, w której podniósł – w świetle informacji ujawnionych przez Edwarda Snowdena na temat działalności amerykańskich służb wywiadowczych – że prawo i praktyka obowiązujące w Stanach Zjednoczonych nie zapewniają wystarczającej ochrony danych przekazywanych do tego kraju. Irlandzki organ odrzucił tę skargę na tej podstawie, że w decyzji z dnia 26 lipca 2000 r. Komisja uznała, że w ramach programu „bezpiecznej przystani" Stany Zjednoczone zapewniają odpowiedni poziom ochrony przekazywanych danych osobowych. Decyzja ta została zaskarżona przed sądem najwyższym (High Court) w Irlandii, który skierował do TSUE wniosek o wydanie w tej sprawie orzeczenia w trybie prejudycjalnym.

Trybunał orzekł, że decyzja Komisji w sprawie odpowiedniego poziomu ochrony zapewnianej w ramach programu „bezpiecznej przystani" jest nieważna. Trybunał zauważył przede wszystkim, że decyzja umożliwiała ograniczenie stosowania zasad ochrony danych w ramach programu „bezpiecznej przystani" ze względów bezpieczeństwa narodowego, interesu publicznego lub przestrzegania prawa bądź na podstawie prawa krajowego USA. Decyzja ta umożliwiała w ten sposób ingerencję w prawa podstawowe osób, których dane osobowe zostały lub mogły zostać przekazane do Stanów Zjednoczonych[676]. Trybunał zauważył ponadto, że decyzja nie zawierała żadnego stwierdzenia dotyczącego istnienia w Stanach Zjednoczonych

674 Decyzja Komisji 2000/520/WE z dnia 26 lipca 2000 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA, Dz.U. L 215 z 25.8.2000,. Trybunał Sprawiedliwości stwierdził nieważność tej decyzji wyrokiem w sprawie C-632/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI].

675 Sprawa C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

676 Tamże, pkt 84.

reguł służących do ograniczenia ewentualnych ingerencji ani skutecznej ochrony prawnej przed ingerencją tego rodzaju[677]. Trybunał podkreślił, że gwarantowany w Unii poziom ochrony podstawowych praw i wolności wymaga, by uregulowania stanowiące ingerencję w prawa gwarantowane w art. 7 i 8 zawierały jasne i dokładne reguły dotyczące zakresu i sposobu stosowania środków, a także wymaga ustanowienia minimalnych zabezpieczeń, odstępstw od ochrony danych osobowych i jej ograniczeń[678]. Zważywszy, że w decyzji Komisji nie stwierdzono, że Stany Zjednoczone rzeczywiście zapewniają odpowiedni poziom ochrony ze względu na swoje prawo krajowe lub zobowiązania międzynarodowe, TSUE uznał, że decyzja ta narusza wymogi stosownych przepisów dyrektywy o ochronie danych dotyczących przekazywania danych oraz że jest w związku z tym nieważna[679].

Poziom ochrony zapewniany w Stanach Zjednoczonych nie był zatem „merytorycznie równoważny" ochronie podstawowych praw i wolności gwarantowanej przez UE[680]. Trybunał stwierdził, że doszło do naruszenia szeregu artykułów Karty praw podstawowych UE. Po pierwsze naruszano zasadniczą istotę art. 7, ponieważ ustawodawstwo Stanów Zjednoczonych pozwalało „władzom publicznym na uzyskanie powszechnego dostępu do treści wiadomości elektronicznych". Po drugie dochodziło też do naruszenia zasadniczej istoty art. 47, ponieważ amerykańskie prawo nie zapewniało jednostkom środków prawnych, które umożliwiałyby dostęp do danych osobowych, ich sprostowanie lub usunięcie. Wreszcie z uwagi na to, że ustalenia dotyczące „bezpiecznej przystani" naruszały powyższe artykuły, dane osobowe nie były przetwarzane zgodnie z prawem, co pociągało za sobą naruszenie art. 8.

Po tym jak TSUE stwierdził nieważność ustaleń dotyczących „bezpiecznej przystani", Komisja i USA uzgodniły nowe ramy, znane jako Tarcza Prywatności UE–USA. W dniu 12 lipca 2016 r. Komisja przyjęła decyzję stwierdzającą, że Stany Zjednoczone

677 Tamże, pkt 88–89.

678 Tamże, pkt 91–92.

679 Tamże, pkt 96–97.

680 Tamże, pkt 73–74 i 96.

zapewniają odpowiedni poziom ochrony danych osobowych przekazywanych z Unii do organizacji w USA w ramach Tarczy Prywatności[681].

Podobnie jak ustalenia dotyczące „bezpiecznej przystani", ramy Tarczy Prywatności UE–USA również mają na celu ochronę danych osobowych przekazywanych z UE do USA do celów handlowych[682]. Amerykańskie spółki mogą dobrowolnie zadeklarować, że zapewniają zgodność z wykazem Tarczy Prywatności, zobowiązując się przestrzegać stosownych norm ochrony danych. Właściwe organy USA monitorują i weryfikują przestrzeganie tych standardów przez certyfikowane spółki.

Program Tarcza Prywatności przewiduje w szczególności:

- nałożenie na spółki otrzymujące dane osobowe z UE obowiązków ochrony danych;

- zapewnienie osobom fizycznym ochrony i środków dochodzenia roszczeń, zwłaszcza ustanowienie mechanizmu rzecznika niezależnego od amerykańskich służb wywiadowczych, który rozpatruje skargi osób na rzekome niezgodne z prawem wykorzystanie ich danych osobowych przez amerykańskie organy w obszarze bezpieczeństwa narodowego;

- przeprowadzenie rocznego wspólnego przeglądu, mającego na celu monitorowanie wdrożenia ram[683]; pierwszy taki przegląd miał miejsce we wrześniu 2017 r.[684].

681 Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, Dz.U. L 207 z 1.8.2016. Grupa Robocza Art. 29 z zadowoleniem przyjęła udoskonalenia, jakie mechanizm Tarczy Prywatności gwarantował w porównaniu z decyzją dotyczącą „bezpiecznej przystani", i wyraziła uznanie dla Komisji i organów USA za uwzględnienie w ostatecznej wersji dokumentów dotyczących Tarczy Prywatności obaw wyrażonych w opinii WP 238 na temat projektu decyzji w sprawie adekwatności ochrony Tarczy Prywatności UE–USA. Zwróciła jednak uwagę na szereg problemów, których w dalszym ciągu nie rozwiązano. Więcej informacji zob. Grupa Robocza Art. 29, *Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, WP 238, 13 kwietnia 2016 r., 16/EN.

682 Więcej informacji zob. EU-U.S. Private Shield factsheet.

683 Więcej informacji zob. strona internetowa Komisji Europejskiej poświęcona Tarczy Prywatności UE–USA.

684 Komisja Europejska, Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie pierwszego rocznego przeglądu funkcjonowania Tarczy Prywatności UE–USA, COM(2017) 611 final, 18 października 2017 r. Zob. także Grupa Robocza Art. 29, *EU-U.S. Privacy Shield – First annual Joint Review*, przyjęty 28 listopada 2017 r., WP 255.

Rząd USA sporządził pisemne zobowiązania i zapewnienia, które towarzyszą decyzji w sprawie Tarczy Prywatności. Zapewniają one ograniczenia i środki ochrony odnoszące się do dostępu rządu USA do danych osobowych ze względów egzekwowania prawa i bezpieczeństwa narodowego.

7.3.2. Przekazywanie z zastrzeżeniem odpowiednich zabezpieczeń

Zarówno **prawo UE**, jak i **prawo RE** uznają odpowiednie zabezpieczenia między administratorem dokonującym przekazania danych i odbiorcą w państwie trzecim lub międzynarodowej organizacji za możliwy sposób zapewnienia wystarczającego poziomu ochrony danych u odbiorcy.

Zgodnie z **prawem UE** przekazywanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej jest dozwolone, jeżeli administrator lub podmiot przetwarzający zapewnią odpowiednie zabezpieczenia i egzekwowalne prawa i jeżeli osoby, których dane dotyczą, mogą skorzystać ze skutecznych środków ochrony prawnej[685]. Środki uznawane za „odpowiednie zabezpieczenia" są wymienione wyłącznie w unijnym prawie o ochronie danych. Odpowiednie zabezpieczenia można zapewnić za pomocą:

- prawnie wiążącego i egzekwowalnego instrumentu między organami lub podmiotami publicznymi;
- wiążących reguł korporacyjnych;
- standardowych klauzul ochrony danych przyjętych przez Komisję Europejską lub organ nadzorczy;
- kodeksów postępowania;
- mechanizmów certyfikacji[686].

Kolejnym środkiem zapewnienia odpowiednich zabezpieczeń są niestandardowe klauzule umowne między administratorem lub podmiotem przetwarzającym dane

685 Ogólne rozporządzenie o ochronie danych, art. 46.

686 Ogólne rozporządzenie o ochronie danych, art. 46 ust. 1 lit. c) i d), art. 46 ust. 2 lit. a), b), e) i f) oraz art. 47.

w UE a odbiorcą danych w państwie trzecim. Zanim jednak takie klauzule umowne będą mogły posłużyć jako narzędzie umożliwiające przekazanie danych osobowych, wymagają zezwolenia właściwego organu nadzorczego. Podobnie organy publiczne mogą skorzystać z postanowień uzgodnień administracyjnych dotyczących ochrony danych – o ile organ nadzorczy je zatwierdzi[687].

Zgodnie z prawem RE przepływ danych do państwa lub organizacji międzynarodowej niebędącej stroną zaktualizowanej konwencji nr 108 jest dopuszczony pod warunkiem zapewnienia odpowiedniego poziomu ochrony. Można to osiągnąć za pomocą:

- prawa danego państwa bądź danej organizacji międzynarodowej; lub
- doraźnych lub ustandaryzowanych zabezpieczeń zapisanych w prawnie wiążącym dokumencie[688].

Przekazywanie z zastrzeżeniem klauzul umownych

Zarówno w **prawie RE**, jak i w **prawie UE** uznano klauzule umowne między administratorem dokonującym przekazania danych i odbiorcą w państwie trzecim za możliwy sposób zapewnienia wystarczającego poziomu ochrony danych u odbiorcy[689].

Na szczeblu UE Komisja Europejska z pomocą Grupy Roboczej Art. 29 wypracowała standardowe klauzule ochrony danych, które zostały oficjalnie uznane decyzją Komisji za dowód odpowiedniej ochrony danych[690]. Jako że decyzje Komisji są w całości wiążące w państwach członkowskich, organy krajowe odpowiedzialne za nadzorowanie przekazywania danych muszą uwzględnić te standardowe klauzule umowne w swoich procedurach[691]. Tak więc jeżeli administrator dokonujący przekazania danych oraz odbiorca z państwa trzeciego uzgodnią i podpiszą takie klauzule, powinny one wystarczyć organowi nadzorczemu za dowód, że wdrożono odpowiednie zabezpieczenia. W sprawie *Schrems* TSUE uznał jednak, że Komisja Europejska nie jest uprawniona do ograniczenia kompetencji krajowych organów nadzorczych w kwestii nadzoru nad przekazywaniem danych osobowych do państwa

687 Tamże, art. 46 ust. 3.

688 Zaktualizowana konwencja nr 108, art. 14 ust. 3 lit. b).

689 Ogólne rozporządzenie o ochronie danych, art. 46 ust. 3; zaktualizowana konwencja nr 108, art. 14 ust. 3 lit. b).

690 Tamże, art. 46 ust. 2 lit. b) i art. 46 ust. 5.

691 Tamże, art. 46 ust. 2 lit. c);Traktat o funkcjonowaniu Unii Europejskiej, art. 288.

trzeciego będącego przedmiotem decyzji Komisji stwierdzającej odpowiedni poziom ochrony[692]. Nic nie stoi zatem na przeszkodzie wykonywaniu przez krajowe organy nadzorcze ich kompetencji, w tym uprawnień do zawieszenia lub zakazania przekazania danych osobowych w przypadku gdy przekazywanie odbywa się z naruszeniem unijnego lub krajowego prawa o ochronie danych, na przykład gdy podmiot odbierający dane nie przestrzega standardowych klauzul umownych[693].

Istnienie standardowych klauzul umownych w ramach prawnych UE nie uniemożliwia administratorom sformułowania innych doraźnych, indywidualnych klauzul umownych, pod warunkiem że organ nadzorczy wyrazi na nie zgodę[694]. Muszą jednak zapewniać taki sam poziom ochrony, jaki przewidziano w standardowych klauzulach umownych. Przy zatwierdzaniu doraźnych klauzul organy nadzorcze są obowiązane stosować mechanizm spójności, aby zapewnić spójność regulacji w całej UE[695]. Oznacza to, że właściwy organ nadzorczy musi zgłosić projekt decyzji dotyczącej klauzul Europejskiej Radzie Ochrony Danych. Europejska Rada Ochrony Danych wyda opinię w tej kwestii, a organ nadzorczy musi w jak największym stopniu tę opinię uwzględnić przy wydawaniu decyzji. Jeżeli nie zamierza zastosować się do opinii Europejskiej Rady Ochrony Danych, zostanie uruchomiony mechanizm rozstrzygania sporów przez Europejską Radę Ochrony Danych i wyda ona wiążącą decyzję[696].

Najważniejszymi cechami standardowych klauzul umownych są:

- klauzula beneficjenta będącego stroną trzecią, która umożliwia osobom, których dane dotyczą, wykonywanie praw na podstawie umowy, mimo że nie są jej stroną;

692 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r., pkt 96–98 i 102–105.

693 Aby uwzględnić stanowisko TSUE wyrażone w sprawie *Schrems*, Komisja zmieniła decyzję w sprawie standardowych klauzul umownych. Decyzja wykonawcza Komisji (UE) 2016/2297 z dnia 16 grudnia 2016 r. zmieniająca decyzje 2001/497/WE i 2010/87/UE w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych państwom trzecim oraz podmiotom przetwarzającym dane mającym siedzibę w takich państwach, na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.U. L 344 z 17.12.2016.

694 Ogólne rozporządzenie o ochronie danych, art. 46 ust. 3 lit. a).

695 Tamże, art. 63 i art. 64 ust. 1 lit. e).

696 Tamże, art. 64 i art. 65.

- zgoda odbiorcy lub podmiotu odbierającego dane na poddanie się decyzji krajowego organu nadzorczego administratora przekazującego dane lub tamtejszych sądów w przypadku sporu.

Dostępne są obecnie dwa zestawy standardowych klauzul w przypadku przekazywania danych między administratorami, spośród których administrator przekazujący dane może dokonać wyboru[697]. W przypadku przekazywania danych między administratorami a podmiotami przetwarzającymi obowiązuje tylko jeden zestaw standardowych klauzul umownych[698]. Standardowe klauzule umowne są jednak obecnie przedmiotem postępowania sądowego.

Przykład: Po stwierdzeniu przez TSUE nieważności decyzji dotyczącej „bezpiecznej przystani"[699] przekazywanie danych osobowych do Stanów Zjednoczonych nie mogło już odbywać się na podstawie tej decyzji. W oczekiwaniu na zakończenie negocjacji z organami USA i przyjęcie nowej decyzji w sprawie adekwatności ochrony (którą ostatecznie przyjęto dnia 12 lipca 2016 r.) przekazywanie mogło się odbywać wyłącznie w oparciu o inne podstawy prawne, na przykład standardowe klauzule umowne lub wiążące reguły korporacyjne[700]. Szereg spółek, w tym Facebook Ireland (przeciwko której wszczęto sprawę, która doprowadziła do unieważnienia decyzji dotyczącej „bezpiecznej przystani"), zaczęło korzystać ze standardowych klauzul umownych, by móc w dalszym ciągu przekazywać dane z UE do USA.

697 Zestaw I zawarto w załączniku do: Komisja Europejska (2001), Decyzja Komisji 2001/497/WE z dnia 15 czerwca 2001 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, na mocy dyrektywy 95/46/WE, Dz.U. L 181 z 4.7.2001; zestaw II zawarto w załączniku do: Komisja Europejska (2004), Decyzja Komisji 2004/915/WE z dnia 27 grudnia 2004 r. zmieniająca decyzję 2001/497/WE w zakresie wprowadzenia alternatywnego zestawu standardowych klauzul umownych dotyczących przekazywania danych osobowych do państw trzecich, Dz.U. L 385 z 29.12.2004.

698 Komisja Europejska (2010), Decyzja Komisji 2010/87 z dnia 5 lutego 2010 r. w sprawie standardowych klauzul umownych dotyczących przekazywania danych osobowych podmiotom przetwarzającym dane mającym siedzibę w krajach trzecich na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, Dz.U. L 39 z 12.2.2010. W czasie gdy opracowywano niniejszy podręcznik, korzystanie ze standardowych klauzul umownych jako podstawy przekazywania danych osobowych do Stanów Zjednoczonych było przedmiotem postępowania toczącego się przez sądem najwyższym w Irlandii.

699 TSUE, C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.

700 Decyzja wykonawcza Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r. przyjęta na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA, Dz.U. L 207 z 1.8.2016.

M. Schrems przedłożył skargę do irlandzkiego organu nadzorczego, w której zażądał zawieszenia przekazywania danych do Stanów Zjednoczonych na podstawie standardowych klauzul umownych. Zasadniczo twierdził on, że gdy jego dane osobowe są przekazywanie przez podmiot zależny Facebooka w Irlandii do spółki Facebook Inc. oraz na inne serwery zlokalizowane na terytorium Stanów Zjednoczonych, nie jest możliwe zagwarantowanie ochrony tych danych. Spółka Facebook Inc. podlega amerykańskim przepisom, które mogą nakładać na nią obowiązek ujawnienia danych osobowych amerykańskim organom ścigania, i nie jest dostępny sądowy środek ochrony prawnej, z którego osoby fizyczne z Europy mogłyby skorzystać, by tę praktykę zaskarżyć[701]. Z tego względu TSUE stwierdził nieważność decyzji dotyczącej „bezpiecznej przystani" – i choć orzeczenie Trybunału ograniczało się do zbadania tej decyzji, skarżący uznał, że podniesione kwestie w równej mierze dotyczą przekazywania danych na podstawie klauzul umownych. W czasie opracowywania niniejszego podręcznika sprawa była rozpatrywana przez sąd najwyższy w Irlandii. Skarżący najwyraźniej zamierza skierować sprawę do TSUE w celu zakwestionowania ważności decyzji Komisji Europejskiej w sprawie standardowych klauzul umownych. Jak opisano w rozdziale 5, wyłącznie TSUE może stwierdzić nieważność instrumentu UE.

Przekazywanie z zastrzeżeniem wiążących reguł korporacyjnych

Prawo UE dopuszcza ponadto przekazywanie danych osobowych na podstawie wiążących reguł korporacyjnych w przypadku międzynarodowego przekazywania danych w obrębie tej samej grupy przedsiębiorstw lub przedsiębiorców, jeżeli stanowi to element wspólnej działalności gospodarczej[702]. Zanim wiążące reguły korporacyjne będą mogły posłużyć jako narzędzie do przekazywania danych osobowych, właściwy organ nadzorczy musi je zatwierdzić zgodnie z wiążącymi regułami korporacyjnymi, za pomocą mechanizmu spójności.

Aby wiążące reguły korporacyjne mogły zostać zatwierdzone, muszą być prawnie wiążące, obejmować wszystkie podstawowe zasady ochrony danych, mieć zastosowanie do każdego z członków grupy i być przez każdego z nich egzekwowane. Muszą wyraźnie przyznawać osobom, których dane dotyczą, egzekwowalne prawa,

701 Więcej informacji zob. zmieniona skarga irlandzkiego Data Protection Commissioner przeciwko spółce Facebook Ireland Ltd. i Maximillianowi Schremsowi z dnia 1 grudnia 2015 r.

702 Ogólne rozporządzenie o ochronie danych, art. 47.

obejmować wszystkie podstawowe zasady ochrony danych i spełniać określone wymogi formalne, takie jak określenie struktury przedsiębiorstwa, opisanie przekazywania danych i sposobu stosowania zasad ochrony danych. Obowiązek ten obejmuje przekazywanie takich informacji osobom, których dane dotyczą. Wiążące reguły korporacyjne muszą określać między innymi prawa osób, których dane dotyczą, i postanowienia dotyczące odpowiedzialności za wszelkie przypadki naruszenia reguł[703]. Przy zatwierdzaniu wiążących reguł korporacyjnych będzie uruchamiany mechanizm spójności na potrzeby współpracy organów nadzorczych (opisany w rozdziale 5).

W ramach mechanizmu spójności wiodący organ nadzorczy dokonuje przeglądu proponowanych wiążących reguł korporacyjnych, przyjmuje projekt decyzji i zgłasza go Europejskiej Radzie Ochrony Danych. Europejska Rada Ochrony Danych wydaje opinię w tej kwestii, a wiodący organ nadzorczy może formalnie zatwierdzić wiążące reguły korporacyjne, „w jak największym stopniu" uwzględniając tę opinię. Opinia ta nie jest wprawdzie prawnie wiążąca, ale jeżeli organ nadzorczy nie zamierza jej uwzględnić, wówczas uruchamiany jest mechanizm rozstrzygania sporów, a Europejska Rada Ochrony Danych zostaje wezwana do przyjęcia prawnie wiążącej decyzji większością dwóch trzecich głosów swoich członków[704].

Zgodnie z **prawem RE** do doraźnych lub ustandaryzowanych zabezpieczeń zapisanych w prawnie wiążącym dokumencie[705] należą również wiążące reguły korporacyjne.

7.3.3. Wyjątki w szczególnych sytuacjach

Zgodnie z prawem UE przekazywanie danych osobowych do państwa trzeciego może być uzasadnione nawet w przypadku braku odpowiedniej decyzji lub zabezpieczeń, takich jak standardowe klauzule umowne lub wiążące reguły korporacyjne, jeżeli zaistnieją poniższe okoliczności:

- osoba, której danej dotyczą, wyraźnie wyraziła zgodę na przekazanie danych;
- osoba, której dane dotyczą, nawiąże – bądź zamierza nawiązać – stosunek umowny, do którego jest niezbędne przekazanie danych za granicę;

703 Bardziej szczegółowy opis zob. ogólne rozporządzenie o ochronie danych, art. 47.

704 Tamże, art. 57 ust. 1 lit. s), art. 58 ust. 1 lit. j), art. 64 ust. 1 lit. f) oraz art. 65 ust. 1 i 2.

705 Zaktualizowana konwencja nr 108, art. 12 ust. 3 lit. b).

- w celu zawarcia umowy między administratorem danych a osobą trzecią w interesie osoby, której dane dotyczą;
- z uwagi na względy interesu publicznego;
- w celu ustalenia, dochodzenia lub ochrony roszczeń;
- w celu ochrony żywotnych interesów osoby, której dane dotyczą;
- w celu przekazania danych z rejestrów publicznych (to przykład nadrzędnego interesu publicznego w dostępie do informacji przechowywanych w rejestrach publicznych)[706].

Jeżeli żaden z powyższych warunków nie ma zastosowania i gdy przekazywanie danych nie może się odbywać na podstawie decyzji stwierdzającej odpowiedni poziom ochrony ani odpowiednich zabezpieczeń, przekazanie danych może nastąpić wyłącznie wówczas, gdy nie jest powtarzalne, dotyczy ograniczonej liczby osób, których dane dotyczą, jest niezbędne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, wobec których charakteru nadrzędnego nie mają interesy ani prawa osoby, której dane dotyczą[707]. W takich sytuacjach administrator musi ocenić okoliczności przekazania danych i zapewnić odpowiednie zabezpieczenia. Administrator musi ponadto poinformować organ nadzorczy i osoby, których dane dotyczą, zarówno o przekazaniu, jak i o prawnie uzasadnionych interesach leżących u jego podstawy.

Fakt, że odstępstwa umożliwiają zgodne z prawem przekazanie danych tylko w ostateczności[708] (można z nich skorzystać wyłącznie jeżeli brak jest decyzji stwierdzającej odpowiedni poziom ochrony i nie są zapewnione żadne inne zabezpieczenia), uwydatnia ich wyjątkowy charakter, który został dodatkowo podkreślony w motywach RODO[709]. W związku z powyższym odstępstwa dopuszcza się w przypadku „przekazywania w niektórych okolicznościach" na podstawie zgody i „jeżeli przekazywanie jest sporadyczne i niezbędne"[710] w związku z umową lub roszczeniem.

706 Ogólne rozporządzenie o ochronie danych, art. 49.

707 Tamże.

708 Tamże, art. 49 ust. 1.

709 Zob. ogólne rozporządzenie o ochronie danych, art. 49 ust. 1 lit. a), b) i e) oraz motyw 113.

710 Tamże, art. 49 ust. 1.

Ponadto zgodnie z wytycznymi Grupy Roboczej Art. 29 na odstępstwach odnoszących się do określonych sytuacji można się opierać wyłącznie w wyjątkowych, rozpatrywanych w każdym przypadku indywidualnie okolicznościach, i nie można z nich korzystać na potrzeby masowego bądź powtarzającego się przekazywania danych[711]. Europejski Inspektor Ochrony danych podkreślił ponadto nadzwyczajny charakter wyjątków stanowiących podstawę prawną przekazywania danych na mocy rozporządzenia (WE) nr 45/2001 i zauważył, że po takie rozwiązanie powinno się sięgać „w ograniczonej liczbie przypadków" i „sporadycznie"[712].

Przykład: Spółka świadcząca usługi globalnego systemu dystrybucji (GDS), mająca siedzibę w Stanach Zjednoczonych, jest dostawcą internetowego systemu rezerwacji na potrzeby wielu linii lotniczych, hoteli i statków na całym świecie, w ramach którego to systemu przetwarza dane dziesiątek milionów osób w UE. Aby pierwotnie przekazać dane na swoje serwery w Stanach Zjednoczonych, spółka działa na podstawie odstępstwa, w myśl którego można zgodnie z prawem przekazać dane, jeżeli jest to niezbędne do zawarcia umowy. Spółka nie zapewnia zatem żadnych innych zabezpieczeń w odniesieniu do danych osobowych pochodzących z Europy, które są przekazywane do USA, a następnie rozpowszechniane dalej wśród hoteli na całym świecie (co oznacza brak zabezpieczeń również w odniesieniu do dalszego przekazywania). Spółka ta nie przestrzega wymogów RODO dotyczących zgodnego z prawem międzynarodowego przekazywania danych, ponieważ wykorzystuje odstępstwa jako podstawę przekazywania danych na masową skalę.

O ile nie obowiązuje decyzja stwierdzająca odpowiedni poziom ochrony, UE lub jej państwa członkowskie są uprawnione do ograniczania przekazywania określonych kategorii danych osobowych do państwa trzeciego – pomimo spełnienia innych warunków takiego przekazania – ze względu na interes publiczny. Ograniczenia te należy uznawać za nadzwyczajne, a państwa członkowskie muszą poinformować o odpowiednich postanowieniach Komisję[713].

711 Grupa Robocza Art. 29 (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, Bruksela, 25 listopada 2005 r.

712 Europejski Inspektor Ochrony Danych, *The transfer of personal data to third countries and international organisations by EU institutions and bodies*, stanowisko, Bruksela, 14 lipca 2014 r., s. 15.

713 Zob. ogólne rozporządzenie o ochronie danych, art. 49 ust. 5.

Prawo RE dopuszcza przepływ danych na terytoria, na których nie zapewnia się odpowiedniego poziomu ochrony, w przypadkach gdy:

- osoba, której dane dotyczą, wyraziła na to zgodę;
- interes osoby, której dane dotyczą, wymaga takiego przekazania;
- istnieją nadrzędne, prawnie uzasadnione interesy – zwłaszcza ważny interes publiczny – przewidziane w prawie;
- stanowi to konieczny i proporcjonalny środek w społeczeństwie demokratycznym[714].

7.3.4. Przekazywanie na podstawie umów międzynarodowych

Unia Europejska może zawierać z państwami trzecimi umowy międzynarodowe regulujące przekazywanie danych osobowych do określonych celów. Takie umowy muszą obejmować stosowne zabezpieczenia zapewniające ochronę danych osobowych osób, których dotyczą. Rozporządzenie pozostaje bez uszczerbku dla tych umów międzynarodowych[715].

Państwa członkowskie mogą też zawierać umowy międzynarodowe z państwami trzecimi lub organizacjami międzynarodowymi, zapewniające odpowiedni poziom ochrony podstawowych praw i wolności jednostek, o ile takie umowy pozostają bez wpływu na stosowanie RODO.

Podobną zasadę przewidziano w art. 12 ust. 3 lit. a) zaktualizowanej konwencji nr 108.

Do umów międzynarodowych dotyczących przekazywania danych osobowych należą umowy w sprawie danych dotyczących przelotu pasażera (PNR).

Dane dotyczące przelotu pasażera

Dane PNR są gromadzone przez przewoźników lotniczych podczas procesu rezerwacyjnego i obejmują nazwiska, adresy, dane kart kredytowych oraz numery

714 Zaktualizowana konwencja nr 108, art. 14 ust. 4.

715 Ogólne rozporządzenie o ochronie danych, motyw 102.

miejsc pasażerów. Przewoźnicy lotniczy zbierają te dane również do własnych celów handlowych. Unia Europejska zawarła z określonymi państwami trzecimi (Australią, Kanadą i Stanami Zjednoczonymi) umowy w sprawie przekazywania danych PNR z myślą o zapobieganiu przestępstwom terrorystycznym i poważnej przestępczości transgranicznej, ich wykrywaniu, prowadzeniu postępowań przygotowawczych w ich sprawie i ich ściganiu. Ponadto w 2016 r. Unia przyjęła dyrektywę (UE) 2016/861, znaną jako dyrektywa UE PNR[716]. Dyrektywa zapewnia ramy prawne umożliwiające państwom członkowskim UE przekazywanie danych PNR właściwym organom w innych państwach trzecich, również z myślą o zapobieganiu przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywaniu, prowadzeniu postępowań przygotowawczych w ich sprawie i ich ściganiu. Przekazywanie danych PNR do organów państw trzecich odbywa się na podstawie oceny każdego przypadku oraz indywidualnej weryfikacji, czy przekazanie jest niezbędne do celów określonych w dyrektywie, a także z zastrzeżeniem poszanowania praw podstawowych.

Co się tyczy umów w sprawie danych PNR między UE a państwami trzecimi, zakwestionowano ich zgodność z podstawowymi prawami do prywatności i ochrony danych, zapisanymi w Karcie praw podstawowych UE. Kiedy w 2014 r. – w następstwie negocjacji z Kanadą – UE podpisała umowę o przekazywaniu i przetwarzaniu danych PNR, Parlament Europejski postanowił skierować sprawę do TSUE, by ten ocenił zgodność umowy z prawem UE, zwłaszcza z art. 7 i 8 karty.

Przykład: W opinii dotyczącej zgodności z prawem umowy PNR między UE a Kanadą[717] TSUE uznał, że w ówczesnej postaci przedmiotowa umowa była niezgodna z prawami podstawowymi uznanymi w karcie, a co za tym idzie – że nie mogła zostać zawarta. Ze względu na to, że obejmowała przetwarzanie danych osobowych, stanowiła ingerencję w prawo do ochrony danych osobowych, chronione na mocy art. 8 karty. Jednocześnie powodowała ograniczenie prawa do poszanowania życia prywatnego, zapisanego w art. 7, ponieważ dane PNR w ujęciu całościowym mogą być agregowane i analizowane w sposób umożliwiający poznanie nawyków turystycznych, związków pomiędzy poszczególnymi osobami, informacji o ich sytuacji finansowej, zwyczajów żywieniowych i sytuacji zdrowotnej, co jest równoznaczne z ingerencją w ich życie prywatne.

716 Dyrektywa (UE) 2016/681 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119 z 4.5.2016.

717 TSUE, *Opinia 1/15 Trybunału* [WI], 26 lipca 2017 r.

Ingerencja w prawa podstawowe, które ta umowa za sobą pociągała, miała za cel realizację interesu ogólnego, tj. bezpieczeństwo publiczne i walkę z terroryzmem i poważną przestępczością. Trybunał przypomniał jednak, że aby ingerencja była uzasadniona, musi ograniczać się do tego, co jest absolutnie konieczne do osiągnięcia założonego celu. Po przeanalizowaniu zapisów umowy TSUE stwierdził, że nie spełniała ona tego kryterium. Do czynników, które TSUE wziął pod uwagę, dochodząc do tego wniosku, należały:

- Fakt, że przedmiotowa umowa obejmowała przekazywanie danych szczególnie chronionych. Dane PNR zbierane na mocy rzeczonej umowy mogły obejmować dane szczególnie chronione, na przykład takie, które informowały o pochodzeniu rasowym bądź etnicznym, religii lub stanie zdrowia pasażera. Przekazywanie i przetwarzanie danych szczególnie chronionych przez kanadyjskie organy mogło zagrażać zasadzie niedyskryminacji i z tego względu wymagało szczegółowego i silnego uzasadnienia, opartego na innych względach niż bezpieczeństwo publiczne i walka z poważną przestępczością. Przedmiotowa umowa takiego uzasadnienia nie zapewniała[718].

- Przechowywanie danych PNR wszystkich pasażerów przez pięć lat, nawet po opuszczeniu przez nich kraju, również uznano za wykraczające poza granice absolutnej konieczności. Trybunał uznał, że można by dopuścić przechowywanie przez kanadyjskie organy danych pasażerów, co do których istnieją obiektywne dowody sugerujące, że mogą oni stanowić zagrożenie dla bezpieczeństwa publicznego, nawet po opuszczeniu przez nich kraju. Natomiast przechowywanie danych *wszystkich* pasażerów, w przypadku których nie istnieją nawet pośrednie dowody świadczące o stwarzaniu zagrożenia dla bezpieczeństwa publicznego, nie ma uzasadnienia[719].

Komitet Konsultacyjny ds. Konwencji nr 108 przedstawił opinię na temat skutków dla ochrony danych umów dotyczących PNR w świetle prawa RE[720].

718 Tamże, pkt 165.

719 Tamże, pkt 204–207.

720 Rada Europy, *Opinion on the Data protection implications of the processing of Passenger Name Records*, T-PD(2016)18rev, 19 sierpnia 2016 r.

Dane z komunikatów

Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (ang. Society for Worldwide Interbank Financial Telecommunication, SWIFT) z siedzibą w Belgii, które przetwarza większość globalnych przelewów środków z banków europejskich, prowadziło działania w bliźniaczym ośrodku w Stanach Zjednoczonych i Departament Skarbu USA zażądał od niego ujawnienia danych na potrzeby dochodzeń w sprawie terroryzmu w ramach Programu śledzenia środków finansowych należących do terrorystów (TFTP)[721].

Z punktu widzenia UE nie było wystarczających podstaw prawnych ujawnienia tych danych – dotyczących głównie obywateli UE – Stanom Zjednoczonym wyłącznie dlatego, że znajdował się tam jeden z ośrodków przetwarzania danych SWIFT.

W 2010 r. zawarto specjalną umowę między UE a Stanami Zjednoczonymi, znaną jako umowa SWIFT, aby zapewnić niezbędną podstawę prawną i odpowiedni poziom ochrony danych[722].

Na mocy tej umowy dane finansowe przechowywane przez SWIFT są nadal udostępniane Departamentowi Skarbu USA w celu zapobiegania terroryzmowi, prowadzenia dochodzeń w sprawie terroryzmu, wykrywania bądź ścigania terroryzmu lub jego finansowania. Departament Skarbu USA może zwrócić się o dane finansowe SWIFT pod warunkiem, że wniosek:

- określa dane finansowe jak najwyraźniej;
- wyraźnie uzasadnia konieczność otrzymania danych;

721 W tym kontekście zob. Grupa Robocza Art. 29 (2011), *Opinia 14/2011 dotycząca kwestii ochrony danych w odniesieniu do zapobiegania zjawiskom prania pieniędzy i finansowania terroryzmu*, WP 186, Bruksela, 13 czerwca 2011 r.; Grupa Robocza Art. 29 (2006), *Opinia 10/2006 w sprawie przetwarzania danych osobowych przez Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (Society for Worldwide Interbank Financial Telecommunication, SWIFT)*, WP 128, Bruksela, 22 listopada 2006 r.; Commission de la protection de la vie privée (belgijska komisja ds. ochrony prywatności) (2008), Control and recommendation procedure initiated with respect to the company SWIFT scrl, decyzja, 9 grudnia 2008 r.

722 Decyzja Rady 2010/412/UE z dnia 13 lipca 2010 r. w sprawie zawarcia Umowy między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu z Unii Europejskiej do Stanów Zjednoczonych danych z komunikatów finansowych do celów Programu śledzenia środków finansowych należących do terrorystów, Dz.U. L 195 z 27.7.2010, s. 3 i 4. Tekst umowy dołączono do decyzji, Dz.U. L 195 z 27.7.2010, s. 5–14.

- jest jak najbardziej zawężony w taki sposób, by dotyczył jak najmniejszej ilości danych;

- nie dotyczy żadnych danych odnoszących się do Jednolitego Europejskiego Obszaru Płatniczego (SEPA)[723].

Europol musi otrzymać kopię każdego wniosku skierowanego przez Departament Skarbu USA i zweryfikować, czy zasady umowy SWIFT są przestrzegane[724]. Jeżeli zostanie potwierdzone, że są one przestrzegane, SWIFT ma obowiązek dostarczyć dane finansowe bezpośrednio Departamentowi Skarbu USA. Departament ma obowiązek zabezpieczyć dane finansowe środkami ochrony fizycznej i udostępnić je wyłącznie analitykom badającym terroryzm lub jego finansowanie, a dane finansowe nie mogą być łączone z żadną inną bazą danych. Co do zasady dane finansowe otrzymane od SWIFT muszą zostać usunięte nie później niż pięć lat po ich otrzymaniu. Dane finansowe, które są istotne dla konkretnych dochodzeń lub operacji ścigania, mogą być zatrzymywane nie dłużej, niż jest to konieczne do celów tych dochodzeń lub operacji ścigania.

Departament Skarbu USA może przekazać informacje pochodzące z danych otrzymanych od SWIFT konkretnym organom ścigania, organom odpowiedzialnym za zapewnienie bezpieczeństwa publicznego lub zwalczanie terroryzmu na terenie Stanów Zjednoczonych bądź poza nimi wyłącznie do celów zapobiegania terroryzmowi, dochodzeń w sprawie terroryzmu, wykrywania bądź ścigania terroryzmu lub jego finansowania. W przypadku gdy dalsze przekazanie danych finansowych dotyczy obywatela lub rezydenta państwa członkowskiego UE, każde udostępnienie danych organom państwa trzeciego jest uzależnione od uprzedniej zgody właściwych organów danego państwa członkowskiego. Wyjątki można uczynić w przypadkach, w których udostępnienie danych ma istotne znaczenie dla zapobieżenia nagłemu i poważnemu zagrożeniu bezpieczeństwa publicznego.

Przestrzeganie zasad umowy SWIFT monitorują niezależni obserwatorzy, w tym osoba wyznaczona przez Komisję Europejską. Są oni uprawnieni do przeprowadzania w czasie rzeczywistym i retrospektywnie przeglądu wszystkich wyszukiwań dostarczanych danych, do złożenia wniosku o dodatkowe informacje w celu uzasadnienia związku tych wyszukań z terroryzmem, jak również do blokowania każdego

723 Tamże, art. 4 ust. 2.

724 Wspólny Organ Nadzorczy Europolu przeprowadza kontrole działań Europolu w tym obszarze.

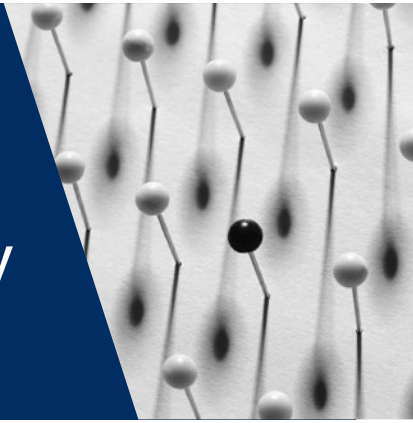
lub wszystkich wyszukiwań, które okażą się naruszać zabezpieczenia przewidziane w umowie.

Osoby, których dane dotyczą, mają prawo uzyskać od właściwego urzędu ochrony danych w UE potwierdzenie, że ich prawa do ochrony danych osobowych są przestrzegane. Osoby, których dane dotyczą, mają również prawo do sprostowania, usunięcia lub zablokowania swoich danych gromadzonych i przechowywanych przez Departament Skarbu USA na mocy umowy SWIFT. Prawa dostępu osób, których dane dotyczą, mogą jednak podlegać pewnym ograniczeniom prawnym. W przypadku odmowy dostępu osoba, której dane dotyczą, musi zostać poinformowana w formie pisemnej o odmowie oraz przysługującym jej prawie do administracyjnych i sądowych środków zaskarżenia w Stanach Zjednoczonych.

Umowa SWIFT obowiązuje przez pięć lat, pierwszy okres jej obowiązywania upłynął w sierpniu 2015 r. Jej okres obowiązywania będzie automatycznie przedłużany na kolejne okresy roczne, chyba że jedna ze stron zawiadomi drugą z przynajmniej sześciomiesięcznym wyprzedzeniem, że nie zamierza przedłużyć okresu obowiązywania umowy. Umowę automatycznie przedłużono w sierpniu 2015, 2016 i 2017 r., co zapewnia obowiązywanie umowy SWIFT co najmniej do sierpnia 2018 r.[725].

725 Tamże, art. 23 ust. 2.

8 Ochrona danych w kontekście współpracy policyjnej i sądowej w sprawach karnych



UE	Omówione zagadnienia	RE
Dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości	**Ogólne**	Zaktualizowana konwencja nr 108
	Policja	Rekomendacja dotycząca policji Praktyczny przewodnik dotyczący wykorzystywania danych osobowych w sektorze policji
	Nadzór	ETPC, *B.B. przeciwko Francji*, nr 5335/06, 2009 r. ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 2008 ETPC, *Allan przeciwko Zjednoczonemu Królestwu*, nr 48539/99, 2002 r. ETPC, *Malone przeciwko Zjednoczonemu Królestwu*, nr 8691/79, 1984 r. ETPC, *Klass i in. przeciwko Niemcom*, nr 5029/71, 1978 r. ETPC, *Szabó i Vissy przeciwko Węgrom*, nr 37138/14, 2016 r. ETPC, *Vetter przeciwko Francji*, nr 59842/00, 2005 r.
	Cyberprzestępczość	Konwencja o cyberprzestępczości

UE	Omówione zagadnienia	RE
Inne szczegółowe akty prawne		
Decyzja w sprawie konwencji z Prüm	**W odniesieniu do danych szczególnych: odciski palców, DNA, chuligaństwo, informacje o pasażerach linii lotniczych, dane telekomunikacyjne itp.**	Artykuł 6 zaktualizowanej konwencji nr 108 Rekomendacja dotycząca policji, Praktyczny przewodnik dotyczący wykorzystywania danych osobowych w sektorze policji
Inicjatywa szwedzka (decyzja ramowa Rady 2006/960/WSiSW)	**Uproszczenie wymiany informacji i danych wywiadowczych między organami ścigania**	ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], nr 30562/04 i 30566/04, 2008
Dyrektywa (UE) 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd oraz Kärntner Landesregierung i in.* [WI], 2014 TSUE, sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige* oraz *Home Department przeciwko Tomowi Watsonowi i in.* [WI], 2016	**Zatrzymywanie danych osobowych**	ETPC, *B.B. przeciwko Francji*, nr 5335/06, 2009 r.
Rozporządzenie w sprawie Europolu Decyzja w sprawie Eurojustu	**Przez agencje specjalne**	Rekomendacja dotycząca policji
Decyzja w sprawie Schengen II Rozporządzenie w sprawie VIS Rozporządzenie Eurodac Decyzja w sprawie CIS	**Przez specjalne wspólne systemy informacji**	Rekomendacja dotycząca policji ETPC, *Dalea przeciwko Francji*, nr 964/07, 2010 r.

W celu wyważenia interesów jednostki w zakresie ochrony danych oraz interesów społeczeństwa w zakresie gromadzenia danych w celu walki z przestępczością, jak też zapewnienia bezpieczeństwa narodowego i publicznego, RE oraz UE uchwaliły konkretne akty prawne. W niniejszej sekcji omówiono prawo RE (sekcja 8.1) i UE (sekcja 8.2) dotyczące ochrony danych w kontekście współpracy policyjnej i sądowej w sprawach karnych.

8.1. Prawo RE o ochronie danych w kontekście bezpieczeństwa narodowego oraz współpracy policyjnej i sądowej w sprawach karnych

Najważniejsze kwestie

- Zaktualizowana konwencja nr 108 i rekomendacja RE dotycząca policji dotyczą ochrony danych we wszystkich obszarach pracy policyjnej.
- Konwencja o cyberprzestępczości (konwencja budapeszteńska) jest wiążącym międzynarodowym aktem prawnym dotyczącym przestępstw popełnianych przeciwko sieciom elektronicznym oraz z ich wykorzystaniem. Odnosi się ona również do prowadzenia dochodzeń w sprawie innych przestępstw, w których to dochodzeniach wykorzystywane są dowody elektroniczne.

Istotną różnicą między prawem RE i UE jest to, że **prawo RE**, w przeciwieństwie do przepisów unijnych, odnosi się również do bezpieczeństwa narodowego. Oznacza to, że umawiające się strony muszą przestrzegać zapisów art. 8 EKPC nawet w przypadku działań związanych z bezpieczeństwem narodowym. Europejski Trybunał Praw Człowieka wydał kilka wyroków dotyczących działań państw w tych wrażliwych obszarach, jakimi są przepisy i praktyka w zakresie bezpieczeństwa narodowego[726].

Jeśli chodzi o współpracę policyjną i sądową w sprawach karnych, na szczeblu europejskim zaktualizowana konwencja nr 108 obejmuje wszystkie dziedziny przetwarzania danych osobowych, a jej postanowienia mają w zamierzeniu regulować

726 Zob. na przykład ETPC, *Klass i in. przeciwko Niemcom*, nr 5029/71, 6 września 1978 r.; ETPC, *Rotaru przeciwko Rumunii* [WI], nr 28341/95, 4 maja 2000 r. oraz ETPC, *Szabó i Vissy przeciwko Węgrom*, nr 37138/14, 12 stycznia 2016 r.

przetwarzanie danych osobowych w ujęciu całościowym. W związku z tym zaktualizowana konwencja nr 108 ma zastosowanie do ochrony danych w kontekście działań policji i organów wymiaru sprawiedliwości w sprawach karnych. Przetwarzanie danych genetycznych, danych osobowych dotyczących przestępstw, postępowań karnych i wyroków skazujących oraz związanych z nimi środków bezpieczeństwa, danych biometrycznych umożliwiających ujawnienie tożsamości osoby, jak również wszelkich danych szczególnie chronionych jest dopuszczone wyłącznie wówczas, gdy zapewni się odpowiednie zabezpieczenia przed ryzykiem, jakie przetwarzanie takich danych może stanowić dla interesów, praw i podstawowych wolności osoby, której dane dotyczą, zwłaszcza ryzykiem dyskryminacji[727].

Zadania prawne policji i organów wymiaru sprawiedliwości w sprawach karnych często wymagają przetwarzania danych osobowych, co może pociągać za sobą poważne konsekwencje dla osób, których dane są przetwarzane. Przyjęta przez RE w 1987 r. rekomendacja dotycząca policji zawiera wskazówki dla państw RE, w jaki sposób powinny wprowadzić w życie zasady konwencji nr 108 w związku z przetwarzaniem danych osobowych przez organy policyjne[728]. Rekomendacja została uzupełniona przez praktyczny podręcznik dotyczący wykorzystywania danych osobowych w sektorze policji, przyjęty przez Komitet Konsultacyjny ds. Konwencji nr 108[729].

Przykład: W sprawie *D.L. przeciwko Bułgarii*[730] służby społeczne, działając na podstawie postanowienia sądu, umieściły skarżącą w bezpiecznej placówce edukacyjnej. Jej korespondencja oraz rozmowy telefoniczne podlegały nieograniczonemu i masowemu nadzorowi ze strony placówki. Trybunał uznał, że doszło do naruszenia art. 8, ponieważ przedmiotowy środek nie był konieczny w demokratycznym społeczeństwie. Trybunał stwierdził, że należy podjąć wszystkie możliwe kroki, by umożliwić nieletnim umieszczonym w instytucji utrzymywanie wystarczającego kontaktu ze światem zewnętrznym, jako że stanowi to integralną część ich prawa do godnego traktowania i jest absolutnie kluczowe w przygotowaniu ich do ponownej integracji społecznej. Ma to zastosowanie w równym stopniu do wizyt, jak i korespondencji oraz rozmów telefonicznych. Ponadto nadzór

727 Zaktualizowana konwencja nr 108, art. 6.

728 Rada Europy, Komitet Ministrów (1987), zalecenie R (87) 15 dla państw członkowskich dotyczące ochrony danych osobowych wykorzystywanych w sektorze policji, 17 września 1987 r.

729 Rada Europy (2018), Komitet Konsultacyjny ds. Konvencji nr 108, Praktyczny przewodnik dotyczących wykorzystywania danych w sektorze policji, T-PD(2018)1.

730 ETPC, *D.L. przeciwko Bułgarii*, nr 7472/14, 19 maja 2016 r.

prowadzono bez dokonywania rozróżnienia między komunikacją wymienianą z członkami rodziny, organizacjami pozarządowymi reprezentującymi prawa dzieci czy prawnikami. Co więcej, decyzja o przechwytywaniu komunikacji nie opierała się na jakiejkolwiek zindywidualizowanej analizie wchodzących w grę zagrożeń.

Przykład: W sprawie *Dragojević przeciwko Chorwacji*[731] skarżącego podejrzewano o udział w nielegalnym obrocie środkami odurzającymi. Skarżącego uznano za winnego po tym, jak sędzia śledczy dopuścił zastosowanie środków niejawnego nadzoru w celu przechwytywania jego połączeń telefonicznych. Trybunał uznał, że zaskarżony środek stanowił ingerencję w prawo do poszanowania życia prywatnego i korespondencji. Wyrażona przez sędziego śledczego zgoda opierała się wyłącznie na stwierdzeniu przez organ ścigania, że „nie było możliwe prowadzenie dochodzenia za pomocą innych środków". Trybunał zauważył ponadto, że sądy karne przeprowadziły jedynie ograniczoną ocenę wykorzystania środków nadzoru oraz że rząd nie przedstawił dostępnych środków ochrony prawnej. W związku z tym doszło do naruszenia art. 8.

8.1.1. Rekomendacja dotycząca policji

ETPC konsekwentnie orzekał, że przechowywanie i zatrzymywanie danych osobowych przez policję lub krajowe organy bezpieczeństwa stanowi naruszenie art. 8 ust. 1 EKPC. Kwestii uzasadnienia takiej ingerencji dotyczy wiele wyroków Trybunału[732].

Przykład: W sprawie *B.B. przeciwko Francji*[733] skarżącego skazano za przestępstwa seksualne przeciwko 15-letnim dzieciom popełnione z nadużyciem zaufania. Zakończył odbywanie kary pozbawienia wolności w 2000 r. Rok później zwrócił się o usunięcie wzmianki o jego wyroku z rejestru karnego, ale jego wniosek odrzucono. W 2004 r. na mocy francuskiego prawa utworzono krajową sądową bazę przestępców seksualnych, a skarżącego powiadomiono o ujęciu jego danych w tej bazie. Trybunał uznał, że ujęcie

731 ETPC, *Dragojević przeciwko Chorwacji*, nr 68955/11, 15 stycznia 2015 r.

732 Zob. na przykład ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.; ETPC, *M.M. przeciwko Zjednoczonemu Królestwu*, nr 24029/07, 13 listopada 2012 r.; ETPC, *M.K. przeciwko Francji*, nr 19522/09, 18 kwietnia 2013 r. lub ETPC, *Aycaguer przeciwko Francji*, nr 8806/12, 22 czerwca 2017 r.

733 ETPC, *B.B. przeciwko Francji*, nr 5335/06, 17 grudnia 2009 r.

danych osoby skazanej za przestępstwa seksualne w krajowej sądowej bazie danych wchodziło w zakres art. 8 EKPC. Zważywszy jednak na to, że zastosowane zostały wystarczające zabezpieczenia ochrony danych, takie jak prawo osoby, której dane dotyczą, do zażądania usunięcia danych, ograniczenie czasu przechowywania danych oraz ograniczony dostęp do nich, osiągnięto właściwą równowagę między konkurującymi interesami prywatnymi i publicznymi dochodzącymi do głosu w tej sprawie. Trybunał orzekł zatem, że nie doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu*[734] obydwaj skarżący zostali oskarżeni o przestępstwa, lecz nie skazani. Ich odciski palców, profile DNA i próbki tkanek były niemniej przechowywane przez policję. W przypadku gdy daną osobę podejrzewano o popełnienie przestępstwa, w ustawie zezwolono na zatrzymanie danych biometrycznych na czas nieokreślony, nawet jeżeli podejrzany został później uniewinniony lub uwolniony od zarzutów. Trybunał uznał, że nieograniczone, masowe zatrzymywanie danych osobowych, w przypadku którego brak było ograniczeń czasowych, a uniewinnieni mieli jedynie ograniczone możliwości żądania usunięcia danych, stanowiło nieproporcjonalną ingerencję w prawa skarżących do poszanowania życia prywatnego. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Istotną w kontekście komunikacji elektronicznej kwestią jest ingerencja organów publicznych w prawa do prywatności i ochrony danych. Środki nadzoru lub przechwytywania komunikacji, na przykład urządzenia podsłuchowe, są dopuszczalne wyłącznie wówczas, gdy przewidują to przepisy i gdy jest to środek konieczny w demokratycznym społeczeństwie, podejmowany w interesie:

- ochrony bezpieczeństwa narodowego;
- bezpieczeństwa publicznego;
- ochrony interesów finansowych państwa;
- zwalczania przestępczości; lub
- ochrony osoby, której dane dotyczą, oraz praw i wolności innych osób.

734 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu* [WI], skargi nr 30562/04 i 30566/04, 4 grudnia 2008 r., pkt 119 i 125.

Wiele innych wyroków ETPC dotyczy uzasadnienia wynikającej z prowadzenia nadzoru ingerencji w prawo do ochrony prywatności.

Przykład: W sprawie *Allan przeciwko Zjednoczonemu Królestwu*[735] władze potajemnie nagrały prywatne rozmowy więźnia ze znajomym w sali odwiedzin oraz ze współoskarżonym w więziennej celi. Trybunał orzekł, że korzystanie z urządzeń nagrywających dźwięk i obraz w celi skarżącego, w sali odwiedzin oraz w stosunku do współwięźnia stanowiło ingerencję w prawo skarżącego do życia prywatnego. Ponieważ w omawianym okresie nie istniał ustawowy system regulujący wykorzystywanie przez policję tajnych urządzeń rejestrujących, ingerencja ta nie była zgodna z prawem. Trybunał orzekł zatem, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Roman Zakharov przeciwko Rosji*[736] skarżący wniósł sprawę przeciwko trzem operatorom sieci komórkowych. Twierdził, że doszło do naruszenia jego prawa do prywatności komunikacji telefonicznej, ponieważ operatorzy zainstalowali urządzenie, które umożliwiało Federalnej Służbie Bezpieczeństwa przechwytywanie rozmów telefonicznych bez uprzedniej zgody organu sądowego. Trybunał uznał, że przepisy krajowe regulujące przechwytywanie komunikacji nie przewidują skutecznych gwarancji na wypadek arbitralności i ryzyka nadużyć. W szczególności prawo krajowe nie wymaga usunięcia danych po osiągnięciu celu, w którym były przechowywane. Co więcej, choć wymagano zgody organu sądowego, nadzór sądowy nie był wystarczający.

Przykład: W sprawie *Szabó i Vissy przeciwko Węgrom*[737] skarżący twierdzili, że węgierska ustawa narusza art. 8 EKPC, ponieważ nie jest wystarczająco szczegółowa i precyzyjna. Podnoszono ponadto, że ustawa ta nie przewiduje wystarczających gwarancji na wypadek nadużyć i arbitralności. Trybunał orzekł, że węgierska ustawa nie wymagała uzyskania zgody sądu na nadzór. Zauważył jednak, że choć nadzór wymagał zezwolenia ministra sprawiedliwości, miał on zdecydowanie charakter polityczny, przez co nie było możliwe zapewnienie wymaganej oceny „absolutnej konieczności". Co więcej, prawo krajowe nie zapewniało kontroli sądowej, ponieważ osoby, których działania te dotyczyły, nie otrzymały żadnego powiadomienia. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

735 ETPC, *Allan przeciwko Zjednoczonemu Królestwu*, nr 48539/99, 5 listopada 2002 r.

736 ETPC, *Roman Zakharov przeciwko Rosji*, nr 47143/06, 4 grudnia 2015 r.

737 ETPC, *Szabo i Vissy przeciwko Węgrom*, nr 37138/14, 12 stycznia 2016 r.

Przetwarzanie danych przez organy policyjne może mieć znaczący wpływ na zainteresowane osoby, zachodzi więc szczególna potrzeba opracowania szczegółowych przepisów dotyczących ochrony danych w odniesieniu do przetwarzania danych osobowych w tym obszarze. W rekomendacji RE dotyczącej policji dołożono starań, aby rozwiązać ten problem, przedstawiając wskazówki dotyczące sposobu gromadzenia danych do celów policyjnych; sposobu prowadzenia akt w tym obszarze; osób, które powinny mieć dostęp do tych akt, w tym warunków przekazywania danych osobowych zagranicznym organom policyjnym; sposobu wykonywania praw do ochrony danych przez osoby, których dane dotyczą; oraz sposobu sprawowania kontroli przez niezależne organy. Uwzględniono także obowiązek zapewnienia prawidłowego stopnia bezpieczeństwa danych.

W rekomendacji nie przewiduje się nieograniczonego, masowego gromadzenia danych osobowych przez organy policyjne. Ogranicza się w nim gromadzenie danych osobowych przez organy policyjne do zakresu niezbędnego w celu zapobiegania realnemu niebezpieczeństwu lub ścigania określonego przestępstwa. Gromadzenie danych w jakimkolwiek dodatkowym zakresie musiałoby odbywać się na podstawie konkretnych przepisów krajowych. Przetwarzanie danych szczególnie chronionych należy ograniczyć do zakresu bezwzględnie koniecznego w kontekście konkretnego dochodzenia.

W przypadku gdy dane osobowe są gromadzone bez wiedzy osoby, której dane dotyczą, osobę tę należy poinformować o gromadzeniu danych, gdy tylko takie ujawnienie nie stoi już na przeszkodzie prowadzeniu dochodzenia. Gromadzenie danych wskutek nadzoru technicznego lub innych zautomatyzowanych środków powinno również opierać się na konkretnych przepisach.

Przykład: W sprawie *Versini-Campinchi i Crasnianski przeciwko Francji*[738] skarżąca, prawniczka, odbyła rozmowę telefoniczną z klientem, którego połączenia były przechwytywane na polecenie sędziego śledczego. Z transkrypcji rozmowy wynika, że ujawniła mu informacje objęte poufnością wymiany informacji między prawnikiem a klientem. Prokurator przekazał tę informację Radzie Adwokackiej, a ta nałożyła na skarżącą karę. Trybunał potwierdził, że doszło do ingerencji w prawo do poszanowania życia prywatnego i korespondencji nie tylko osoby, której telefon był na podsłuchu, lecz także skarżącej, której komunikację przechwycono i poddano

738 ETPC, *Versini-Campinchi i Crasnianski przeciwko Francji*, nr 49176/11, 16 czerwca 2016 r.

transkrypcji. Ingerencja była zgodna z prawem i służyła uzasadnionemu celowi zapobiegania naruszaniu porządku. Na wniosek skarżącej przeprowadzono ocenę zgodności z prawem przekazania transkrypcji podsłuchanej rozmowy telefonicznej w kontekście wszczętego przeciwko niej postępowania dyscyplinarnego. Choć nie zdołała doprowadzić do anulowania transkrypcji tej rozmowy, Trybunał stwierdził, że istniała skuteczna kontrola, która mogła umożliwić ograniczenie zaskarżonej ingerencji do tego, co konieczne w demokratycznym społeczeństwie. Trybunał uznał, iż argument, że możliwość wszczęcia postępowania karnego przeciwko prawnikowi na podstawie transkrypcji mogła zniechęcać do korzystania ze swobody komunikacji między prawnikiem a jego klientem, a co za tym idzie – ograniczyć prawa klienta do obrony – nie był wiarygodny w sytuacji, gdy ujawnienie informacji przez samą prawniczkę mogło być niezgodne z prawem. W związku z powyższym Trybunał nie stwierdził naruszenia art. 8.

Rekomendacja RE dotycząca policji stanowi, że podczas przechowywania danych osobowych należy uczynić wyraźne rozróżnienie między: danymi administracyjnymi i danymi policyjnymi; danymi osobowymi różnych rodzajów osób, których dane dotyczą, np. podejrzanych, skazanych, pokrzywdzonych i świadków; a także danymi uważanymi za fakty oraz opartymi na podejrzeniach lub przypuszczeniach.

Cele, do których można wykorzystywać dane policyjne, powinny być ściśle ograniczone. Ma to konsekwencje dla ujawniania danych policyjnych osobom trzecim: przekazywanie lub ujawnianie takich danych w sektorze policji powinno być uwarunkowane tym, czy istnieje uzasadniony interes w udostępnieniu informacji. Przekazywanie lub ujawnianie takich danych poza sektor policji powinno być dopuszczalne tylko wtedy, gdy istnieje wyraźny obowiązek prawny lub wyraźne upoważnienie.

Przykład: W sprawie *Karabeyoğlu przeciwko Turcji*[739] monitorowano linie telefoniczne skarżącego, sędziego, w kontekście śledztwa dotyczącego nielegalnej organizacji, gdyż podejrzewano go o przynależność do tej organizacji lub udzielanie jej wsparcia i pomocy. Po podjęciu decyzji o niewszczynaniu postępowania prokurator prowadzący śledztwo zniszczył uzyskane w ten sposób nagrania. Kopia nagrań pozostała jednak w posiadaniu sędziów śledczych, którzy wykorzystali zarejestrowane

739 ETPC, *Karabeyoğlu przeciwko Turcji*, nr 30083/10, 7 czerwca 2016 r.

materiały w postępowaniu dyscyplinarnym przeciwko skarżącemu. Trybunał uznał, że naruszono przepisy, które miały w tym przypadku zastosowanie, ponieważ informacje zostały wykorzystane w celach innych niż te, w których je zgromadzono, a dodatkowo nie zniszczono ich w przewidzianym w przepisach terminie. Jeżeli chodzi o postępowanie dyscyplinarne wszczęte przeciwko skarżącemu, ingerencja w prawo skarżącego do poszanowania życia prywatnego nie była zgodna z prawem.

Międzynarodowe przekazywanie lub ujawnianie danych powinno ograniczać się do zagranicznych organów policyjnych i opierać się na specjalnych przepisach prawnych, ewentualnie umowach międzynarodowych, chyba że jest ono niezbędne dla zapobieżenia poważnemu i bezpośredniemu niebezpieczeństwu.

Przetwarzanie danych przez policję musi podlegać niezależnemu nadzorowi w celu zapewnienia zgodności z krajowym prawem o ochronie danych. Osoby, których dane dotyczą, muszą dysponować wszystkimi prawami dostępu zapisanymi w zaktualizowanej konwencji nr 108. W przypadku gdy prawa dostępu osób, których dane dotyczą, zostały ograniczone zgodnie z art. 9 konwencji nr 108 w interesie skuteczności dochodzenia policyjnego i wykonywania sankcji karnych, osobie, której dane dotyczą, musi na mocy prawa krajowego przysługiwać prawo do odwołania się do krajowego organu nadzorczego ds. ochrony danych lub do innego niezależnego organu.

8.1.2. Konwencja budapeszteńska o cyberprzestępczości

Jako że działania przestępcze w coraz większym stopniu wykorzystują elektroniczne systemy przetwarzania danych i wpływają na ich działanie, potrzebne są nowe przepisy prawa karnego, które pozwolą sprostać temu wyzwaniu. Dlatego RE przyjęła międzynarodowy akt prawny – konwencję o cyberprzestępczości, znaną również jako konwencja budapeszteńska – dotyczący przestępstw popełnianych przeciwko sieciom elektronicznym oraz z ich wykorzystaniem[740]. Do konwencji mogą przystąpić także państwa niebędące członkami Rady Europy. Na początku 2018 r.

740 Rada Europy, Komitet Ministrów (2001), Konwencja o cyberprzestępczości, CETS nr 185, Budapeszt, 23 listopada 2001 r., weszła w życie 1 lipca 2004 r.

stronami konwencji było 14 państw spoza RE[741], a siedem innych państw niebędących członkami RE zostało zaproszonych do przystąpienia.

Konwencja o cyberprzestępczości pozostaje najważniejszym układem międzynarodowym dotyczącym naruszeń prawa w Internecie lub innych sieciach informacyjnych. Strony konwencji są zobowiązane zaktualizować i zharmonizować swoje prawo karne dotyczące hakowania oraz innych naruszeń bezpieczeństwa, w tym naruszeń praw autorskich, oszustw komputerowych, pornografii dziecięcej oraz innych nielegalnych działań w cyberprzestrzeni. Konwencja przyznaje także uprawnienia procesowe, w tym przeszukiwanie sieci komputerowych oraz przechwytywanie komunikatów w kontekście walki z cyberprzestępczością. Wreszcie umożliwia ona skuteczną współpracę międzynarodową. Protokół dodatkowy do konwencji dotyczy kryminalizacji rasistowskiej i ksenofobicznej propagandy w sieciach komputerowych.

Chociaż konwencja nie jest aktem mającym na celu ochronę danych, penalizuje ona działania mogące naruszać prawo osoby, której dane dotyczą, do ochrony swoich danych. Co więcej, zobowiązuje umawiające się strony do przyjęcia środków prawnych umożliwiających organom krajowym przechwytywanie danych dotyczących ruchu i treści[742]. Zobowiązuje też umawiające się strony do dbałości przy jej wdrażaniu o odpowiednią ochronę praw człowieka i wolności, w tym praw zagwarantowanych w EKPC, takich jak prawo do ochrony danych[743]. Umawiające się strony nie muszą być stronami konwencji nr 108, by móc przystąpić do konwencji budapeszteńskiej o cyberprzestępczości.

741 Australia, Chile, Dominikana, Izrael, Japonia, Kanada, Kolumbia, Mauritius, Panama, Senegal, Sri Lanka, Stany Zjednoczone, Tonga i Tunezja. Zob. Tabela podpisów i ratyfikacji traktatu nr 185, stan na lipiec 2017 r.

742 Rada Europy, Komitet Ministrów (2001), Konwencja o cyberprzestępczości, CETS nr 185, Budapeszt, 23 listopada 2001 r., art. 20 i 21.

743 Tamże, art. 15 ust. 1.

8.2. Prawo UE o ochronie danych w kontekście współpracy policyjnej i sądowej w sprawach karnych

Najważniejsze kwestie

- W UE ochrona danych w sektorze policji i organów wymiaru sprawiedliwości w sprawach karnych została uregulowana w kontekście krajowego i transgranicznego przetwarzania danych przez organy policji i wymiaru sprawiedliwości państw członkowskich i podmiotów unijnych.
- Na szczeblu państw członkowskich dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości musi zostać wdrożona do prawa krajowego.
- Konkretne akty prawne regulują ochronę danych w kontekście transgranicznej współpracy policji i organów ścigania, zwłaszcza zwalczania terroryzmu i przestępczości transgranicznej.
- Istnieją szczególne zasady ochrony danych dotyczące Europejskiego Urzędu Policji (Europol) i Europejskiej Jednostki Współpracy Sądowej (Eurojust) oraz nowo ustanowionej Prokuratury Europejskiej, które są organami UE wspomagającymi i wspierającymi transgraniczną współpracę organów ścigania.
- Szczególne zasady ochrony danych obowiązują też w odniesieniu do wspólnych systemów informacyjnych ustanowionych na szczeblu UE w celu transgranicznej wymiany danych między właściwymi organami policyjnymi i sądowymi. Ważnymi przykładami są system informacyjny Schengen drugiej generacji (SIS II), wizowy system informacyjny (VIS) oraz Eurodac – scentralizowany system zawierający dane daktyloskopijne obywateli państw trzecich i bezpaństwowców ubiegających się o azyl w jednym z państw członkowskich UE.
- W UE trwa proces aktualizacji wymienionych powyżej przepisów o ochronie danych, który ma na celu zapewnienie ich zgodności z przepisami dyrektywy o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości.

8.2.1. Dyrektywa o ochronie danych osobowych przetwarzanych przez policję i organy wymiaru sprawiedliwości

Dyrektywa (UE) 2016/680 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania

przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych (dyrektywa o ochronie danych osobowych przez policję i organy wymiaru sprawiedliwości)[744] ma na celu ochronę danych osobowych zbieranych i przetwarzanych do celów wymiaru sprawiedliwości w sprawach karnych, takich jak:

- zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie i ściganie czynów zabronionych i wykonywanie kar, w tym do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom;

- wykonywanie kar;

- w przypadkach gdy policja lub inne organy ścigania działają z zamiarem utrzymywania porządku oraz zapobiegania zagrożeniom dla bezpieczeństwa publicznego i praw podstawowych społeczeństwa oraz zapobiegania takim zagrożeniom, które mogą stanowić czyn zabroniony.

Dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości służy ochronie danych osobowych różnych kategorii osób biorących udział w postępowaniu karnym, na przykład świadków, informatorów, ofiary, podejrzanych i ich wspólników. Policja i organy wymiaru sprawiedliwości w sprawach karnych są zobowiązane przestrzegać przepisów dyrektywy podczas przetwarzania takich danych osobowych do celów ścigania przestępstw, zarówno w ramach zakresu podmiotowego, jak i przedmiotowego dyrektywy[745].

Dozwolone jest jednak również wykorzystanie danych do innych celów, z zastrzeżeniem określonych warunków. Przetwarzanie danych w innym celu związanym ze ściganiem przestępstw niż ten, w którym dane zostały zebrane, jest dopuszczone wyłącznie wówczas, gdy jest to zgodne z prawem, niezbędne i proporcjonalne

744 Dyrektywa (UE) 2016/680 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89 (dyrektywa o ochronie danych osobowych przez policję i organy wymiaru sprawiedliwości).

745 Dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości, art. 2 ust. 1.

w świetle prawa krajowego lub prawa UE[746]. W przypadku celów niespełniających tych kryteriów zastosowanie ma ogólne rozporządzenie o ochronie danych. Ewidencjonowanie czynności i dokumentowanie udostępniania danych to jeden ze szczególnych obowiązków właściwych organów, który ma ułatwić wyjaśnienie odpowiedzialności wynikającej ze skarg.

Właściwe organy działające w sektorze policji i wymiaru sprawiedliwości w sprawach karnych to organy publiczne lub organy, które na mocy prawa krajowego i uprawnień publicznych są uprawnione do wykonywania funkcji organu publicznego[747], na przykład prowadzenia prywatnych więzień[748]. Stosowanie dyrektywy obejmuje zarówno przetwarzanie danych na szczeblu krajowym, jak i transgraniczne przetwarzanie przez policję i organy wymiaru sprawiedliwości państw członkowskich, a także międzynarodowe przekazywanie danych przez właściwe organy do państw trzecich i organizacji międzynarodowych[749]. Zakresem aktu nie jest objęte bezpieczeństwo narodowe ani przetwarzanie danych osobowych przez instytucje, organy, urzędy i agencje UE[750].

Dyrektywa w dużej mierze opiera się na zasadach i definicjach zawartych w ogólnym rozporządzeniu o ochronie danych, które uwzględniają szczególny charakter pracy policji i organów wymiaru sprawiedliwości w sprawach karnych. Nadzór mogą sprawować te same organy państw członkowskich, które wykonują ten obowiązek zgodnie z ogólnym rozporządzeniem o ochronie danych. Wyznaczenie inspektorów ochrony danych i przeprowadzanie ocen skutków dla ochrony danych to nowe obowiązki policji i organów wymiaru sprawiedliwości w sprawach karnych wprowadzone dyrektywą[751]. Choć pojęcia te są zainspirowane ogólnym rozporządzeniem o ochronie danych, dyrektywa odnosi się do szczególnego charakteru działań policji i organów wymiaru sprawiedliwości w sprawach karnych. W przeciwieństwie

746 Tamże, art. 4 ust. 2.

747 Tamże, art. 3 pkt 7.

748 Komisja Europejska (2016), Komunikat Komisji do Parlamentu Europejskiego na podstawie art. 294 ust. 6 Traktatu o funkcjonowaniu Unii Europejskiej dotyczący stanowiska Rady w sprawie przyjęcia dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich, ścigania lub wykonywania kar kryminalnych oraz w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW, COM(2016) 213 final, Bruksela, 11 kwietnia 2016 r.

749 Dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości, rozdział V.

750 Tamże, art. 2 ust. 3.

751 Tamże, odpowiednio art. 32 i art. 27.

do przetwarzania danych do celów komercyjnych, które reguluje rozporządzenie, przetwarzanie do celów związanych z bezpieczeństwem może wymagać pewnego stopnia elastyczności. Przykładowo zapewnienie osobom, których dane dotyczą, takiego samego poziomu ochrony prawa do informacji, dostępu do swoich danych osobowych lub ich usunięcia, jaki przewidziano w ogólnym rozporządzeniu o ochronie danych, mogłoby oznaczać, że jakiekolwiek czynności nadzoru realizowane do celów ścigania przestępstw byłyby nieskuteczne. Z tego względu w dyrektywie nie ujęto zasady przejrzystości. Podobnie zasady minimalizacji danych i celowości, zgodnie z którymi dane osobowe muszą ograniczać się wyłącznie do tego, co jest niezbędne do celów, w których są przetwarzane, oraz wymagające przetwarzania ich wyłącznie w konkretnym i wyraźnie określonym celu, również muszą być stosowane elastycznie w przypadku przetwarzania do celów związanych z bezpieczeństwem. Informacje zbierane i przechowywane przez właściwe organy na potrzeby danej sprawy mogą okazać się niezwykle przydatne w przypadku spraw rozpatrywanych w przyszłości.

Zasady dotyczące przetwarzania

W dyrektywie o ochronie danych przez policję i organy wymiaru sprawiedliwości określono pewne kluczowe zabezpieczenia odnoszące się do wykorzystywania danych osobowych. Nakreśla ona również zasady regulujące przetwarzanie takich danych osobowych. Państwa członkowskie mają obowiązek zapewnić, by dane osobowe były:

- przetwarzane zgodnie z prawem i rzetelnie;
- zbierane w konkretnych, wyraźnych i uzasadnionych celach i nieprzetwarzane w sposób niezgodny z tymi celami;
- adekwatne, stosowne i nienadmierne do celów, dla których są przetwarzane;
- prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe, w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
- przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów ich przetwarzania;

- przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych[752].

W myśl dyrektywy przetwarzanie jest zgodne z prawem wyłącznie wówczas, gdy odbywa się w zakresie niezbędnym do wykonania danego zadania. Co więcej, właściwy organ powinien wykonywać te czynności z myślą o realizacji celów określonych w dyrektywie oraz powinny one mieć podstawę w prawie UE lub prawie krajowym[753]. Dane nie mogą być przechowywane przez okres dłuższy niż jest to niezbędne, i należy je usuwać lub poddawać okresowemu przeglądowi w określonych terminach. Dane muszą być wykorzystywane wyłącznie przez właściwy organ oraz do celu, w jakim je zgromadzono, przekazano bądź udostępniono.

Prawa osoby, której dotyczą dane

Dyrektywa określa ponadto prawa osoby, której dane dotyczą. Należą do nich:

- Prawo do informacji. Państwa członkowskie muszą zobowiązać administratora danych do udostępnienia osobie, której dane dotyczą 1) tożsamości i danych kontaktowych administratora, 2) danych kontaktowych inspektora ochrony danych, 3) informacji o celach zamierzonego przetwarzania, 4) informacji o prawie do wniesienia skargi do organu nadzorczego oraz danych kontaktowych organu nadzorczego oraz 5) informacji o prawie żądania dostępu do danych osobowych, sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania tych danych[754]. Oprócz tych ogólnych wymogów dotyczących informacji w dyrektywie przewidziano, że w konkretnych przypadkach i w celu wykonywania przez osoby, których dane dotyczą, swoich praw administratorzy muszą udostępnić takim osobom informacje o podstawie prawnej przetwarzania oraz okresie przechowywania danych. W przypadku gdy dane mają zostać przekazane innym odbiorcom, w tym do państw trzecich lub organizacji międzynarodowych, osoby, których dane dotyczą, trzeba poinformować o kategoriach takich odbiorców. Ponadto administratorzy muszą przekazać wszelkie dalsze informacje, uwzględniając szczególne okoliczności przetwarzania danych – przykładowo gdy dane zostały zebrane w drodze niejawnego nadzoru, tj. bez wiedzy

752 Tamże, art. 4 ust. 1.

753 Tamże, art. 8.

754 Tamże, art. 13 ust. 1.

osoby, której dane dotyczą. W ten sposób można zagwarantować rzetelne przetwarzanie danych osoby, której dane dotyczą[755].

- Prawo dostępu do danych osobowych. Państwa członkowskie muszą zapewnić osobom, których dane dotyczą, prawo do wiedzy, czy ich dane osobowe są przetwarzane. Jeżeli są, takie osoby powinny mieć dostęp do określonych informacji na ten temat, na przykład o kategoriach przetwarzanych danych[756]. Prawo to jednak może być ograniczone – na przykład w celu zapobieżenia utrudnianiu postępowań przygotowawczych lub zakłócaniu ścigania przestępstw bądź w celu ochrony bezpieczeństwa publicznego oraz praw i wolności innych osób[757].

- Prawo do sprostowania danych osobowych. Państwa członkowskie mają obowiązek zapewnić, by osoba, której dane dotyczą, mogła bez zbędnej zwłoki uzyskać od administratora sprostowanie danych, jeżeli są nieprawidłowe. Ponadto osoba, której dane dotyczą, ma również prawo do uzyskania uzupełnienia niekompletnych danych osobowych[758].

- Prawo do usunięcia danych osobowych i ograniczenia ich przetwarzania. W określonych przypadkach administrator ma obowiązek usunąć dane osobowe. Ponadto osoba, której dane dotyczą, może uzyskać usunięcie swoich danych osobowych, ale wyłącznie wówczas, gdy są one przetwarzane niezgodnie z prawem[759]. W określonych sytuacjach zamiast usuwać dane osobowe, można ograniczyć ich przetwarzanie. Może to mieć miejsce, gdy 1) zostanie zakwestionowana prawidłowość danych osobowych, ale nie można tego stwierdzić, lub 2) dane osobowe muszą zostać zachowane do celów dowodowych[760].

Gdy administrator odmówi sprostowania lub usunięcia danych osobowych lub ograniczenia przetwarzania danych, musi o tym pisemnie poinformować osobę, której dane dotyczą. Państwa członkowskie mogą ograniczyć to prawo do informacji

755 Tamże, art. 13 ust. 2.
756 Tamże, art. 14.
757 Tamże, art. 15.
758 Tamże, art. 16 ust. 1.
759 Tamże, art. 16 ust. 2.
760 Tamże, art. 16 ust. 3.

między innymi w celu ochrony bezpieczeństwa publicznego lub praw i wolności innych osób z tych samych względów, co w przypadku prawa dostępu[761].

Osoba, której dane dotyczą, jest co do zasady uprawniona do uzyskania informacji o przetwarzaniu jej danych osobowych i ma prawo dostępu, sprostowania lub usunięcia danych bądź ograniczenia ich przetwarzania, które to prawo może wyegzekwować bezpośrednio od administratora. Na mocy dyrektywy o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości możliwe jest też ewentualne pośrednie wykonanie praw osób, których dane dotyczą, za pośrednictwem organu nadzorującego ochronę danych. Z takiej ewentualności można skorzystać wówczas, gdy administrator ogranicza prawa osoby, której dane dotyczą[762]. Artykuł 17 dyrektywy wymaga od państw członkowskich przyjęcia środków gwarantujących, że osoba, której dane dotyczą, może wykonywać swoje prawa także za pośrednictwem właściwego organu nadzorczego. Z tego względu administrator danych musi informować osobę, której dane dotyczą, o możliwości uzyskania dostępu pośrednio.

Obowiązki administratora i podmiotu przetwarzającego

W kontekście dyrektywy o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości administratorami danych są właściwe organy publiczne bądź inne organy dysponujące właściwymi uprawnieniami publicznymi i sprawujące władzę publiczną, które ustalają cele i sposoby przetwarzania danych osobowych. W dyrektywie przewidziano szereg obowiązków administratorów danych, które mają na celu zapewnienie wysokiego poziomu ochrony danych osobowych przetwarzanych do celów ścigania przestępstw.

Właściwe organy muszą prowadzić ewidencję operacji przetwarzania realizowanych przez nie w zautomatyzowanych systemach przetwarzania. Należy ewidencjonować przynajmniej takie czynności jak zbieranie, modyfikowanie, przeglądanie, ujawnianie wraz z przekazywaniem, łączenie i usuwanie danych osobowych[763]. W dyrektywie przewidziano, że ewidencja przeglądania i ujawniania musi pozwalać ustalić zasadność, datę i godzinę takich operacji oraz w miarę możliwości tożsamość osoby, która przeglądała system lub ujawniła dane osobowe, oraz tożsamość odbiorców takich danych osobowych. Ewidencja może być używana wyłącznie do weryfikacji

761 Tamże, art. 16 ust. 4.

762 Tamże, art. 17.

763 Tamże, art. 25 ust. 1.

zgodności przetwarzania z prawem, do monitorowania własnej działalności, zapewnienia integralności i bezpieczeństwa danych osobowych oraz na potrzeby postępowania karnego[764]. Administrator i podmiot przetwarzający muszą udostępnić ewidencję organowi nadzorczemu na jego żądanie.

Przede wszystkim na administratorach spoczywa ogólny obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z dyrektywą i aby móc to wykazać[765]. Opracowując te środki, administratorzy muszą uwzględnić charakter, zakres i kontekst przetwarzania oraz – co istotne – wszelkie potencjalne ryzyko naruszenia praw lub wolności osób fizycznych. Administratorzy powinni przyjąć polityki wewnętrzne i wdrożyć środki zapewniające zgodność z zasadami ochrony danych, zwłaszcza z zasadą uwzględniania ochrony danych w fazie projektowania oraz domyślnej ochrony danych[766]. Jeżeli przetwarzanie może skutkować powstaniem wysokiego ryzyka naruszenia praw osób fizycznych – na przykład ze względu na wykorzystanie nowych technologii – administrator przed przetworzeniem musi dokonać oceny skutków dla ochrony danych osobowych[767]. W dyrektywie wymieniono również środki, które administratorzy muszą wdrożyć, żeby zapewnić bezpieczeństwo przetwarzania. Należą do nich środki, które uniemożliwiają osobom nieuprawnionym dostęp do danych osobowych przetwarzanych przez administratorów, gwarantują, że osoby uprawnione mają dostęp wyłącznie do danych osobowych objętych posiadanym przez nie uprawnieniem oraz zapewniają prawidłowe działanie funkcji systemu przetwarzania i odporność przechowywanych danych na uszkodzenia powodowane błędnym działaniem systemu[768]. Jeżeli mimo to dojdzie do naruszenia ochrony danych, administratorzy mają obowiązek zgłoszenia tego organowi nadzorczemu w ciągu trzech dni, opisując przy tym charakter naruszenia, jego możliwe konsekwencje, kategorie danych osobowych, których dotyczy naruszenie, oraz przybliżoną liczbę osób, których dane dotyczą, dotkniętych naruszeniem. Należy „bez zbędnej zwłoki" zawiadomić osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli naruszenie to może powodować wysokie ryzyko naruszenia praw i wolności tej osoby[769].

764 Tamże, art. 25 ust. 2.

765 Tamże, art. 19.

766 Tamże, art. 20.

767 Tamże, art. 27.

768 Tamże, art. 29.

769 Tamże, art. 30 i 31.

W dyrektywie zawarto również zasadę rozliczalności, a na administratorów nałożono obowiązek wdrożenia środków mających na celu zapewnienie zgodności z tą zasadą. Administratorzy muszą prowadzić wykaz wszystkich kategorii czynności przetwarzania, za które odpowiadają – zawartość takich wykazów precyzuje art. 24 dyrektywy. Wykazy należy udostępniać organowi nadzorczemu na jego żądanie, by mógł on monitorować operacje przetwarzania realizowane przez administratora. Kolejnym ważnym środkiem mającym na celu zwiększenie rozliczalności jest wyznaczenie inspektora ochrony danych. Administratorzy muszą wyznaczyć inspektora ochrony danych, choć dyrektywa umożliwia państwom członkowskim zwolnienie z tego obowiązku sądów i innych niezależnych organów sądowych[770]. Obowiązki inspektora ochrony danych są zbliżone do tych wynikających z ogólnego rozporządzenia o ochronie danych. Osoba taka monitoruje przestrzeganie dyrektywy oraz informuje pracowników zajmujących się przetwarzaniem danych o obowiązkach spoczywających na nich na mocy przepisów o ochronie danych. Ponadto inspektor ochrony danych przedstawia zalecenia co do potrzeby przeprowadzenia oceny skutków dla ochrony danych oraz pełni funkcję punktu kontaktowego wobec organu nadzorczego.

Przekazywanie danych do państw trzecich lub organizacji międzynarodowych

Podobnie jak w przypadku ogólnego rozporządzenia o ochronie danych dyrektywa ustanawia warunki przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Gdyby dane osobowe były swobodnie przekazywane poza obszar jurysdykcji UE, zabezpieczenia oraz silna ochrona zagwarantowane na mocy unijnego prawa mogłyby zostać naruszone. Same warunki w znacznym stopniu różnią się jednak od tych, jakie przewiduje ogólne rozporządzenie o ochronie danych. Przekazywanie danych do państw trzecich lub organizacji międzynarodowych jest możliwe, jeżeli[771]:

- Przekazanie jest niezbędne do celów dyrektywy.

- Dane osobowe są przekazywane właściwemu organowi – w rozumieniu dyrektywy – państwa trzeciego lub organizacji międzynarodowej, przy czym w indywidualnych, konkretnych przypadkach obowiązuje odstępstwo od tej reguły[772].

770 Tamże, art. 32.

771 Tamże, art. 35.

772 Tamże, art. 39.

- Przekazanie do państw trzecich lub organizacji międzynarodowych danych osobowych uzyskanych w drodze współpracy międzynarodowej wymaga zgody państwa członkowskiego, z którego dane pochodzą, przy czym w pilnych przypadkach są przewidziane odstępstwa.

- Komisja Europejska przyjęła decyzję stwierdzającą odpowiedni stopień ochrony, zostały zapewnione odpowiednie zabezpieczenia lub mają zastosowanie wyjątki dotyczące przekazywania w szczególnych sytuacjach.

- Dalsze przekazanie danych do innego państwa trzeciego bądź organizacji międzynarodowej wymaga wcześniejszej zgody właściwego organu, który dokonał pierwotnego przekazania, uwzględniającej między innymi powagę czynu zabronionego i poziom ochrony danych osobowych w państwie, do którego dane mają zostać dalej przekazane[773].

Zgodnie z dyrektywą przekazanie danych osobowych może mieć miejsce wyłącznie wówczas, gdy spełniony jest jeden z trzech warunków. Pierwszym z nich jest stwierdzenie przez Komisję Europejską odpowiedniego stopnia ochrony na mocy dyrektywy. Decyzja może obejmować całe terytorium państwa trzeciego bądź odnosić się do konkretnych sektorów w takim państwie lub do organizacji międzynarodowej. Wymaga to jednak zapewnienia odpowiedniego poziomu ochrony i spełnienia warunków określonych w dyrektywie[774]. W takich przypadkach przekazanie danych osobowych nie wymaga zezwolenia państwa członkowskiego[775]. Komisja Europejska musi monitorować zmiany mogące wpłynąć na obowiązywanie decyzji stwierdzających odpowiedni poziom ochrony. Ponadto decyzja musi przewidywać mechanizm okresowego przeglądu. Komisja może również uchylić, zmienić lub zawiesić decyzję, jeżeli z dostępnych informacji wynika, że okoliczności w państwie trzecim lub organizacji międzynarodowej nie zapewniają już odpowiedniego poziomu ochrony. W takim przypadku Komisja musi podjąć konsultacje z państwem trzecim lub organizacją międzynarodową w celu podjęcia próby naprawy sytuacji.

W razie braku decyzji stwierdzającej odpowiedni stopień ochrony przekazywanie może się opierać na odpowiednich zabezpieczeniach. Zabezpieczenia te może wprowadzać prawnie wiążący akt lub administrator może samodzielnie przeprowadzić ocenę okoliczności towarzyszących przekazaniu danych osobowych i stwierdzić, że

773 Tamże, art. 35 ust. 1.

774 Tamże, art. 36.

775 Tamże, art. 36 ust. 1.

istnieją odpowiednie zabezpieczenia. Taka samodzielna ocena powinna uwzględniać ewentualne umowy o współpracy zawarte przez Europol lub Eurojust z państwami trzecimi lub organizacjami międzynarodowymi, istnienie obowiązków zachowania poufności i zasady ograniczonego celu, a także zapewnienia, że dane osobowe nie posłużą do umożliwienia żadnego rodzaju okrutnego lub nieludzkiego traktowania, w tym kary śmierci[776]. W przypadku samodzielnej oceny administrator ma obowiązek poinformować właściwy organ nadzorczy o kategoriach tego typu przekazań[777].

W razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń przekazywanie danych nadal jest możliwe w szczególnych sytuacjach wskazanych w dyrektywie. Należą do nich między innymi ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby oraz zapobieżenie bezpośredniemu, poważnemu ryzyku naruszenia bezpieczeństwa publicznego państwa członkowskiego lub państwa trzeciego[778].

W indywidualnych, konkretnych przypadkach przekazywanie danych przez właściwe organy odbiorcom mającym siedzibę w państwach trzecich, niebędącym właściwymi organami, może mieć miejsce, jeżeli oprócz zachowania opisanych powyżej trzech warunków spełnione są ponadto dodatkowe warunki wskazane w art. 39 dyrektywy. Przede wszystkim przekazanie danych musi być bezwzględnie niezbędne do wykonania zadania właściwego organu przekazującego, który jest ponadto odpowiedzialny za stwierdzenie, że podstawowe prawa ani wolności osób fizycznych nie są nadrzędne wobec interesu publicznego przemawiającego za przekazaniem. W takich przypadkach przekazanie danych musi być udokumentowane, a właściwy organ przekazujący musi przekazać informacje właściwemu organowi nadzorczemu[779].

Ponadto w odniesieniu do państw trzecich i organizacji międzynarodowych dyrektywa wymaga też wypracowania mechanizmów współpracy międzynarodowej ułatwiających skuteczne egzekwowanie przepisów, a zatem pomaga organom nadzorującym ochronę danych współpracę z ich zagranicznymi odpowiednikami[780].

776 Tamże, motyw 71.

777 Tamże, art. 37 ust. 1.

778 Tamże, art. 38 ust. 1.

779 Tamże, art. 37 ust. 3.

780 Tamże, art. 40.

Niezależna kontrola oraz środki ochrony prawnej dostępne dla osób, których dane dotyczą

Każde państwo członkowskie musi zapewnić, by za monitorowanie stosowania przepisów przyjętych na mocy przedmiotowej dyrektywy oraz doradztwo w tym zakresie odpowiadał co najmniej jeden niezależny krajowy organ nadzorczy[781]. Organ nadzorczy powołany do celów dyrektywy może być tożsamy z organem ustanowionym na mocy ogólnego rozporządzenia o ochronie danych, niemniej państwa członkowskie mogą wyznaczyć inny organ, pod warunkiem, że spełnia on kryterium niezależności. Organy nadzorcze rozpatrują ponadto wnoszone przez osoby skargi dotyczące ochrony ich praw i wolności w związku z przetwarzaniem danych osobowych przez właściwe organy.

W przypadku uzasadnionej istotnymi podstawami odmowy wykonania praw osoby, której dane dotyczą, osobie takiej musi przysługiwać prawo wniesienia odwołania do właściwego krajowego organu nadzorczego lub sądu. Jeżeli osoba poniesie szkodę w wyniku naruszenia prawa krajowego wdrażającego przedmiotową dyrektywę, ma prawo do otrzymania od administratora lub innego organu właściwego w świetle prawa państwa członkowskiego odszkodowania[782]. Co do zasady osoby, których dane dotyczą, muszą mieć dostęp do środka prawnego przed sądem w przypadku jakiegokolwiek naruszenia ich praw zagwarantowanych w przepisach krajowych wdrażających dyrektywę[783].

8.3. Inne szczegółowe akty prawne o ochronie danych w kontekście ścigania przestępstw

Oprócz dyrektywy o ochronie danych przez policję i organy wymiaru sprawiedliwości wymianę informacji będących w posiadaniu państw członkowskich w określonych obszarach reguluje szereg aktów prawnych, między innymi decyzja ramowa Rady 2009/315/WSiSW w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, decyzja Rady 2000/642/WSiSW dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu

781 Tamże, art. 41.

782 Tamże, art. 56.

783 Tamże, art. 54.

do wymiany informacji oraz decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej[784].

Co istotne, współpraca transgraniczna[785] między właściwymi organami w coraz większym stopniu wiąże się z wymianą danych dotyczących imigracji. Ta dziedzina prawa nie należy do kompetencji policji i wymiaru sprawiedliwości w sprawach karnych, ale jest pod wieloma względami istotna dla pracy organów policyjnych i sądowych. To samo dotyczy danych na temat towarów przywożonych do UE lub wywożonych z niej. Zniesienie kontroli na granicach wewnętrznych strefy Schengen zwiększyło ryzyko nadużyć, więc państwa członkowskie muszą zacieśnić współpracę, w szczególności usprawniając transgraniczną wymianę informacji, aby skuteczniej wykrywać i ścigać naruszenia krajowego oraz unijnego prawa celnego. Ponadto w ostatnich latach doszło do nasilenia poważnej i zorganizowanej przestępczości oraz terroryzmu, które to zjawiska mogą się wiązać z podróżami międzynarodowymi i wskazują na to, że w wielu przypadkach istnieje potrzeba zacieśnienia transgranicznej współpracy policji i organów ścigania[786].

Decyzja w sprawie konwencji z Prüm

Ważnym przykładem zinstytucjonalizowanej współpracy transgranicznej polegającej na wymianie danych posiadanych przez poszczególne kraje jest decyzja Rady 2008/615/WSiSW w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (decyzja w sprawie konwencji z Prüm), na mocy której w 2008 r. włączono konwencję z Prüm do prawa UE,

784 Rada Unii Europejskiej (2009), Decyzja ramowa Rady 2009/315/WSiSW z dnia 26 lutego 2009 r. w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji, Dz.U. L 93 z 7.4.2009; Rada Unii Europejskiej (2000), Decyzja Rady 2000/642/WSiSW z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego Państw Członkowskich w odniesieniu do wymiany informacji, Dz.U. L 271 z 24.10.2000; Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania Państw Członkowskich Unii Europejskiej, Dz.U. L 386 z 29.12.2006.

785 Komisja Europejska (2012), Komunikat Komisji do Parlamentu Europejskiego i Rady – Zacieśnienie współpracy organów ścigania w UE – europejski model wymiany informacji (EIXM), COM(2012) 735 final, Bruksela, 7 grudnia 2012 r.

786 Zob. Komisja Europejska (2011), Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, COM(2011) 32 final, Bruksela, 2 lutego 2011 r., s. 1.

oraz przepisy wdrażające tę decyzję ujęte w decyzji 2008/615/WSiSW[787]. Konwencja z Prüm to międzynarodowe porozumienie o współpracy policyjnej zawarte między Austrią, Belgią, Francją, Niemcami, Luksemburgiem, Holandią i Hiszpanią[788].

Decyzja w sprawie konwencji z Prüm ma pomóc państwom członkowskim w usprawnieniu wymiany informacji w celu zapobiegania i zwalczania przestępczości w trzech obszarach: terroryzmu, przestępczości transgranicznej oraz nielegalnej migracji. W tym celu w decyzji zawarto przepisy dotyczące:

- zautomatyzowanego dostępu do profili DNA, danych daktyloskopijnych i określonych krajowych danych rejestracyjnych pojazdów;
- dostarczania danych w związku z istotnymi wydarzeniami rangi międzynarodowej;
- dostarczania informacji służących zapobieganiu przestępstwom terrorystycznym;
- innych środków na rzecz intensyfikacji transgranicznej współpracy policji.

Kwestie baz danych udostępnianych na mocy decyzji w sprawie konwencji z Prüm reguluje wyłącznie prawo krajowe, natomiast wymiana danych podlega dodatkowo omawianej decyzji, która ma zostać oceniona pod kątem zgodności z dyrektywą o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości. Organami właściwymi do nadzorowania takiego przepływu danych są krajowe organy nadzorujące ochronę danych.

787 Rada Unii Europejskiej (2008), Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej, Dz.U. L 210 z 6.8.2008.

788 Konwencja zawarta między Królestwem Belgii, Republiką Federalną Niemiec, Królestwem Hiszpanii, Republiką Francuską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów i Republiką Austrii w sprawie intensywniejszej współpracy transgranicznej, szczególnie w walce z terroryzmem, przestępczością transgraniczną i nielegalną migracją.

Decyzja ramowa 2006/960/WSiSW – inicjatywa szwedzka

Decyzja ramowa 2006/960/WSiSW (inicjatywa szwedzka)[789] to kolejny przykład transgranicznej współpracy w obszarze wymiany danych będących w posiadaniu organów ścigania w poszczególnych krajach. Inicjatywa szwedzka skupia się w szczególności na wymianie danych wywiadowczych i informacji, a w art. 8 przewiduje konkretne zasady ochrony danych.

Zgodnie z tym aktem wykorzystanie wymienianych informacji i danych wywiadowczych musi przebiegać zgodnie z krajowymi przepisami z zakresu ochrony danych obowiązującymi w państwie członkowskim otrzymującym informacje na tych samych zasadach, co dane gromadzone w tym państwie. Artykuł 8 idzie o krok dalej. Stwierdzono w nim, że przy udostępnianiu informacji i danych wywiadowczych właściwy organ ścigania może zgodnie z prawem krajowym nałożyć warunki dotyczące ich wykorzystania przez otrzymujący je właściwy organ ścigania. Takie warunki mogą również odnosić się do składania sprawozdań z wyników dochodzenia karnego lub operacji wywiadowczej dotyczącej przestępstwa, w ramach których była konieczna wymiana informacji i danych wywiadowczych. Niemniej jednak gdy prawo krajowe uchyla ograniczenia dotyczące wykorzystania danych i informacji (na przykład w odniesieniu do organów sądowych, organów ustawodawczych itp.), informacje i dane wywiadowcze mogą zostać wykorzystane wyłącznie po uprzedniej konsultacji z przekazującym państwem członkowskim.

Udostępnione informacje i dane wywiadowcze mogą być wykorzystywane:

- do celów, w których zostały dostarczone; oraz
- do zażegnania bezpośredniego i poważnego zagrożenia dla bezpieczeństwa publicznego;

Ich przetwarzanie w innych celach jest dopuszczalne, ale wyłącznie po uzyskaniu zezwolenia przekazującego państwa członkowskiego.

W inicjatywie szwedzkiej stwierdzono ponadto, że przetwarzane dane osobowe muszą podlegać ochronie zgodnie z międzynarodowymi instrumentami, takimi jak:

789 Rada Unii Europejskiej (2006), Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej, Dz.U. L 386 z 29.12.2006, s. 89.

- Konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych[790];

- Protokół dodatkowy z dnia 8 listopada 2001 r. do tej konwencji, dotyczący organów nadzoru i transgranicznych przepływów danych[791];

- Rekomendacja nr R(87) 15 Rady Europy dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji[792].

Dyrektywa UE w sprawie danych PNR

Dane dotyczące przelotu pasażera (PNR) odnoszą się do informacji o pasażerach lotniczych, zbieranych i przechowywanych w systemach rezerwacji i odpraw pasażerskich przewoźników do celów prowadzonej przez nich działalności gospodarczej. Dane te obejmują różnego rodzaju informacje, takie jak daty podróży, trasa podróży, informacje o bilecie, dane kontaktowe, biuro podróży, za pośrednictwem którego rezerwowano bilet, zastosowana metoda płatności, numer miejsca i informacje o bagażu[793]. Przetwarzanie danych PNR może pomóc organom ścigania identyfikować znanych lub potencjalnych podejrzanych oraz sprawdzać pasażerów na podstawie wzorców podróżowania i innych wskaźników zwyczajowo powiązanych z działalnością przestępczą. Analiza danych PNR umożliwia również retrospektywne prześledzenie tras podróży i danych kontaktowych osób podejrzanych o udział w działalności przestępczej, co może pozwolić organom ścigania wykrywać siatki przestępcze[794]. Unia Europejska zawarła z państwami trzecimi umowy dotyczące wymiany danych PNR, co opisano w sekcji 7. Ponadto wprowadziła przetwarzanie danych PNR w UE w drodze dyrektywy 2016/681/UE w sprawie wykorzystywania danych PNR w celu zapobiegania przestępstwom terrorystycznym i poważnej

790 Rada Europy (1981), Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, ETS nr 108.

791 Rada Europy (2001), Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, ETS nr 108.

792 Rada Europy (1987), Rekomendacja R(87) 15 Komitetu Ministrów do państw członkowskich dotycząca ochrony danych osobowych wykorzystywanych w sektorze policji (przyjęta przez Komitet Ministrów dnia 17 września 1987 r. podczas 410. spotkania delegatów Ministrów).

793 Komisja Europejska (2011), Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, COM(2011) 32 final, Bruksela, 2 lutego 2011 r., s. 1.

794 Komisja Europejska (2015), nota informacyjna Fighting terrorism at EU level, an overview of Commission's actions, measures and initiatives, Bruksela, 11 stycznia 2015 r.

przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (dyrektywa UE w sprawie danych PNR)[795]. Dyrektywa przewiduje obowiązek przekazywania przez przewoźników lotniczych danych PNR właściwym organom i ustanawia rygorystyczne zabezpieczenia ochrony danych odnoszące się do przetwarzania i zbierania takich danych. Dyrektywa UE w sprawie danych PNR ma zastosowanie do lotów międzynarodowych do UE i z UE, a także do lotów wewnątrzunijnych, jeżeli państwo członkowskie podejmie taką decyzję[796].

Zbierane dane PNR powinny zawierać wyłącznie informacje, o których mowa w dyrektywie UE w sprawie danych PNR. Dane te muszą być zatrzymywane w jednej jednostce do spraw informacji, w bezpiecznej lokalizacji na terytorium każdego państwa członkowskiego. Dane PNR należy poddać depersonalizacji sześć miesięcy po ich przekazaniu przez przewoźnika lotniczego, a maksymalny okres ich przechowywania wynosi pięć lat[797]. Dane PNR są wymieniane między państwami członkowskimi, między państwami członkowskimi a Europolem oraz udostępniane państwom trzecim, ale wyłącznie na podstawie indywidualnej oceny każdego przypadku.

Przekazywanie i przetwarzanie danych PNR oraz prawa gwarantowane osobom, których dane dotyczą, muszą być zgodne z dyrektywą o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości oraz zapewniać wysoki poziom ochrony prywatności i danych osobowych, jaki przewidziano w karcie praw podstawowych, zmodernizowanej konwencji nr 108 i EKPC.

Niezależne krajowe organy nadzorcze właściwe na mocy dyrektywy o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości odpowiadają ponadto za doradztwo i monitorowanie w zakresie stosowania przepisów przyjętych przez państwa członkowskie na podstawie dyrektywy UE w sprawie danych PNR.

795 Dyrektywa (UE) 2016/681 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, Dz.U. L 119 z 4.5.2016, s. 132.

796 Dyrektywa w sprawie danych PNR, L 119, s. 132, art. 1 ust. 1 i art. 2 ust. 1.

797 Tamże, art. 12 ust. 1 i art. 12 ust. 2.

Zatrzymywanie danych telekomunikacyjnych

Dyrektywa w sprawie zatrzymywania danych[798] – uznana za nieważną 8 kwietnia 2014 r. wyrokiem w sprawie *Digital Rights Ireland* – nakładała na dostawców usług łączności obowiązek przechowywania metadanych na potrzeby szczególnych celów związanych ze zwalczaniem poważnej przestępczości przez co najmniej sześć miesięcy, ale nie dłużej niż 24 miesiące, niezależnie od tego, czy dane te nadal były dostawcy usług potrzebne do naliczania opłat lub świadczenia usługi.

Zatrzymywanie danych telekomunikacyjnych stanowi ewidentną ingerencję w prawo do ochrony danych[799]. Zasadność tej ingerencji zakwestionowano w kilku postępowaniach sądowych w państwach członkowskich UE[800].

Przykład: W sprawach *Digital Rights Ireland* i *Kärntner Landesregierung i in.*[801] grupa Digital Rights i M. Seitlinger wystąpili odpowiednio do wysokiego trybunału (High Court) w Irlandii i Trybunału Konstytucyjnego w Austrii kwestionując zgodność z prawem środków umożliwiających zatrzymywanie danych dotyczących telekomunikacji elektronicznej. Digital Rights zwróciła się do irlandzkiego trybunału o stwierdzenie nieważności dyrektywy 2006/24 oraz części krajowego prawa karnego odnoszącej się do przestępstw o charakterze terrorystycznym. Podobnie M. Seitlinger i ponad 11 000 innych skarżących zaskarżyli przepis austriackiej ustawy o telekomunikacji wdrażającej dyrektywę 2006/24 i zażądali jego unieważnienia.

Odpowiadając na te wnioski o wydanie orzeczenia w trybie prejudycjalnym, TSUE stwierdził nieważność dyrektywy w sprawie zatrzymywania danych. Zdaniem Trybunału całokształt danych, które mogły być zatrzymywane

798 Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz.U. L 105 z 13.4.2006.

799 EIOD (2011), Opinia z dnia 31 maja 2011 r. na temat sprawozdania z oceny Komisji dla Rady i Parlamentu Europejskiego w sprawie dyrektywy w sprawie zatrzymywania danych (dyrektywa 2006/24/WE), 31 maja 2011 r.

800 Niemcy, Federalny Trybunał Konstytucyjny (*Bundesverfassungsgericht*), 1 BvR 256/08, 2 marca 2010 r.; Rumunia, Federalny Trybunał Konstytucyjny (*Curtea Constituțională a României*), nr 1258, 8 października 2009 r.; Czechy, Trybunał Konstytucyjny (Ústavní soud České republiky), 94/2011 Coll., 22 marca 2011 r.

801 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in*. [WI], 8 kwietnia 2014 r., pkt 65.

zgodnie z dyrektywą, dostarczał precyzyjnych informacji na temat poszczególnych osób. Ponadto TSUE zbadał powagę ingerencji w podstawowe prawa do poszanowania życia prywatnego i ochrony danych osobowych. Trybunał stwierdził, że zatrzymywanie danych odpowiada celowi w postaci interesu ogólnego, tj. zwalczania poważnej przestępczości, a co za tym idzie – zapewniania bezpieczeństwa publicznego. Niemniej jednak TSUE zważył, że przyjmując dyrektywę, unijny prawodawca dopuścił się naruszenia zasady proporcjonalności. Choć dyrektywa może być odpowiednia do osiągnięcia tego celu, „szeroka i mocna ingerencja dyrektywy w podstawowe prawa do poszanowania prywatności i ochrony danych osobowych nie jest na tyle precyzyjne uregulowana, by zapewnić, że ingerencja ta rzeczywiście nie będzie wykraczać poza to, co ściśle niezbędne".

W obliczu braku szczegółowych przepisów dotyczących zatrzymywania danych zatrzymywanie danych jest dopuszczone w ramach wyjątku od poufności danych telekomunikacyjnych przewidzianej w dyrektywie 2002/58/WE (dyrektywa o prywatności i łączności elektronicznej)[802] jako środek zapobiegawczy, ale wyłącznie do celów zwalczania poważnej przestępczości. Takie zatrzymywanie danych musi ograniczać się do tego, co jest ściśle niezbędne pod kątem kategorii zatrzymywanych danych, środków komunikacji i osób, których ono dotyczy, oraz planowanego czasu zatrzymania. Organy krajowe mogą uzyskać dostęp do zatrzymywanych danych na ściśle określonych warunkach, w tym po uprzednim przeglądzie przez niezależny organ. Dane te muszą być zatrzymywane na terytorium UE.

Przykład: Po wydaniu wyroku w sprawach *Digital Rights Ireland* i *Kärntner Landesregierung i in.*[803] do TSUE trafiły dwie kolejne sprawy odnoszące się do ogólnego obowiązku nałożonego w Szwecji i Zjednoczonym Królestwie na podmioty świadczące usługi komunikacji elektronicznej, zgodnie z którym wymagano od nich zatrzymywania danych telekomunikacyjnych na zasadach przewidzianych w unieważnionej dyrektywie w sprawie zatrzymywania danych. W sprawach *Tele2 Sverige* oraz *Home Department*

802 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej), Dz.U. L 201 z 31.7.2002.

803 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.

przeciwko Tomowi Watsonowi i in.[804] TSUE orzekł, że przepisy krajowe, które przewidują uogólnione i niezróżnicowane zatrzymywanie danych, a nie wymagają przy tym istnienia żadnego związku między danymi, których zatrzymania się wymaga, a zagrożeniem dla bezpieczeństwa publicznego ani nie określają żadnych warunków – np. okresu zatrzymania, obszaru geograficznego, grupy osób, co do których istnieje prawdopodobieństwo zaangażowania w poważną przestępczość – wykraczają poza to, co ściśle niezbędne, i nie znajdują uzasadnienia w demokratycznym społeczeństwie, czego wymaga dyrektywa 2002/58/WE rozpatrywana w świetle Karty praw podstawowych UE.

Perspektywa

W styczniu 2017 r. Komisja Europejska opublikowała wniosek dotyczący rozporządzenia w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej, uchylającego i zastępującego dyrektywę 2002/58/WE[805]. We wniosku tym nie przewidziano żadnych konkretnych zapisów dotyczących zatrzymywania danych. Przewidziano w nim jednak możliwość prawnego ograniczenia przez państwa członkowskie niektórych obowiązków i praw wynikających z rozporządzenia, o ile takie ograniczenie stanowi niezbędny i proporcjonalny środek ochrony określonych interesów publicznych, w tym bezpieczeństwa narodowego, obrony, bezpieczeństwa publicznego, oraz zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub też wykonywania sankcji karnych[806]. Państwa członkowskie mogłyby zatem utrzymać lub stworzyć krajowe ramy zatrzymywania danych, które umożliwiałyby – między innymi – stosowanie środków ukierunkowanego zatrzymywania danych, o ile ramy te byłyby spójne z ogólnymi zasadami prawa Unii, uwzględniając przy tym orzecznictwo TSUE dotyczące wykładni dyrektywy o prywatności i łączności elektronicznej oraz Karty praw podstawowych[807]. W czasie opracowy-

804 TSUE, sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.* [WI], 21 grudnia 2016 r.

805 Komisja Europejska (2017), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final, Bruksela, 10 stycznia 2017 r.

806 Tamże, motyw 26.

807 Zob. uzasadnienie do wniosku dotyczącego rozporządzenia w sprawie prywatności i łączności elektronicznej COM(2017) 10 final, pkt 1.3.

wania niniejszego podręcznika trwały dyskusje na temat przyjęcia wspomnianego rozporządzenia.

Umowa parasolowa między UE a USA w sprawie ochrony informacji osobowych wymienianych w celach ścigania czynów zabronionych

1 lutego 2017 r. w życie weszła zawarta ze Stanami Zjednoczonymi umowa parasolowa między UE a USA w sprawie przetwarzania informacji osobowych w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych[808]. Umowa parasolowa między UE a USA ma na celu zapewnienie obywatelom UE wysokiego poziomu ochrony danych przy jednoczesnym zacieśnieniu współpracy unijnych i amerykańskich organów ścigania. Akt ten uzupełnia istniejące umowy między UE a USA oraz państwami członkowskimi a USA zawarte przez organy ścigania, a także pomaga wdrożyć przejrzyste i zharmonizowane zasady ochrony danych na potrzeby kolejnych porozumień w tej dziedzinie. W tym względzie umowa ma na celu utworzenie trwałych ram umożliwiających wymianę informacji.

Umowa sama w sobie nie jest właściwą podstawą prawną wymiany danych osobowych, gwarantuje jednak osobom fizycznym odpowiednie zabezpieczenia. Obejmuje ona wszystkie przypadki przetwarzania danych osobowych niezbędne do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych, w tym terroryzmu[809].

W umowie przewidziano wiele zabezpieczeń, które gwarantują wykorzystanie danych osobowych wyłącznie do celów określonych w umowie. W szczególności zapewnia ona obywatelom Unii ochronę w zakresie:

- ograniczenia wykorzystywania danych: dane osobowe mogą być wykorzystywane wyłącznie w celu zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych;

808 Zob. Rada UE (2016), Enhanced data protection rights for EU citizens in law enforcement cooperation: EU and US sign 'Umbrella agreement', komunikat prasowy 305/16, 2 czerwca 2016 r.

809 Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych z dnia 18 maja 2016 r., (OR. en) 8557/16, art. 3 ust. 1. Zob. także komunikat Komisji w sprawie negocjacji umowy między UE i USA w sprawie ochrony danych z 26 maja 2010 r., MEMO/10/216 oraz komunikat prasowy Komisji Europejskiej (2010) o wysokich standardach prywatności w umowie między UE i USA w sprawie ochrony danych z dnia 26 maja 2010 r., IP/10/609.

- ochrony przed arbitralną i nieuzasadnioną dyskryminacją;

- dalszego przekazywania informacji: wszelkie dalsze przekazywanie informacji do państwa innego niż USA lub państwa nienależącego do UE bądź do organizacji międzynarodowej wymaga uprzedniej zgody właściwego organu w państwie, które pierwotnie przekazało dane;

- jakości danych: dane osobowe muszą być utrzymywane z zachowaniem ich prawidłowości, odpowiedniości, terminowości i kompletności;

- bezpieczeństwa przetwarzania, w tym powiadamiania o naruszeniach ochrony danych osobowych;

- przetwarzania danych szczególnie chronionych – może się ono odbywać wyłącznie przy zagwarantowaniu odpowiednich zabezpieczeń przewidzianych prawem;

- okresów zatrzymywania informacji: danych osobowych nie można zatrzymywać przez okres dłuższy niż to konieczne i stosowne;

- prawa dostępu i prawa do sprostowania: każdej osobie fizycznej przysługuje prawo dostępu do swoich danych osobowych, z zastrzeżeniem określonych warunków, i każda taka osoba będzie miała możliwość zażądania poprawienia danych, jeżeli są one nieprawidłowe;

- decyzji zautomatyzowanych – wymagają one zastosowania odpowiednich zabezpieczeń, w tym możliwości interwencji człowieka;

- skutecznego nadzoru uwzględniającego współpracę między unijnymi i amerykańskimi organami nadzoru; oraz

- sądowych środków zaskarżania i możliwości dochodzenia praw: Obywatele Unii mają prawo[810] korzystać z sądowych środków zaskarżania przed sądami USA, jeżeli organy tego kraju odmówią im dostępu do ich danych lub ich sprostowania bądź ujawnią ich dane osobowe w sposób niezgodny z prawem.

810 Prezydent Obama podpisał ustawę o sądowych środkach zaskarżenia (US Judicial Redress Act) 24 lutego 2016 r.

W „umowie parasolowej" ustanowiono ponadto system powiadamiania – w razie potrzeby – o naruszeniach ochrony danych właściwego organu nadzorczego w państwie członkowskim osoby, której dotyczy naruszenie. Gwarancje prawne przewidziane w umowie zapewniają równe traktowanie obywateli UE w USA w przypadku naruszenia ochrony prywatności[811].

8.3.1. Ochrona danych w organach sądowych i organach ścigania UE

Europol

Europol, czyli organ ścigania UE, ma siedzibę w Hadze, natomiast jego jednostki krajowe (ENU) znajdują się w każdym państwie członkowskim. Europol ustanowiono w 1998 r., a jego obecny status prawny jako instytucji UE opiera się na rozporządzeniu w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (rozporządzenie w sprawie Europolu)[812]. Europol ma na celu pomoc w zapobieganiu przestępczości zorganizowanej, terroryzmowi i innym formom poważnej przestępczości, które wymieniono w załączniku I do rozporządzenia w sprawie Europolu, i które dotyczą co najmniej dwóch państw członkowskich, jak też w prowadzeniu dochodzeń w powyższych sprawach. Europol osiąga te cele poprzez wymianę informacji i działanie w charakterze centrum informacyjnego UE, a także dostarczanie analiz danych wywiadowczych i ocen zagrożenia.

Aby osiągnąć swoje cele, Europol ustanowił system informacyjny Europolu, który udostępnia państwom członkowskim bazę danych służącą wymianie danych wywiadowczych w sprawach karnych oraz informacji za pośrednictwem jednostek krajowych. System informacyjny Europolu może być wykorzystywany w celu udostępniania danych odnoszących się do: osób, które są podejrzane o popełnienie przestępstwa lub zostały skazane za popełnienie przestępstwa podlegającego

811 Europejski Inspektor Ochrony Danych wydał opinię na temat umowy między UE i USA, w której zalecił między innymi wprowadzenie następujących zmian: 1) dodanie słów „w konkretnych celach, dla których zostały przekazane" do artykułu poświęconego zatrzymywaniu danych dłużej niż to konieczne i odpowiednie oraz 2) wyłączenie masowego przekazywania danych szczególnie chronionych, które może być dozwolone. Zob. Europejski Inspektor Ochrony Danych, Opinia 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*, pkt 35.

812 Rozporządzenie (UE) 2016/794 Parlamentu Europejskiego i Rady z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW, Dz.U. L 135 z 24.5.2016, s. 53.

kompetencjom Europolu, bądź osób, w przypadku których istnieją przesłanki faktyczne, by sądzić, że popełnią one takie przestępstwa. Europol i jego jednostki krajowe mogą wprowadzać dane bezpośrednio do systemu informacyjnego Europolu oraz pobierać dane z tego systemu. Tylko strona, która wprowadziła dane do systemu, może je zmieniać, korygować lub usuwać. Organy UE, państwa trzecie i organizacje międzynarodowe również mogą dostarczać dane Europolowi.

Europol może także pozyskiwać informacje, w tym dane osobowe, ze źródeł powszechnie dostępnych, na przykład z Internetu. Przekazywanie danych osobowych organom Unii jest dopuszczone wyłącznie wówczas, gdy jest to niezbędne do wykonywania zadań Europolu lub organu UE będącego odbiorcą danych. Przekazywanie danych osobowych państwom trzecim i organizacjom międzynarodowym jest możliwe wyłącznie w przypadku, gdy Komisja Europejska uzna, że dane państwo lub dana organizacja międzynarodowa zapewnia odpowiedni poziom ochrony (na podstawie „decyzji stwierdzającej odpowiedni poziom ochrony"), bądź gdy zawarto umowę międzynarodową lub umowę o współpracy. Europol może otrzymywać i przetwarzać dane pochodzące od osób i podmiotów prywatnych z tym wyraźnym zastrzeżeniem, że dane te zostały przekazane przez ENU zgodnie z prawem krajowym, przez punkt kontaktowy w państwie trzecim lub organizacji międzynarodowej, z którymi Europol współpracuje na mocy umowy o współpracy, lub przez organ państwa trzeciego lub organizacji międzynarodowej, w odniesieniu do których wydano decyzję stwierdzającą odpowiedni poziom ochrony lub z którymi EU zawarła umowę międzynarodową. Wymiana informacji odbywa się zawsze za pośrednictwem aplikacji sieci bezpiecznej wymiany informacji (SIENA).

W reakcji na zachodzące zmiany w Europolu utworzono wyspecjalizowane ośrodki. W 2013 r. w ramach Europolu ustanowiono Europejskie Centrum ds. Walki z Cyberprzestępczością[813]. Pełni ono rolę unijnego węzła informacyjnego w zakresie danych o cyberprzestępczości, przyczyniając się do szybszej reakcji na przestępstwa internetowe, opracowania i wdrożenia cyfrowych technik kryminalistycznych oraz wypracowania najlepszych praktyk w zakresie dochodzeń dotyczących cyberprzestępczości. Centrum skupia się na cyberprzestępczości:

- którą zajmują się zorganizowane grupy w celu osiągania dużych zysków z przestępstw, takiej jak oszustwa internetowe;

813 Zob. także EIOD (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, Bruksela, 29 czerwca 2012 r.

- która skutkuje poważnymi szkodami dla ofiar, takiej jak wykorzystywanie seksualne dzieci w Internecie;

- która ma wpływ na krytyczną infrastrukturę i systemy informacyjne w UE.

W styczniu 2016 r. utworzono Europejskie Centrum ds. Zwalczania Terroryzmu (ECTC), którego zadaniem jest udzielanie państwom członkowskim wsparcia operacyjnego przy prowadzeniu dochodzeń związanych z przestępstwami o charakterze terrorystycznym. Centrum sprawdza krzyżowo pozyskiwane na bieżąco dane operacyjne na tle danych, którymi Europol już dysponuje, umożliwiając szybką identyfikację źródeł finansowania, oraz analizuje wszystkie dostępne dane wywiadowcze, aby pomóc w nakreśleniu uporządkowanego obrazu sieci terrorystycznej[814].

Europejskie Centrum Zwalczania Przemytu Migrantów utworzono w lutym 2016 r. w następstwie posiedzenia Rady z listopada 2015 r. Ma ono na celu wspieranie państw członkowskich w podejmowaniu ukierunkowanych działań przeciwko sieciom przestępczym zajmującym się przemytem migrantów oraz rozbijaniu takich sieci. Stanowi ono centrum wymiany informacji wspierające biura regionalnych grup zadaniowych Unii Europejskiej w Katanii (Włochy) i Pireusie (Grecja), które udzielają organom krajowym pomocy w kilku obszarach, między innymi wymiany danych wywiadowczych, prowadzenia śledztw i ścigania siatek przestępczych zajmujących się przemytem ludzi[815].

System ochrony danych regulujący działania Europolu opiera się na zasadach przewidzianych w rozporządzeniu o ochronie danych przez instytucje UE[816] oraz jest zgodny z dyrektywą o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości, zaktualizowaną konwencją nr 108 i rekomendacją dotyczącą policji.

Przetwarzanie danych osobowych dotyczących ofiar przestępstw, świadków lub innych osób, które mogą dostarczać informacji na temat przestępstw, oraz osób poniżej 18. roku życia dopuszcza się wyłącznie wówczas, gdy jest to absolutnie niezbędne i proporcjonalne do zapobiegania przestępczości objętej celami Europolu lub

814 Zob. strona internetowa Europolu poświęcona ECTC.

815 Zob. strona internetowa Europolu poświęcona Europejskiemu Centrum Zwalczania Przemytu Migrantów.

816 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

do jej zwalczania[817]. Przetwarzanie danych szczególnie chronionych jest zabronione, chyba że jest to absolutnie niezbędne i proporcjonalne do zapobiegania przestępczości objętej celami Europolu lub do jej zwalczania oraz gdy dane takie uzupełniają inne dane osobowe przetwarzane przez Europol[818]. W obu przypadkach do danych dostęp ma wyłącznie Europol[819].

Dane mogą być przechowywane nie dłużej niż jest to niezbędne i proporcjonalne, a konieczność ich dalszego przechowywania jest weryfikowana co trzy lata. W przypadku braku decyzji o dalszym przechowywaniu danych są one automatycznie usuwane[820].

Europol może, w określonych okolicznościach, przekazywać dane osobowe organowi Unii lub organowi państwa trzeciego bądź bezpośrednio organizacji międzynarodowej[821]. O naruszeniach ochrony danych, które mogą w sposób istotny negatywnie wpłynąć na prawa i wolności osób, których dane dotyczą, należy bez zbędnej zwłoki zawiadomić te osoby[822]. Na szczeblu państw członkowskich zostaną wyznaczone krajowe organy nadzorcze, których zadaniem będzie monitorowanie przetwarzania danych osobowych przez Europol[823].

EIOD jest odpowiedzialny za monitorowanie i zapewnianie ochrony podstawowych praw i wolności osób fizycznych w zakresie przetwarzania danych osobowych przez Europol oraz za doradzanie Europolowi i osobom, których dane dotyczą, we wszelkich sprawach związanych z przetwarzaniem danych osobowych. W tym celu wykonuje on obowiązki organu badającego i przyjmującego skargi oraz działa w ścisłej współpracy z krajowymi organami nadzorczymi[824]. EIOD i krajowe organy nadzorcze będą się zbierać co najmniej dwa razy w roku w ramach Rady Współpracy, pełniącej funkcję doradczą[825]. Państwa członkowskie mają obowiązek z mocy ustawy powołać organ nadzorczy, którego zadaniem jest monitorowanie dopuszczalności przekazywania, pobierania i wszelkiego rodzaju udostępniania przez dane państwo

817 Rozporządzenie w sprawie Europolu, art. 30 ust. 1.
818 Tamże, art. 30 ust. 2.
819 Tamże, art. 30 ust. 3.
820 Tamże, art. 31.
821 Tamże, odpowiednio art. 24 i art. 25.
822 Tamże, art. 35.
823 Rozporządzenie w sprawie Europolu, art. 42.
824 Tamże, art. 43 i art. 44.
825 Tamże, art. 45.

członkowskie danych osobowych do Europolu[826]. Państwa członkowskie mają ponadto obowiązek zapewnić krajowemu organowi nadzorczemu możliwość w pełni niezależnego wykonywania jego zadań i obowiązków wynikających z rozporządzenia w sprawie Europolu[827]. Do celów weryfikacji zgodności z prawem przetwarzania danych, samodzielnego monitorowania swoich działań i zapewniania właściwej integralności i bezpieczeństwa danych Europol prowadzi rejestry lub dokumentację działań związanych z przetwarzaniem danych osobowych. Takie rejestry zawierają informacje o operacjach przetwarzania w zautomatyzowanych systemach przetwarzania, dotyczące zbierania, modyfikowania, przeglądania, ujawniania, łączenia, usuwania danych osobowych[828].

Odwołanie od decyzji EIOD można wnieść do TSUE[829]. Każdy, kto poniósł szkodę w wyniku niezgodnego z prawem przetwarzania danych, ma prawo do uzyskania odszkodowania od Europolu lub odpowiedzialnego państwa członkowskiego, w którym to celu może wnieść pozew do TSUE w pierwszym przypadku lub do właściwego sądu krajowego w drugim przypadku[830]. Co więcej, działania Europolu może kontrolować grupa ds. wspólnej kontroli parlamentarnej (GWKP), utworzona wspólnie przez parlamenty narodowe i Parlament Europejski[831]. Każdej osobie fizycznej przysługuje prawo dostępu do wszelkich danych osobowych na swój temat, jakimi Europol może dysponować, a także prawo żądania sprawdzenia, sprostowania lub usunięcia takich danych. W odniesieniu do tych praw mogą obowiązywać wyjątki i ograniczenia.

Eurojust

Ustanowiony w 2002 r. Eurojust jest organem UE z siedzibą w Hadze. Wspiera współpracę sądową w ramach dochodzeń i postępowań w sprawie poważnych

826 Tamże, art. 42 ust. 1.
827 Tamże, art. 42 ust. 1.
828 Tamże, art. 40.
829 Tamże, art. 48.
830 Tamże, art. 50.
831 Tamże, art. 51.

przestępstw dotyczących co najmniej dwóch państw członkowskich[832]. Do właściwości Eurojustu należy:

- stymulowanie i usprawnianie koordynacji dochodzeń oraz postępowań między właściwymi organami sądowymi poszczególnych państw członkowskich;

- ułatwianie wykonywania wniosków i decyzji dotyczących współpracy sądowej.

Zadania Eurojustu wykonują członkowie wyznaczeni przez kraje. Każde państwo członkowskie deleguje do Eurojustu sędziego lub prokuratora, którego status jest określony w prawie krajowym i który dysponuje niezbędnymi kompetencjami do wykonywania czynności niezbędnych w celu stymulowania oraz usprawniania współpracy sądowej. Dodatkowo członkowie krajowi działają wspólnie jako kolegium, wykonując zadania specjalne Eurojustu.

Eurojust może przetwarzać dane osobowe w zakresie niezbędnym do osiągnięcia jego celów. Zakres przetwarzania jest jednak ograniczony do konkretnych informacji na temat osób podejrzanych o popełnienie przestępstwa lub udział w przestępstwie bądź skazanych za przestępstwo podlegające kompetencjom Eurojustu. Eurojust może także przetwarzać określone informacje dotyczące świadków lub ofiar przestępstw podlegających jego kompetencjom[833]. W wyjątkowych przypadkach Eurojust może także, przez ograniczony czas, przetwarzać szerszy zakres danych osobowych odnoszących się do okoliczności przestępstwa, gdy dotyczą one bezpośrednio trwającego dochodzenia. W ramach swoich kompetencji Eurojust może współpracować z innymi instytucjami, organami i agencjami UE oraz wymieniać z nimi dane osobowe. Eurojust może również współpracować z państwami trzecimi i organizacjami oraz wymieniać z nimi dane osobowe.

W odniesieniu do ochrony danych Eurojust musi zagwarantować poziom ochrony co najmniej równoważny określonemu w zaktualizowanej konwencji nr 108

832 Rada Unii Europejskiej (2002), Decyzja Rady 2002/187/WSiSW z dnia 28 lutego 2002 r. ustanawiająca Eurojust w celu zintensyfikowania walki z poważną przestępczością, Dz.U. L 63 z 6.3.2002; Rada Unii Europejskiej (2003), Decyzja Rady 2003/659/WSiSW z dnia 18 czerwca 2003 r. zmieniająca decyzję 2002/187/WSiSW ustanawiającą Eurojust w celu zintensyfikowania walki z poważną przestępczością, Dz.U. L 44 z 29.9.2003; Rada Unii Europejskiej (2009), Decyzja Rady 2009/426/WSiSW z dnia 16 grudnia 2008 r. w sprawie wzmocnienia Eurojustu i w sprawie zmiany decyzji 2002/187/WSiSW ustanawiającej Eurojust w celu zintensyfikowania walki z poważną przestępczością, Dz.U. L 138 z 4.6.2009 (Decyzje w sprawie Eurojustu).

833 Wersja skonsolidowana decyzji Rady 2002/187/WSiSW zmienionej decyzją Rady 2003/659/WSiSW oraz decyzją Rady 2009/426/WSiSW, art. 15 ust. 2.

z późniejszymi zmianami. W przypadku wymiany danych przestrzegane muszą być szczegółowe reguły i ograniczenia określone w umowie o współpracy lub w uzgodnieniach roboczych zgodnie z decyzjami Rady w sprawie Eurojustu oraz regulaminem ochrony danych Eurojustu[834].

W ramach Eurojustu ustanowiono niezależny wspólny organ nadzorczy, którego zadaniem jest monitorowanie prowadzonego przez Eurojust przetwarzania danych osobowych. Osoby fizyczne mogą odwołać się do wspólnego organu nadzorczego, jeżeli uznają odpowiedź Eurojustu na wniosek o dostęp, poprawienie, zablokowanie lub usunięcie danych osobowych za niezadowalającą. W przypadku niezgodnego z prawem przetwarzania danych osobowych Eurojust odpowiada zgodnie z prawem krajowym państwa członkowskiego, w którym mieści się jego siedziba, czyli Niderlandów, za wszelkie szkody wyrządzone osobie, której dane dotyczą.

Perspektywa

W lipcu 2013 r. Komisja Europejska przedłożyła wniosek dotyczący rozporządzenia w sprawie reformy Eurojustu. Towarzyszył mu wniosek w sprawie ustanowienia Prokuratury Europejskiej (zob. poniżej). Przedmiotowe rozporządzenie ma na celu usprawnienie funkcjonowania i struktury Eurojustu zgodnie z Traktatem z Lizbony. Reforma ma też na celu wyraźne rozdzielenie działalności operacyjnej Eurojustu, wykonywanej przez Kolegium Eurojustu, i jego zadań administracyjnych. Umożliwi również państwom członkowskim poświęcenie większej uwagi zadaniom operacyjnym. Zostanie ustanowiony nowy zarząd, którego funkcją będzie wspieranie kolegium w wykonywaniu zadań administracyjnych[835].

Prokuratura Europejska

Państwa członkowskie dysponują wyłącznymi kompetencjami w zakresie ścigania przestępstw oszustwa i niewłaściwego wykonywania budżetu UE, które mogą mieć również wymiar transgraniczny. Znaczenie dochodzenia, ścigania i stawiania przed sądem sprawców takich przestępstw rośnie, zwłaszcza w świetle trwającego kryzysu gospodarczego[836]. Komisja Europejska przedłożyła wniosek dotyczący roz-

834 Przepisy regulaminu wewnętrznego Eurojustu dotyczące przetwarzania i ochrony danych osobowych, 19 marca 2005 r., Dz.U. C 68 z 19.3.2005, s. 1.

835 Zob. strona internetowa Komisji Europejskiej dotycząca Eurojustu.

836 Zob. Komisja Europejska (2013), Wniosek dotyczący rozporządzenia Rady w sprawie ustanowienia Prokuratury Europejskiej, COM(2013) 534 final, Bruksela, 17 lipca 2013 r., s. 1 oraz strona internetowa Komisji dotycząca EPPO.

porządzenia w sprawie ustanowienia niezależnej Prokuratury Europejskiej (EPPO), która ma na celu zwalczanie przestępstw przeciwko interesom finansowym Unii[837]. EPPO będzie ustanawiana w ramach procedury wzmocnionej współpracy, która umożliwia grupie co najmniej dziewięciu państw członkowskich podjęcie rozbudowanej współpracy w jednej z dziedzin objętych przez struktury UE bez udziału pozostałych państw członkowskich[838]. Belgia, Bułgaria, Chorwacja, Cypr, Czechy, Estonia, Finlandia, Francja, Niemcy, Grecja, Łotwa, Litwa, Luksemburg, Portugalia, Rumunia, Słowenia, Słowacja i Hiszpania przystąpiły do wzmocnionej współpracy, natomiast Austria i Włochy wyraziły taki zamiar[839].

EPPO będzie miała kompetencje do prowadzenia dochodzeń i postępowań karnych w sprawach nadużyć finansowych w UE i innych przestępstw godzących w interesy finansowe Unii z myślą o skutecznej koordynacji dochodzeń i postępowań w różnych krajowych porządkach prawnych oraz usprawnieniu korzystania z zasobów i wymiany informacji na szczeblu europejskim[840].

Na czele EPPO będzie stał Prokurator Europejski, a w każdym państwie członkowskim prowadzeniem dochodzeń i postępowań będzie kierował co najmniej jeden delegowany prokurator europejski.

We wniosku ustanowiono silne zabezpieczenia gwarantujące prawa osób biorących udział w dochodzeniu prowadzonym przez EPPO przewidziane w prawie krajowym, prawie Unii i Karcie praw podstawowych UE. Czynności dochodzeniowe, które w największej mierze dotykają sfery praw podstawowych, będą wymagały uprzedniego zatwierdzenia przez sąd krajowy[841]. Dochodzenia EPPO będą podlegały kontroli sądowej dokonywanej przez sądy krajowe[842].

837 Komisja Europejska (2013), Wniosek dotyczący rozporządzenia Rady w sprawie ustanowienia Prokuratury Europejskiej, COM(2013) 534 final, Bruksela, 17 lipca 2013 r.

838 Traktat o funkcjonowaniu Unii Europejskiej, art. 86 ust. 1 i art. 329 ust. 1.

839 Zob. Rada Unii Europejskiej (2017), *20 państw członkowskich uzgodniło szczegóły działania Prokuratury Europejskiej*, komunikat prasowy, 8 czerwca 2017 r.

840 Komisja Europejska (2013), Wniosek dotyczący rozporządzenia Rady w sprawie ustanowienia Prokuratury Europejskiej, COM(2013) 534 final, Bruksela, 17 lipca 2013 r., s. 1 i 51–51. Zob. strona internetowa Komisji dotycząca EPPO.

841 Komisja Europejska (2013), Wniosek rozporządzenie Rady w sprawie ustanowienia Prokuratury Europejskiej, COM(2013) 534 final, Bruksela, 17 lipca 2013 r., art. 26 ust. 4.

842 Tamże, art. 36.

Rozporządzenie w sprawie ochrony danych przez instytucje UE[843] będzie miało zastosowanie do przetwarzania administracyjnych danych osobowych przez EPPO. Jeżeli chodzi o przetwarzanie danych osobowych w związku z działaniami operacyjnymi, w EPPO – podobnie jak w Europolu – będzie obowiązywał system ochrony danych zbliżony do systemu regulującego działania Europolu i Eurojustu, ponieważ wykonywanie funkcji EPPO będzie wymagało wymiany danych osobowych z organami ścigania i egzekwowania prawa na poziomie państw członkowskich. Zasady ochrony danych w EPPO są zatem niemal identyczne z przewidzianymi w dyrektywie o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości. W myśl wniosku w sprawie ustanowienia EPPO przetwarzanie danych osobowych musi przebiegać z poszanowaniem zasad zgodności z prawem i rzetelności, ograniczenia celu, minimalizacji danych, prawidłowości, integralności i poufności. Prokuratura Europejska musi w maksymalnym możliwym zakresie dokonywać jasnego rozróżnienia między danymi osobowymi różnych kategorii osób, których dane dotyczą, na przykład osób skazanych za przestępstwa, osób, które są zaledwie podejrzanymi, ofiar i świadków. EPPO musi ponadto dążyć do weryfikacji przetwarzanych danych osobowych oraz rozróżniania – na tyle, na ile to możliwe – danych osobowych opartych na faktach i danych bazujących na indywidualnych ocenach.

Wniosek zawiera zapisy dotyczące praw osób, których dane dotyczą, zwłaszcza prawa do informacji, dostępu do swoich danych osobowych, poprawienia, usunięcia danych i ograniczenia ich przetwarzania, oraz przewiduje, że takie prawa można wykonywać również pośrednio, za pośrednictwem EIOD. Obejmuje on ponadto zasady bezpieczeństwa przetwarzania i rozliczalności, gdyż wymaga od EPPO wdrożenia odpowiednich środków technicznych i organizacyjnych z myślą o zapewnieniu poziomu ochrony stosownego do ryzyka związanego z przetwarzaniem, prowadzenia rejestrów wszystkich czynności przetwarzania oraz dokonywania ocen skutków dla ochrony danych przed rozpoczęciem przetwarzania, jeżeli typ przetwarzania (przykładowo przetwarzanie z wykorzystaniem nowych technologii) może skutkować wysokim ryzykiem dla praw osób fizycznych. Ponadto wniosek przewiduje powołanie przez kolegium inspektora ochrony danych, którego należy właściwie włączyć we wszystkie sprawy dotyczące ochrony danych osobowych oraz który musi dbać o przestrzeganie przez EPPO wszystkich stosownych przepisów z zakresu ochrony danych.

843 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

8.3.2. Ochrona danych we wspólnych systemach informacyjnych na szczeblu UE

Oprócz wymiany danych między państwami członkowskimi i utworzenia organów UE wyspecjalizowanych w zwalczaniu przestępczości transgranicznej, takich jak Europol, Eurojust i EPPO, na szczeblu UE ustanowiono pewną liczbę wspólnych systemów informacyjnych mających na celu umożliwienie i ułatwienie współpracy i wymiany danych między właściwymi organami krajowymi i unijnymi w określonych celach w dziedzinie ochrony granic, prawa imigracyjnego i azylowego, oraz celnego. Gdy zawarto międzynarodowe, niezależne od UE porozumienie o utworzeniu strefy Schengen, na podstawie wielostronnych umów opracowano System Informacyjny Schengen (SIS), który został następnie włączony w ramy prawne UE. Wizowy system informacyjny (VIS), Eurodac, Eurosur i system informacji celnej (CIS) zostały utworzone jako instrumenty regulowane prawem Unii.

Nadzór nad tymi systemami sprawują wspólnie krajowe organy nadzorcze i EIOD. Aby zagwarantować wysoki poziom ochrony, organy te współpracują w ramach grup ds. koordynowania nadzoru nad następującymi wielkoskalowymi systemami informatycznymi: 1) Eurodac; 2) wizowy system informacyjny; 3) System Informacyjny Schengen; 4) system informacji celnej i 5) system wymiany informacji na rynku wewnętrznym[844]. Grupy ds. koordynowania nadzoru zazwyczaj spotykają się dwa razy w roku pod kierownictwem wybranego przewodniczącego i przyjmują wytyczne, omawiają sprawy o wymiarze transgranicznym bądź przyjmują wspólne ramy kontroli.

Powołana w 2012 r. Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi (eu-LISA)[845] odpowiada za zarządzanie operacyjne systemem informacyjnym Schengen drugiej generacji (SIS II), wizowym systemem informacyjnym (VIS) i systemem Eurodac. Podstawowym zadaniem eu-LISA jest zapewnienie skutecznego, bezpiecznego i nieprzerwanego działania systemów informatycznych. Agencja jest też odpowiedzialna za przyjęcie niezbędnych środków w celu zapewnienia bezpieczeństwa systemów i danych.

844 Zob. strona internetowa Europejskiego Inspektora Ochrony Danych dotycząca koordynacji nadzoru.

845 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1077/2011 z dnia 25 października 2001 r. ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.U. L 286 z 1.11.2011.

System Informacyjny Schengen

W 1985 r. część państw członkowskich ówczesnych Wspólnot Europejskich zawarła Układ między rządami państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec i Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach (układ z Schengen), mając na celu stworzenie przestrzeni swobodnego przepływu osób bez przeszkód w postaci kontroli granicznych na terytorium Schengen[846]. Aby zrównoważyć zagrożenie dla bezpieczeństwa publicznego, które mogłoby wyniknąć z otwartych granic, wzmocniono kontrole graniczne na granicach zewnętrznych strefy Schengen, a także zacieśniono współpracę krajowych organów policji i wymiaru sprawiedliwości.

W rezultacie przystąpienia do układu z Schengen dodatkowych państw system Schengen ostatecznie włączono w ramy prawne UE na mocy traktatu z Amsterdamu[847]. Decyzję tę wprowadzono w życie w 1999 r. Najnowsza wersja Systemu Informacyjnego Schengen, tzw. SIS II, weszła do eksploatacji 9 kwietnia 2013 r. Obsługuje ona wszystkie państwa członkowskie UE[848] oraz Islandię, Liechtenstein, Norwegię i Szwajcarię[849]. Do SIS II dostęp mają także Europol i Eurojust.

SIS II składa się z systemu centralnego (C-SIS), systemu krajowego (N-SIS) w każdym państwie członkowskim oraz infrastruktury komunikacyjnej łączącej system centralny z systemami krajowymi. System C-SIS zawiera pewne dane wprowadzone przez państwa członkowskie na temat osób i przedmiotów. SIS jest wykorzystywany przez krajowe organy kontroli granicznej, policyjne, celne, wizowe i sądowe w całej strefie Schengen. Każde z państw członkowskich eksploatuje krajową kopię C-SIS. Kopie te są znane jako krajowe systemy informacyjne Schengen (N-SIS) i są stale aktualizowane, co skutkuje aktualizacją C-SIS. W SIS występują różne rodzaje wpisów:

---

846 Układ między Rządami Państw Unii Gospodarczej Beneluksu, Republiki Federalnej Niemiec oraz Republiki Francuskiej w sprawie stopniowego znoszenia kontroli na wspólnych granicach, Dz.U. L 239 z 22.9.2000.

847 Wspólnoty Europejskie (1997), Traktat z Amsterdamu zmieniający Traktat o Unii Europejskiej, Traktaty ustanawiające Wspólnoty Europejskie i niektóre związane z nimi akty, Dz.U. C 340 z 10.11.1997.

848 Chorwacja i Cypr przygotowują się do integracji z SIS II, ale nie są jeszcze jego częścią. Zob. informacje na temat Systemu Informacyjnego Schengen dostępne na stronie internetowej Dyrekcji Generalnej Komisji Europejskiej ds. Migracji i Spraw Wewnętrznych.

849 Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 381 z 28.12.2006 i decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 205 z 7.8.2007.

- dana osoba nie ma prawa wjazdu lub pobytu na terytorium strefy Schengen; lub
- dana osoba lub dany przedmiot są poszukiwane przez organy sądowe bądź ścigania (np. europejskie nakazy aresztowania, wnioski o kontrolę niejawną); lub
- zgłoszono zaginięcie danej osoby; lub
- zgłoszono kradzież lub zaginięcie przedmiotów, takich jak banknoty, samochody osobowe, furgonetki, broń palna i dokumenty tożsamości.

W przypadku wpisu za pośrednictwem biur SIRENE inicjowane są działania następcze. SIS II udostępnia nowe funkcje, takie jak możliwość wprowadzenia: danych biometrycznych, takich jak odciski palców i fotografie; lub nowych kategorii wpisów, np. skradzionych łodzi, samolotów, pojemników lub środków płatniczych; oraz rozszerzonych wpisów dotyczących osób i przedmiotów; kopii europejskich nakazów aresztowania, dotyczących osób poszukiwanych w celu aresztowania, wydania lub ekstradycji.

SIS II opiera się na dwóch uzupełniających się wzajemnie aktach: decyzji w sprawie SIS II[850] i rozporządzeniu w sprawie SIS II[851]. Na potrzeby przyjęcia decyzji i rozporządzenia prawodawca UE skorzystał z różnych podstaw prawnych. Decyzja reguluje wykorzystanie SIS II do celów związanych ze współpracą policyjną i współpracą wymiarów sprawiedliwości w sprawach karnych (wcześniej trzeci filar UE). Rozporządzenie zaś odnosi się do procedur wpisów z dziedziny polityki wizowej, azylowej i imigracyjnej oraz innych obszarów polityki związanych ze swobodnym przepływem osób (wcześniej pierwszy filar). Procedury wpisów dla każdego z filarów wymagały uregulowania za pomocą odrębnych aktów prawnych, ponieważ oba instrumenty przyjęto przed zawarciem Traktatu z Lizbony i zniesieniem struktury opartej na filarach.

Oba akty prawne zawierają przepisy z zakresu ochrony danych. Decyzja w sprawie SIS II przewiduje zakaz przetwarzania danych szczególnie chronionych[852]. Przetwarzanie danych osobowych jest objęte zakresem zaktualizowanej konwencji

850 Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 205, z 7.8.2007.

851 Rozporządzenie (WE) nr 1987/2006 Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (SIS II), Dz.U. L 381 z 28.12.2006.

852 Decyzja w sprawie SIS II, art. 56; rozporządzenie w sprawie SIS II, art. 40.

nr 108[853]. Ponadto osoby mają prawo dostępu do dotyczących ich danych osobowych wprowadzonych do systemu SIS II[854].

Rozporządzenie w sprawie SIS II reguluje warunki i procedury dokonywania i przetwarzania wpisów dotyczących odmowy pozwolenia na wjazd lub pobyt obywateli państw trzecich. W akcie tym przewidziano też zasady wymiany uzupełniających i dodatkowych informacji do celów wjazdu lub pobytu na terytorium państwa członkowskiego[855]. Rozporządzenie zawiera też przepisy dotyczące ochrony danych. Wrażliwe kategorie danych, o których mowa w art. 9 ust. 1 ogólnego rozporządzenia o ochronie danych, nie mogą być przetwarzane[856]. Rozporządzenie w sprawie SIS II przewiduje również określone prawa osób, których dane dotyczą. Do praw tych należą:

- prawo osób, których dane dotyczą, do dostępu do ich danych osobowych[857];
- prawo do poprawienia danych niezgodnych ze stanem faktycznym[858];
- prawo do usunięcia danych przechowywanych z naruszeniem prawa[859];
- prawo do informacji o dokonaniu wpisu na temat osoby, której dane dotyczą. Informacje te są przekazywane na piśmie wraz z kopią lub odesłaniem do decyzji krajowej, która stanowi podstawę dokonania wpisu[860].

Prawo do informacji nie jest zapewniane, jeżeli 1) dane osobowe nie zostały uzyskane od osoby, której dane dotyczą, oraz przekazanie tych informacji okazuje się niemożliwe lub wymagałoby nieproporcjonalnego nakładu pracy; 2) osoba, której dane dotyczą, dysponuje już tymi informacjami; lub 3) prawo krajowe pozwala ograniczyć prawo do informacji, między innymi ze względu na ochronę bezpieczeństwa narodowego lub w celu przeciwdziałania przestępstwom[861].

853 Decyzja w sprawie SIS II, art. 57.
854 Decyzja w sprawie SIS II, art. 58; rozporządzenie w sprawie SIS II, art. 41.
855 Rozporządzenie w sprawie SIS II, art. 2.
856 Tamże, art. 40.
857 Tamże, art. 41 ust. 1.
858 Tamże, art. 41 ust. 5.
859 Tamże, art. 41 ust. 5.
860 Tamże, art. 42 ust. 1.
861 Tamże, art. 42 ust. 2.

Zarówno w przypadku decyzji w sprawie SIS II, jak i przedmiotowego rozporządzenia prawo dostępu osób fizycznych do danych wprowadzonych do SIS II może być wykonywane w dowolnym państwie członkowskim i jest rozpatrywane zgodnie z prawem tego państwa[862].

> Przykład: W sprawie *Dalea przeciwko Francji*[863] skarżącemu odmówiono wizy wjazdowej do Francji, a władze francuskie zamieściły w Systemie Informacyjnym Schengen wpis stwierdzający, że należy odmówić mu wjazdu. Skarżący bezskutecznie starał się o dostęp i sprostowanie lub usunięcie danych w postępowaniu przed francuską komisją ds. ochrony danych, a ostatecznie przed Radą Stanu. ETPC uznał, że zamieszczenie wpisu o skarżącym w Systemie Informacyjnym Schengen było zgodne z prawem i służyło uzasadnionemu celowi ochrony bezpieczeństwa narodowego. Ponieważ skarżący nie wykazał, jaką faktyczną szkodę poniósł w wyniku odmowy wjazdu do strefy Schengen, a wdrożone środki chroniące go przed arbitralnymi decyzjami były wystarczające, ingerencja w jego prawo do poszanowania życia prywatnego była proporcjonalna. Tym samym skargę skarżącego na podstawie art. 8 uznano za niedopuszczalną.

Krajowy N-SIS w każdym państwie członkowskim nadzoruje właściwy krajowy organ nadzorczy. Krajowy organ nadzorczy musi zapewnić przeprowadzenie co najmniej raz na cztery lata audytu czynności przetwarzania danych w krajowym N-SIS[864]. Krajowe organy nadzorcze oraz EIOD współpracują i zapewniają skoordynowany nadzór nad N-SIS, podczas gdy EIOD jest odpowiedzialny za nadzór nad C-SIS. Aby zapewnić przejrzystość, wspólne sprawozdanie z ich działalności musi być przesyłane co dwa lata Parlamentowi Europejskiemu, Radzie i eu-LISA. Grupa ds. koordynowania nadzoru nad SIS II została stworzona z myślą o zapewnieniu koordynacji nadzoru nad SIS i spotyka się dwa razy w roku. Do grupy należą EIOD oraz przedstawiciele organów nadzorczych państw członkowskich, które wdrożyły SIS II, a także Islandii, Liechtensteinu, Norwegii i Szwajcarii. SIS obejmuje również te państwa, ponieważ należą one do Schengen[865]. Cypr, Chorwacja i Irlandia nie należą jeszcze do SIS II, zatem uczestniczą w grupie wyłącznie w roli obserwatorów.

862 Rozporządzenie w sprawie SIS II, art. 41 ust. 1 i decyzja w sprawie SIS II, art. 58.

863 ETPC, *Dalea przeciwko Francji*, nr 964/07, 2 lutego 2010 r.

864 Rozporządzenie w sprawie SIS II, art. 60 ust. 2.

865 Zob. strona internetowa Europejskiego Inspektora Ochrony Danych dotycząca Systemu Informacyjnego Schengen.

W ramach grupy ds. koordynowania nadzoru EIOD i krajowe organy nadzorcze aktywnie współpracują poprzez wymianę informacji, wzajemne wsparcie w prowadzeniu audytów i inspekcji, opracowywanie ujednoliconych wniosków dotyczących wspólnych rozwiązań potencjalnych problemów oraz promowaniu świadomości praw do ochrony danych[866]. Grupa ds. koordynowania nadzoru nad SIS II przyjmuje ponadto wytyczne, które mają być pomocą dla osób, których dane dotyczą. Przykładem jest poradnik ułatwiający osobom, których dane dotyczą, wykonywanie ich praw dostępu[867].

Perspektywa

W 2016 r. Komisja Europejska przeprowadziła ocenę systemu SIS[868], w której wykazała, że wdrożono mechanizmy krajowe umożliwiające osobom, których dane dotyczą, dostęp do ich danych osobowych, ich poprawienie i usunięcie z SIS II lub uzyskanie odszkodowania w związku z wprowadzeniem nieprawidłowych danych. Aby zwiększyć skuteczność i wydajność SIS II, Komisja Europejska przedstawiła trzy wnioski dotyczące rozporządzeń:

- rozporządzenie w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie kontroli granicznych, które uchyli rozporządzenie w sprawie SIS II;
- rozporządzenie w sprawie utworzenia, funkcjonowania i użytkowania SIS w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, które uchyli – między innymi – decyzję w sprawie SIS II;
- rozporządzenie w sprawie użytkowania SIS w odniesieniu do powrotów nielegalnie przebywających obywateli państw trzecich.

Co ważne, wnioski te dopuszczają przetwarzanie innych kategorii danych biometrycznych – nie tylko fotografii i odcisków palców, które są już objęte istniejącym systemem SIS II. W bazie danych SIS będą również przechowywane wizerunki twarzy, odciski dłoni i profile DNA. Dodatkowo, podczas gdy rozporządzenie i decyzja

866 Rozporządzenie w sprawie SIS II, art. 46 i decyzja w sprawie SIS II, art. 62.

867 Zob. grupa ds. koordynowania nadzoru nad SIS II *The Schengen Information System. A guide for exercising the right of access*, dostępny na stronie internetowej EIOD.

868 Komisja Europejska (2016), Sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie oceny Systemu Informacyjnego Schengen drugiej generacji (SIS II) zgodnie z art. 24 ust. 5, art. 43 ust. 3 i art. 50 ust. 5 rozporządzenia (WE) nr 1987/2006 i art. 59 ust. 3 i art. 66 ust. 5 decyzji 2007/533/WSiSW, COM(2016) 880 final, Bruksela, 21 grudnia 2016 r.

w sprawie SIS II przewidywały możliwość wyszukiwania danych w oparciu o odciski palców w celu ustalenia tożsamości danej osoby, przedmiotowe wnioski nakładają taki obowiązek, jeżeli nie jest możliwe ustalenie tożsamości w inny sposób. Wizerunki twarzy, fotografie i odciski dłoni będą służyły do wyszukiwania danych w systemie i ustalania tożsamości osób, gdy stanie się to technicznie możliwe. Nowe przepisy dotyczące cech biometrycznych pociągają za sobą szczególne ryzyko dla praw osób fizycznych. W opinii dotyczącej wniosków Komisji[869] EIOD zauważył, że dane biometryczne są danymi niezwykle wrażliwymi i że wprowadzenie ich do wielkoskalowej bazy danych powinna poprzedzać oparta na dowodach ocena potrzeby włączenia ich do SIS. Innymi słowy, należy wykazać konieczność przetwarzania tych nowych danych. EIOD uznał ponadto, że trzeba doprecyzować, jaki rodzaj informacji można ująć w profilu DNA. Z uwagi na to, że profil DNA może zawierać informacje szczególnie chronione (należy tu wskazać przede wszystkim informacje o stanie zdrowia), profile DNA przechowywane w SIS powinny obejmować: „wyłącznie minimalną ilość informacji, które są absolutnie konieczne do identyfikacji zaginionych osób, z wyraźnym wyłączeniem informacji o stanie zdrowia, pochodzeniu rasowym i wszelkich innych informacji szczególnie chronionych"[870]. We wnioskach ustanowiono jednak dodatkowe zabezpieczenia, aby gromadzenie i dalsze przetwarzanie danych było ograniczone do tego, co jest absolutnie koniecznie i niezbędne z operacyjnego punktu widzenia, oraz ograniczono dostęp do tego rodzaju danych do osób, które muszą przetwarzać takie dane ze względów operacyjnych[871]. Co więcej, upoważniono w nich eu-LISA do sporządzania w regularnych odstępach czasu sprawozdań dotyczących jakości danych dla państw członkowskich, co ma na celu ocenę wpisów z myślą o zapewnieniu jakości danych[872].

869 EIOD (2017), EDPS Opinion on the new legal basis of the Schengen Information System, opinia 7/2017, 2 maja 2017 r.

870 Tamże, pkt 22.

871 Komisja Europejska (2016), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen (SIS) w dziedzinie współpracy policyjnej i współpracy wymiarów sprawiedliwości w sprawach karnych, zmieniającego rozporządzenie (UE) nr 515/2014 i uchylającego rozporządzenie (WE) nr 1986/2006, decyzję Rady 2007/533/WSiSW i decyzję Komisji 2010/261/UE, COM(2016) 883 final, Bruksela, 21 grudnia 2016 r.

872 Tamże, s. 15.

Wizowy system informacyjny

Wizowy system informacyjny (VIS), który jest również eksploatowany przez eu-LISA, stworzono, aby wesprzeć wdrożenie wspólnej polityki wizowej UE[873]. VIS umożliwia państwom Schengen wymianę danych dotyczących osób ubiegających się o wizę za pośrednictwem w pełni scentralizowanego systemu, który łączy konsulaty i ambasady państw strefy Schengen w krajach nienależących do UE z zewnętrznymi przejściami granicznymi wszystkich państw strefy Schengen. VIS przetwarza dane dotyczące wniosków o krótkoterminowe wizy pobytowe lub tranzytowe przez strefę Schengen. VIS umożliwia organom granicznym sprawdzenie za pomocą danych biometrycznych, zwłaszcza odcisków palca, czy osoba przedstawiająca wizę jest jej prawowitym posiadaczem, oraz identyfikację osób, które nie posiadają dokumentów lub posiadają fałszywe dokumenty.

Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS) określa warunki i procedury przekazywania danych osobowych dotyczących wniosków o wydanie wiz krótkoterminowych. Reguluje także kwestię decyzji podejmowanych w związku z takimi wnioskami, w tym decyzji o unieważnieniu, cofnięciu wizy lub przedłużeniu jej ważności[874]. Rozporządzenie w sprawie VIS obejmuje przede wszystkim dane dotyczące osoby ubiegającej się o wizę, jej wizy, fotografie, odciski palców, odsyłacze do poprzednich wniosków oraz pliki danych dotyczących wniosku osób jej towarzyszących bądź też danych dotyczących zaproszeń[875]. Dostęp do VIS w celu wprowadzania, korygowania lub usuwania danych jest zarezerwowany wyłącznie dla organów wizowych, podczas gdy dostęp do celów przeglądania danych jest udostępniany organom wizowym oraz właściwym

873 Rada Unii Europejskiej (2004), Decyzja Rady nr 2004/512/WE z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz.U. L 213 z 15.6.2004; rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz.U. L 218 z 13.8.2008; Rada Unii Europejskiej (2008), Decyzja Rady 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania, w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz.U. L 218 z 13.8.2008.

874 Rozporządzenie w sprawie VIS, art. 1.

875 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 767/2008 z dnia 9 lipca 2008 r. w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (rozporządzenie w sprawie VIS), Dz.U. L 218 z 13.8.2008, art. 5.

organom dokonującym odpraw na zewnętrznych przejściach granicznych, kontroli imigracyjnej i odpowiedzialnym za udzielanie azylu.

Pod pewnymi warunkami krajowe właściwe organy policyjne i Europol mogą wnioskować o dostęp do danych wprowadzonych do VIS w celu zapobiegania terroryzmowi i innym przestępstwom, wykrywania ich oraz prowadzenia dochodzeń w ich sprawie[876]. Ponieważ VIS z założenia jest instrumentem wspierającym wdrożenie wspólnej polityki wizowej, zasada ograniczenia celu, zgodnie z którą – jak wyjaśniono w rozdziale 3.2 – dane osobowe muszą być przetwarzane wyłącznie w konkretnych, wyraźnych i uzasadnionych celach i muszą być adekwatne, stosowne i nie wykraczać poza cele, dla których są przetwarzane, zostałaby naruszona, gdyby VIS stał się narzędziem egzekwowania prawa. Z tego względu krajowym organom ścigania i Europolowi nie przyznano stałego dostępu do bazy danych VIS. Dostęp jest dopuszczalny tylko w indywidualnie rozpatrywanych przypadkach i muszą mu towarzyszyć ścisłe zabezpieczenia. Warunki i zabezpieczenia dostępu oraz przeglądania VIS przez te organy reguluje decyzja Rady 2008/633/WSiSW[877].

Co więcej, rozporządzenie w sprawie VIS nadaje osobom, których dane dotyczą, prawa. Należą do nich:

- Prawo do uzyskania od właściwego państwa członkowskiego informacji o: tożsamości administratora danych, który odpowiada za przetwarzanie danych w tym państwie członkowskim, oraz jego danych kontaktowych; celach przetwarzania danych osobowych w ramach VIS; kategoriach osób, którym dane mogą zostać przesłane (odbiorców); oraz okresie ich przechowywania. Ponadto należy informować osoby ubiegające się o wizę o obowiązku uzyskania danych w ramach VIS do celów rozpatrzenia wniosku wizowego, natomiast państwa członkowskie muszą oprócz tego informować takie osoby o przysługującym im prawie dostępu do danych, prawie zwrócenia się o poprawienie lub usunięcie danych oraz o procedurach umożliwiających takim osobom wykonywanie ich praw[878].

876 Rada Unii Europejskiej (2008), Decyzja Rady 2008/633/WSiSW z dnia 23 czerwca 2008 r. w sprawie dostępu wyznaczonych organów państw członkowskich i Europolu do Wizowego Systemu Informacyjnego (VIS) do celów jego przeglądania w celu zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania, Dz.U. L 218 z 13.8.2008.

877 Tamże.

878 Rozporządzenie w sprawie VIS, art. 37.

- Prawo dostępu do danych osobowych dotyczących danej osoby, zarejestrowanych w VIS[879].

- Prawo do skorygowania błędnych danych[880].

- Prawo do usunięcia danych przechowywanych bezprawnie[881].

Aby zapewnić nadzór nad VIS, utworzono grupę ds. koordynowania nadzoru nad VIS. Składa się z EIOD oraz przedstawicieli organów nadzorczych państw członkowskich. Grupa spotyka się dwa razy w roku. Należą do niej przedstawiciele 28 państw członkowskich UE oraz przedstawiciele Islandii, Liechtensteinu, Norwegii i Szwajcarii.

Eurodac

Nazwa Eurodac oznacza europejski system identyfikacji odcisków palców[882]. Jest to scentralizowany system zawierający dane daktyloskopijne obywateli państw trzecich ubiegających się o azyl w jednym z państw członkowskich UE[883]. System ten działa od stycznia 2003 r., kiedy to przyjęto rozporządzenie Rady (WE) nr 2725/2000. Od 2015 r. obowiązuje wersja przekształcona. Celem systemu jest pomoc w ustaleniu, które państwo członkowskie powinno być odpowiedzialne za rozpatrzenie danego wniosku o udzielenie azylu na mocy rozporządzenia (WE) nr 604/2013. Rozporządzenie to ustanawia kryteria i mechanizmy określania państwa członkowskiego odpowiedzialnego za rozpatrywanie wniosku o udzielenie

879 Tamże, art. 38 ust. 1.

880 Tamże, art. 38 ust. 2.

881 Tamże.

882 Zob. strona internetowa Europejskiego Inspektora Ochrony Danych dotycząca systemu Eurodac.

883 Rozporządzenie Rady (WE) nr 2725/2000 z dnia 11 grudnia 2000 r. dotyczące ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania Konwencji Dublińskiej, Dz.U. L 316 z 15.12.2000; rozporządzenie Rady (WE) nr 407/2002 z dnia 28 lutego 2002 r. ustanawiające niektóre zasady wykonania rozporządzenia (WE) nr 2725/2000 dotyczącego ustanowienia systemu „Eurodac" do porównywania odcisków palców w celu skutecznego stosowania Konwencji dublińskiej, Dz.U. L 62 z 5.3.2002 (rozporządzenia Eurodac); rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 603/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego, oraz zmieniające rozporządzenie (UE) nr 1077/2011 ustanawiające Europejską Agencję ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości, Dz.U. L 180 z 29.6.2013, s. 1 (wersja przekształcona rozporządzenia Eurodac).

ochrony międzynarodowej wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca (rozporządzenie Dublin III)[884]. Dane osobowe przechowywane w systemie Eurodac mają na celu przede wszystkim ułatwienie stosowania rozporządzenia Dublin III[885].

Krajowe organy ścigania i Europol mogą porównywać odciski palców powiązane z dochodzeniami karnymi z odciskami zgromadzonymi w systemie Eurodac, ale tylko do celów zapobiegania przestępstwom terrorystycznym lub innym poważnym przestępstwom, ich wykrywania lub ścigania. Z uwagi na to, że Eurodac z założenia jest instrumentem wspierającym wdrażanie unijnej polityki azylowej, a nie narzędziem utrzymywania porządku publicznego, organy ścigania mają dostęp do bazy danych tylko w określonych przypadkach, w szczególnych okolicznościach i po spełnieniu ścisłych warunków[886]. W odniesieniu do dalszego wykorzystywania danych do celów utrzymywania porządku publicznego zastosowanie ma dyrektywa o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości, natomiast dane służące głównemu celowi, tj. ułatwieniu stosowania rozporządzenia Dublin III, są chronione na mocy ogólnego rozporządzenia o ochronie danych. Dalsze przekazywanie danych osobowych uzyskanych przez państwo członkowskie bądź Europol zgodnie z wersją przekształconą rozporządzenia Eurodac jakiemukolwiek państwu trzeciemu, jakiejkolwiek organizacji międzynarodowej lub jakiemukolwiek podmiotowi prywatnemu mającym siedzibę w Unii lub poza nią jest zabronione[887].

Eurodac składa się z obsługiwanej przez eu-LISA jednostki centralnej, w której przechowywane są i porównywane odciski palców, oraz z systemu do elektronicznego przesyłania danych między państwami członkowskimi a centralną bazą danych. Państwa członkowskie pobierają i przesyłają odciski palców każdej osoby w wieku co najmniej 14 lat, która ubiega się o azyl na ich terytorium, oraz każdego obywatela państwa trzeciego lub bezpaństwowca w wieku co najmniej 14 lat, lub został zatrzymany przy próbie nielegalnego przekroczenia ich zewnętrznej granicy. Państwa członkowskie mogą również pobierać i przesyłać odciski palców obywateli

884 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 604/2013 z dnia 26 czerwca 2013 r. w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca, Dz.U. L 180 z 29.6.2013 (rozporządzenie Dublin III).

885 Wersja przekształcona rozporządzenia Eurodac, Dz.U. L 180 z 29.6.2013, s. 1, art. 1 ust. 1.

886 Tamże, art. 1 ust. 2.

887 Tamże, art. 35.

państw trzecich lub bezpaństwowców, którzy przebywają na ich terytorium bez zezwolenia.

Choć każde państwo członkowskie może przeglądać Eurodac i zwrócić się o porównanie z danymi daktyloskopijnymi, wyłącznie państwo członkowskie, które zgromadziło odciski palców i przesłało je do jednostki centralnej może zmieniać te dane przez ich poprawienie, uzupełnienie lub usunięcie[888]. Agencja eu-Lisa prowadzi rejestr wszystkich operacji przetwarzania danych w celu monitorowania ochrony danych oraz zapewnienia bezpieczeństwa danych[889]. Krajowe organy nadzorcze pomagają i doradzają osobom, których dane dotyczą, w wykonywaniu przysługujących im praw[890]. Zbieranie i przesyłanie danych daktyloskopijnych podlega kontroli sądowej dokonywanej przez sądy krajowe[891]. Rozporządzenie w sprawie ochrony danych przez instytucje UE[892] i nadzór ze strony EIOD mają zastosowanie do czynności przetwarzania dotyczących Eurodac, realizowanych przez system centralny, którym zarządza eu-LISA[893]. Osoba, która poniesie szkodę w wyniku niezgodnego z prawem przetwarzania danych lub jakiegokolwiek działania niezgodnego z rozporządzeniem Eurodac, jest uprawniona do otrzymania odszkodowania od państwa członkowskiego odpowiedzialnego za wyrządzoną szkodę[894]. Należy jednak podkreślić, że osoby ubiegające się o azyl stanowią szczególnie wrażliwą grupę ludzi, którzy wyruszyli w długą i ryzykowną podróż. Z uwagi na tę szczególną, niepewną sytuację, w której osoby te często znajdują się w czasie gdy rozpatrywane są ich wnioski o udzielenie azylu, w praktyce wykonywanie ich praw, w tym prawa do odszkodowania, może być utrudnione.

By móc korzystać z Eurodac na potrzeby ochrony porządku publicznego, państwa członkowskie muszą wyznaczyć organy uprawnione do występowania o dostęp do systemu, a także organy odpowiedzialne za weryfikację zgodności wniosków o porównanie z prawem[895]. Dostęp organów krajowych i Europolu do danych dak-

888 Tamże, art. 27.

889 Tamże, art. 28.

890 Tamże, art. 29.

891 Tamże.

892 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

893 Wersja przekształcona rozporządzenia Eurodac, Dz.U. L 180 z 29.6.2013, s. 1, art. 31.

894 Tamże, art. 37.

895 Roots, L. (2015), „The New EURODAC Regulation: Fingerprints as a Source of Informal Discrimination", *Baltic Journal of European Studies Tallinn University of Technology*, t. 5, nr 2, s. 108–129.

tyloskopijnych jest obwarowany bardzo rygorystycznymi warunkami. Zanim organ wnioskujący przedłoży umotywowany elektroniczny wniosek, musi porównać dane z danymi dostępnymi w innych systemach informacyjnych, takich jak krajowe bazy daktyloskopijne czy VIS. Muszą występować nadrzędne względy dotyczące bezpieczeństwa publicznego, które na zasadzie proporcjonalności uzasadniają porównanie. Porównanie musi być rzeczywiście niezbędne i odnosić się do konkretnej sprawy, a ponadto muszą istnieć uzasadnione powody, by uznać, że porównanie znacznie przyczyni się do zapobiegania wszelkim odnośnym przestępstwom, ich wykrywania lub ścigania, w szczególności w przypadku, gdy zachodzi uzasadnione podejrzenie, że osoba podejrzana o popełnienie przestępstwa terrorystycznego lub innego poważnego przestępstwa, sprawca takich przestępstw lub ich ofiara należą do jednej z kategorii objętych zbieraniem odcisków palców w systemie Eurodac. Porównanie odbywa się wyłącznie na podstawie danych daktyloskopijnych. Europol musi uzyskać upoważnienie państwa członkowskiego, które zgromadziło dane daktyloskopijne.

Przechowywane w systemie Eurodac dane osobowe odnoszące się do osób ubiegających się o azyl są przechowywane przez 10 lat od dnia, w którym pobrano odciski palców, chyba że osoba, której dane dotyczą, uzyska obywatelstwo państwa członkowskiego UE. W takim przypadku dane należy niezwłocznie usunąć. Dane odnoszące się do cudzoziemców zatrzymanych przy próbie nielegalnego przekroczenia granicy zewnętrznej są przechowywane przez 18 miesięcy. Dane te należy niezwłocznie skasować, jeżeli osoba, której dane dotyczą, otrzyma zezwolenie na pobyt, opuści terytorium UE lub uzyska obywatelstwo państwa członkowskiego. Dane osób, którym udzielono azylu, pozostają dostępne przez trzy lata do celów porównania w kontekście zapobiegania przestępstwom terrorystycznym i innym poważnym przestępstwom, ich wykrywania i ścigania.

Oprócz wszystkich państw członkowskich UE system Eurodac na podstawie umów międzynarodowych wykorzystują również Islandia, Norwegia, Liechtenstein i Szwajcaria.

W celu zapewnienia nadzoru nad Eurodac utworzono grupę ds. koordynowania nadzoru nad Eurodac. Składa się z EIOD oraz przedstawicieli organów nadzorczych państw członkowskich. Grupa spotyka się dwa razy w roku. Należą do niej przedstawiciele 28 państw członkowskich UE oraz przedstawiciele Islandii, Liechtensteinu, Norwegii i Szwajcarii[896].

896 Zob. strona internetowa Europejskiego Inspektora Ochrony Danych dotycząca systemu Eurodac.

Perspektywa

W maju 2016 r. Komisja przedłożyła wniosek dotyczący nowej przekształconej wersji rozporządzenia Eurodac w ramach reformy mającej na celu usprawnienie funkcjonowania wspólnego europejskiego systemu azylowego (WESA)[897]. Przekształcenie będące przedmiotem wniosku ma duże znaczenie, ponieważ rozszerzy zakres pierwotnej bazy danych Eurodac. Eurodac został pierwotnie stworzony w celu wspierania wdrażania WESA przez zapewnianie dowodów daktyloskopijnych umożliwiających ustalenie, które państwo członkowskie odpowiada za rozpatrzenie wniosku azylowego złożonego w UE. Przekształcenie będące przedmiotem wniosku rozszerzy zakres bazy danych na potrzeby powrotu nielegalnych migrantów[898]. Organy krajowe będą mogły przeglądać bazę danych w celu identyfikacji obywateli państw trzecich o nieuregulowanym statusie pobytu w Unii lub takich, którzy nielegalnie wjechali na terytorium UE, co pozwoli tym organom uzyskać dowody ułatwiające państwom członkowskim doprowadzenie do powrotu takich osób. Obowiązujący system prawny wymaga gromadzenia i przechowywania wyłącznie odcisków palców, natomiast w przedmiotowym wniosku wprowadzono wymóg zbierania wizerunków twarzy[899], czyli innego rodzaju danych biometrycznych. Wniosek przewiduje też obniżenie minimalnego wieku dzieci, od których można pobrać takie dane, do sześciu lat[900] zamiast dotychczasowych 14, przewidzianych w rozporządzeniu z 2013 r. Rozszerzenie zakresu rozporządzenia oznacza, że będzie ono stanowiło ingerencję w prawa do prywatności i ochrony danych większej liczby osób fizycznych, których dane mogą zostać ujęte w bazie. Aby zrównoważyć tę ingerencję,

897 Komisja Europejska, Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania [rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca] na potrzeby identyfikowania nielegalnie przebywających obywateli państw trzecich lub bezpaństwowców oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego (wersja przekształcona), COM(2016)272 final, 4 maja 2016 r.

898 Zob. uzasadnienie wniosku, s. 3.

899 Komisja Europejska, Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania [rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca] na potrzeby identyfikowania nielegalnie przebywających obywateli państw trzecich lub bezpaństwowców oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego (wersja przekształcona), COM(2016)272 final, 4 maja 2016 r., art. 2 ust. 1.

900 Tamże, art. 2 ust. 2.

przedmiotowy wniosek oraz zmiany zaproponowane przez Komisję LIBE Parlamentu Europejskiego[901] mają na celu umocnienie wymogów w zakresie ochrony danych. W czasie opracowywania niniejszego podręcznika w Parlamencie i Radzie trwały dyskusje na temat wspomnianego wniosku.

Eurosur

Europejski system nadzorowania granic (Eurosur)[902] ma na celu wzmocnienie kontroli zewnętrznych granic strefy Schengen przez wykrywanie, zapobieganie i zwalczanie nielegalnej imigracji oraz przestępczości transgranicznej. Służy on usprawnieniu wymiany informacji i współpracy operacyjnej między krajowymi ośrodkami koordynacji a Frontexem – agencją UE odpowiedzialną za opracowanie i wdrożenie nowej koncepcji zintegrowanego zarządzania granicami[903]. Jego ogólnymi celami są:

- ograniczenie liczby nielegalnych migrantów, którym udaje się niepostrzeżenie przedostać na terytorium UE;
- zredukowanie liczby ofiar wśród nielegalnych migrantów dzięki ocaleniu większej liczby istnień na morzu;
- poprawa bezpieczeństwa wewnętrznego na całym terytorium UE poprzez przyczynienie się do przeciwdziałania przestępczości transgranicznej[904].

---

901 Parlament Europejski, *Sprawozdanie w sprawie wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady w sprawie ustanowienia systemu Eurodac do porównywania odcisków palców w celu skutecznego stosowania [rozporządzenia (UE) nr 604/2013 w sprawie ustanowienia kryteriów i mechanizmów ustalania państwa członkowskiego odpowiedzialnego za rozpatrzenie wniosku o udzielenie ochrony międzynarodowej złożonego w jednym z państw członkowskich przez obywatela państwa trzeciego lub bezpaństwowca] na potrzeby identyfikowania nielegalnie przebywających obywateli państw trzecich lub bezpaństwowców oraz w sprawie występowania o porównanie z danymi Eurodac przez organy ścigania państw członkowskich i Europol na potrzeby ochrony porządku publicznego (przekształcenie)*, PE 597.620v03-00, 9 czerwca 2017 r.

902 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1052/2013 z dnia 22 października 2013 r. ustanawiające europejski system nadzorowania granic (EUROSUR), Dz.U. L 295 z 6.11.2013, s. 295.

903 Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/1624 z dnia 14 września 2016 r. w sprawie Europejskiej Straży Granicznej i Przybrzeżnej oraz zmieniające rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/399 i uchylające rozporządzenie (WE) nr 863/2007 Parlamentu Europejskiego i Rady, rozporządzenie Rady (WE) nr 2007/2004 i decyzję Rady 2005/267/WE, Dz.U. L 251 z 16.9.2016.

904 Zob. także: Komisja Europejska (2008), Komunikat Komisji dla Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów: Analiza projektu stworzenia europejskiego systemu nadzorowania granic (Eurosur), COM(2008) 68 final, Bruksela, 13 lutego 2008 r.; Komisja Europejska (2011), „Impact Assessment accompanying the Proposal for a Regulation of the European Parliament and of the Council establishing the European Border Surveillance System (Eurosur)", dokument roboczy służb, SEC(2011) 1536 final, Bruksela, 12 grudnia 2011 r., s. 18.

System został uruchomiony 2 grudnia 2013 r. we wszystkich państwach członkowskich z granicami zewnętrznymi, w pozostałych zaś – 1 grudnia 2014 r. Rozporządzenie ma zastosowanie do nadzoru lądowych, morskich i powietrznych granic zewnętrznych państw członkowskich. W ramach Eurosur wymienia się i przetwarza dane osobowe w bardzo ograniczonym zakresie, ponieważ państwa członkowskie i Frontex są uprawnione tylko do wymiany numerów identyfikacyjnych statków. Eurosur służy do wymiany informacji operacyjnych, takich jak lokalizacja patroli i miejsca zdarzeń, które co do zasady nie mogą zawierać danych osobowych[905]. W wyjątkowych przypadkach, gdy dochodzi do wymiany danych osobowych w ramach Eurosur, rozporządzenie przewiduje pełne zastosowanie ogólnych ram prawnych UE z zakresu ochrony danych[906].

W związku z tym Eurosur gwarantuje prawo do ochrony danych, a to poprzez stwierdzenie, że wymiana danych osobowych musi przebiegać w zgodzie z kryteriami i zabezpieczeniami określonymi w dyrektywie o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości oraz ogólnym rozporządzeniu o ochronie danych[907].

System informacji celnej

Kolejnym ważnym systemem informacyjnym ustanowionym na szczeblu UE jest system informacji celnej (CIS)[908]. Tworząc rynek wewnętrzny, zniesiono wszystkie kontrole i formalności w odniesieniu do przepływu towarów w obrębie Unii, co zwiększyło ryzyko nadużyć. Ryzyko to zrównoważono dzięki zacieśnieniu współpracy między administracjami celnymi państw członkowskich. Celem CIS jest wspieranie państw członkowskich w zapobieganiu poważnym naruszeniom krajowych i unijnych przepisów celnych oraz rolnych, jak też w prowadzeniu dochodzeń w sprawie tych naruszeń i ich ściganiu. CIS ustanowiono dwoma aktami prawnymi, opierającymi się na różnych podstawach prawnych: Rozporządzenie Rady (WE) nr 515/97

905 Komisja Europejska, *EUROSUR: Protecting the Schengen external borders – protecting migrants' lives. EUROSUR in a nutshell*, 29 listopada 2013 r.

906 Rozporządzenie 1052/2013, motyw 13 i art. 13.

907 Tamże, motyw 13 i art. 13.

908 Rada Unii Europejskiej (1995), Akt Rady z dnia 26 lipca 1995 r. ustanawiający Konwencję w sprawie wykorzystania technologii informatycznej dla potrzeb celnych, Dz.U. C 316 z 27.11.1995, zmieniony przez Radę Unii Europejskiej (2009), rozporządzenie (WE) nr 515/97 z dnia 13 marca 1997 r. w sprawie wzajemnej pomocy między organami administracyjnymi Państw Członkowskich i współpracy między Państwami Członkowskimi a Komisją w celu zapewnienia prawidłowego stosowania przepisów prawa celnego i rolnego, decyzja Rady 2009/917/WSiSW z dnia 30 listopada 2009 r. w sprawie stosowania technologii informatycznej do potrzeb celnych, Dz.U. L 323 z 10.12.2009 (decyzja w sprawie CIS).

odnosi się do współpracy między organami administracyjnymi ds. zwalczania nadużyć finansowych w kontekście unii celnej oraz wspólnej polityki rolnej, natomiast decyzja Rady 2009/917/WSiSW ma na celu wspieranie zapobiegania poważnym naruszeniom przepisów celnych, prowadzenia dochodzeń w sprawie tych naruszeń i ich ścigania. Oznacza to, że zastosowanie CIS nie ogranicza się do utrzymywania porządku publicznego.

CIS zawiera informacje obejmujące dane osobowe w odniesieniu do zatrzymanych, zajętych lub skonfiskowanych towarów, środków transportu, przedsiębiorstw, osób, przedmiotów i gotówki. Kategorie danych, które można przetwarzać, zostały wyraźnie określone. Należą do nich nazwiska, obywatelstwo, płeć, miejsce i data urodzenia danych osób, powód wprowadzenia ich danych do systemu oraz numery rejestracyjne środków transportu[909]. Informacje te mogą być wykorzystywane wyłącznie do celów obserwacji, składania sprawozdań lub prowadzenia kontroli szczególnych lub do celów analiz strategicznych bądź operacyjnych dotyczących osób podejrzanych o naruszenie przepisów celnych.

Dostęp do CIS mają krajowe organy celne, podatkowe, rolne, organy ds. zdrowia publicznego, policja, Europol i Eurojust.

Przetwarzanie danych osobowych musi odbywać się z poszanowaniem szczegółowych zasad określonych w rozporządzeniu (WE) nr 515/97 i decyzji Rady 2009/917/WSiSW, a także przepisów ogólnego rozporządzenia o ochronie danych, rozporządzenia w sprawie ochrony danych przez instytucje UE, postanowień zaktualizowanej konwencji nr 108 i rekomendacji w sprawie policji. EIOD jest odpowiedzialny za nadzór nad zgodnością CIS z rozporządzeniem (WE) nr 45/2001. Co najmniej raz w roku organizuje spotkanie ze wszystkimi krajowymi organami nadzorującymi ochronę danych właściwymi do spraw nadzoru nad CIS.

Interoperacyjność między systemami informacyjnymi UE

Zarządzanie migracją, zintegrowane zarządzanie granicami zewnętrznymi UE i zwalczanie terroryzmu i przestępczości transgranicznej rodzą istotne wyzwania, które w zglobalizowanym świecie stają się coraz bardziej złożone. Ostatnie lata upłynęły w UE pod znakiem opracowywania nowego, kompleksowego podejścia do ochrony i utrzymania bezpieczeństwa bez uszczerbku dla wartości UE i podstawowych wolności. Skuteczna wymiana informacji między krajowymi organami ścigania oraz

909 Zob. decyzja w sprawie CIS, art. 24, 25 i 28.

między państwami członkowskimi a właściwymi agencjami UE ma dla tych prac kluczowe znaczenie[910]. Poszczególne systemy zarządzania granicami i zapewniania bezpieczeństwa wewnętrznego UE mają właściwe sobie cele, strukturę instytucjonalną, osoby, których dane dotyczą, i użytkowników. Unia pracuje nad wyeliminowaniem niedoskonałości w funkcjonowaniu sfragmentaryzowanego zarządzania danymi w UE w różnych systemach informacyjnych, takich jak SIS II, VIS i Eurodac, analizując ich potencjalną interoperacyjność[911]. Głównym założeniem jest zapewnienie właściwym organom policyjnym, celnym i sądowym stałego dostępu do informacji niezbędnych do wykonywania ich obowiązków bez zachwiania równowagi względem poszanowania prawa do prywatności, ochrony danych i innych praw podstawowych.

Interoperacyjność to „zdolność systemów informacyjnych do wymiany danych oraz do umożliwienia dzielenia się informacjami"[912]. Wymiana ta nie może naruszać rygorystycznych zasad dostępu i wykorzystania zagwarantowanych w ogólnym rozporządzeniu o ochronie danych, dyrektywie o ochronie danych przetwarzanych przez policję i organy wymiaru sprawiedliwości, Karty praw podstawowych UE i innych stosownych zasad. Żadne zintegrowane rozwiązanie do zarządzania danymi nie może naruszać zasad celowości, uwzględniania ochrony danych już w fazie projektowania ani domyślnej ochrony danych[913].

910 Komisja Europejska (2016), Komunikat Komisji do Parlamentu Europejskiego i Rady: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205 final, Bruksela, 6 kwietnia 2016 r., Komisja Europejska (2016), Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady: Zwiększanie bezpieczeństwa w mobilnym świecie: ulepszona wymiana informacji na rzecz walki z terroryzmem i wzmocnionych granic zewnętrznych, COM(2016) 602 final, Bruksela, 14 września 2016 r., Komisja Europejska (2016), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie użytkowania Systemu Informacyjnego Schengen w odniesieniu do powrotów nielegalnie przebywających obywateli państw trzecich. Zob. także Komunikat Komisji do Parlamentu Europejskiego, Rady Europejskiej i Rady: Siódme sprawozdanie z postępu prac nad stworzeniem rzeczywistej i skutecznej unii bezpieczeństwa, COM(2017) 261 final, Bruksela, 16 maja 2017 r.

911 Rada Unii Europejskiej (2005), Program haski: wzmacnianie wolności, bezpieczeństwa i sprawiedliwości w Unii Europejskiej, Dz.U. C 53 z 3.3.2005, Komisja Europejska (2010), Komunikat Komisji do Parlamentu Europejskiego i Rady: Przegląd zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, COM(2010) 385 final, Komisja Europejska (2016) Komunikat Komisji do Parlamentu Europejskiego i Rady: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205 final, Bruksela, 6 kwietnia 2016 r., Komisja Europejska (2016), Decyzja Komisji z dnia 17 czerwca 2016 r. ustanawiająca grupę ekspertów wysokiego szczebla ds. systemów informacyjnych i interoperacyjności, Dz.U. C 257 z 15.7.2016.

912 Komisja Europejska (2016), Komunikat Komisji do Parlamentu Europejskiego i Rady: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205 final, Bruksela, 6 kwietnia 2016 r., s. 14.

913 Tamże, s. 4–5.

Oprócz usprawnienia funkcjonowania trzech głównych systemów informacyjnych – SIS II, VIS i Eurodac – Komisja przedłożyła wniosek dotyczący ustanowienia czwartego scentralizowanego systemu zarządzania granicami, ukierunkowanego na obywateli państw trzecich: systemu wjazdu/wyjazdu[914], który ma zostać wdrożony do 2020 r.[915]. Komisja przedstawiła ponadto wniosek dotyczący ustanowienia europejskiego systemu informacji o podróży oraz zezwoleń na podróż (ETIAS), w którym będą gromadzone informacje na temat osób podróżujących do UE bezwizowo, co umożliwi zaawansowane kontrole nielegalnej migracji oraz bezpieczeństwa[916].

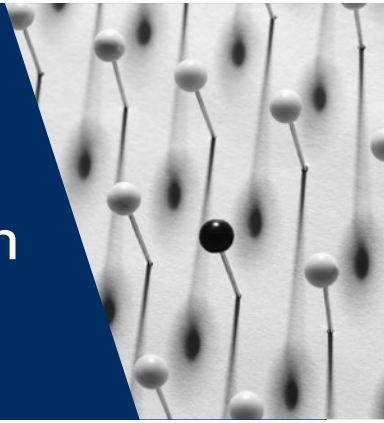
914 Komisja Europejska (2016), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego system wjazdu/wyjazdu w celu rejestrowania danych dotyczących wjazdu i wyjazdu obywateli państw trzecich i danych dotyczących odmowy wjazdu w odniesieniu do obywateli państw trzecich przekraczających granice zewnętrzne państw członkowskich Unii Europejskiej oraz określającego warunki dostępu do systemu wjazdu/wyjazdu na potrzeby ścigania i zmieniającego rozporządzenie (WE) nr 767/2008 i rozporządzenie (UE) nr 1077/2011, COM(2016) 194 final, Bruksela, 6 kwietnia 2016 r.

915 Komisja Europejska (2016), Komunikat Komisji do Parlamentu Europejskiego i Rady: Sprawniejsze i bardziej inteligentne systemy informacyjne do celów zarządzania granicami i zapewnienia bezpieczeństwa, COM(2016) 205 final, Bruksela, 6 kwietnia 2016 r., s. 5.

916 Komisja Europejska (2016), Wniosek dotyczący rozporządzenia Parlementu Europejskiego i Rady ustanawiającego europejski system informacji o podróży oraz zezwoleń na podróż (ETIAS) i zmieniające rozporządzenia (UE) nr 515/2014, (UE) 2016/399, (UE) 2016/794 i (UE) 2016/1624, COM(2016) 731 final, 16 listopada 2016 r.

9

Szczególne rodzaje danych i przepisy w zakresie ich ochrony



UE	Omówione zagadnienia	RE
Ogólne rozporządzenie o ochronie danych Dyrektywa o prywatności i łączności elektronicznej	**Łączność elektroniczna**	Konwencja nr 108 Zalecenie w sprawie usług telekomunikacyjnych
Artykuł 89 ogólnego rozporządzenia o ochronie danych	**Stosunki pracy**	Zaktualizowana konwencja nr 108 Zalecenie w sprawie zatrudnienia ETPC, *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 2007 r.
Artykuł 9 ust. 2 lit. h) i i) ogólnego rozporządzenia o ochronie danych	**Dane medyczne**	Zaktualizowana konwencja nr 108 Zalecenie w sprawie danych medycznych ETPC, *Z przeciwko Finlandii*, nr 22009/93, 1997 r.
Rozporządzenie w sprawie badań klinicznych	**Badania kliniczne**	
Artykuł 6 ust. 4 i art. 89 ogólnego rozporządzenia o ochronie danych	**Statystyka**	Zaktualizowana konwencja nr 108 Zalecenie w sprawie danych statystycznych

UE	Omówione zagadnienia	RE
Rozporządzenie (WE) nr 223/2009 w sprawie statystyki europejskiej TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 2008	**Statystyka publiczna**	Zaktualizowana konwencja nr 108 Zalecenie w sprawie danych statystycznych
Dyrektywa 2014/65/UE w sprawie rynków instrumentów finansowych Rozporządzenie (UE) nr 648/2012 w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, kontrahentów centralnych i repozytoriów transakcji Rozporządzenie (WE) nr 1060/2009 w sprawie agencji ratingowych Dyrektywa 2007/64/WE w sprawie usług płatniczych w ramach rynku wewnętrznego	**Dane finansowe**	Zaktualizowana konwencja nr 108 Zalecenie 90(19) w sprawie ochrony danych osobowych wykorzystywanych do płatności i innych powiązanych czynności ETPC, *Michaud przeciwko Francji*, nr 12323/11, 2012 r.

W kilku przypadkach na szczeblu europejskim przyjęto specjalne akty prawne, w których określono bardziej szczegółowo zastosowanie ogólnych zasad zaktualizowanej konwencji nr 108 lub ogólnego rozporządzenia o ochronie danych do konkretnych sytuacji.

9.1. Łączność elektroniczna

Najważniejsze kwestie

- Szczegółowe zasady dotyczące ochrony danych w dziedzinie telekomunikacji, ze szczególnym uwzględnieniem usług telefonicznych, zawarto w zaleceniu RE z 1995 r.
- Przetwarzanie danych osobowych w związku ze świadczeniem usług łączności na szczeblu UE uregulowano w dyrektywie o prywatności i łączności elektronicznej.
- Poufność łączności elektronicznej odnosi się nie tylko do jej treści, ale także do metadanych, takich jak informacje o tym, kto łączył się z kim, kiedy i na jak długo, oraz danych dotyczących lokalizacji, takich jak skąd zostały przesłane dane.

W przypadku sieci łączności potencjał nieuzasadnionej ingerencji w sferę osobistą użytkowników jest szczególnie wysoki, ponieważ udostępniają one dodatkowe możliwości techniczne podsłuchiwania oraz obserwowania łączności nawiązywanej

w takich sieciach. W związku z tym za niezbędne uznano specjalne regulacje w zakresie ochrony danych współmierne do szczególnych zagrożeń dla użytkowników usług łączności.

W 1995 r. **RE** wydała zalecenie dotyczące ochrony danych w dziedzinie telekomunikacji, ze szczególnym uwzględnieniem usług telefonicznych[917]. Zgodnie z tym zaleceniem gromadzenie i przetwarzanie danych osobowych w kontekście usług telekomunikacyjnych powinno następować tylko w celach: podłączenia użytkownika do sieci, udostępnienia konkretnej usługi telekomunikacyjnej, rozliczeń, weryfikacji, zapewnienia optymalnego funkcjonowania technicznego oraz rozwoju sieci i usługi.

Szczególną uwagę zwrócono także na wykorzystanie sieci łączności do wysyłania wiadomości w celu marketingu bezpośredniego. Zgodnie z ogólną zasadą wiadomości w celu marketingu bezpośredniego nie można kierować do żadnego abonenta, który wyraźnie wskazał, że nie chce otrzymywać takich wiadomości. Automatyczne urządzenia wywołujące służące do przekazywania wstępnie nagranych wiadomości reklamowych mogą być stosowane tylko wtedy, gdy abonent wyraził na to wyraźną zgodę. Szczegółowe przepisy w tym obszarze należy określić w prawie krajowym.

Jeżeli chodzi o **ramy prawne UE**, dyrektywę o prywatności i łączności elektronicznej (po pierwszej próbie podjętej w 1997 r.) przyjęto w 2002 r. i zmieniono w 2009 r. Uczyniono to w celu uzupełnienia i dostosowania przepisów dyrektywy o ochronie danych w odniesieniu do sektora telekomunikacyjnego[918].

Zastosowanie dyrektywy o prywatności i łączności elektronicznej ogranicza się do usług łączności w publicznych sieciach elektronicznych.

W dyrektywie o prywatności i łączności elektronicznej wyróżniono trzy główne kategorie danych generowanych w trakcie połączenia:

---

917 Rada Europy, Komitet Ministrów (1995), Recommendation Rec(95)4 to member states on the protection of personal data in the area of telecommunication services, with particular reference to telephone services, 7 lutego 1995 r.

918 Dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej, Dz.U. L 201 z 31.7.2002 (dyrektywa o prywatności i łączności elektronicznej) zmieniona dyrektywą 2009/136/WE Parlamentu Europejskiego i Rady z dnia 25 listopada 2009 r. zmieniającą dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009.

- dane stanowiące treść wiadomości wysyłanych podczas połączenia; dane te są ściśle poufne;

- dane niezbędne w celu ustanowienia i utrzymania połączenia, tak zwane metadane, w dyrektywie określane pojęciem „dane o ruchu", takie jak informacje dotyczące stron połączenia, czasu jego nawiązania i trwania;

- wśród metadanych znajdują się dane odnoszące się konkretnie do położenia urządzenia komunikacyjnego, tak zwane dane dotyczące lokalizacji – dane te są zarazem danymi dotyczącymi lokalizacji użytkowników urządzeń komunikacyjnych, i są szczególnie istotne w przypadku użytkowników mobilnych urządzeń komunikacyjnych.

Dane o ruchu mogą być wykorzystywane przez usługodawcę jedynie w celach rozliczeniowych i technicznego świadczenia usługi. Za zgodą osoby, której dane dotyczą, dane te mogą jednak zostać ujawnione innym administratorom oferującym usługi tworzące wartość dodaną, np. dostarczającym na podstawie lokalizacji użytkownika informacje na temat położenia najbliższej stacji metra lub apteki bądź prognozę pogody dla danej lokalizacji.

Zgodnie z art. 15 dyrektywy o prywatności i łączności elektronicznej dostęp do danych o łączności w sieciach elektronicznych musi spełniać wymagania dotyczące uzasadnionej ingerencji w prawo do ochrony danych określone w art. 8 ust. 2 EKPC i potwierdzone przez Kartę praw podstawowych w art. 8 i 52. Taki dostęp może obejmować dostęp do celów dochodzeń w sprawie przestępstw.

W 2009 r. w dyrektywie o prywatności i łączności elektronicznej[919] wprowadzono następujące zmiany:

- Ograniczenia nałożone na wysyłanie wiadomości elektronicznych do celów marketingu bezpośredniego rozszerzono na krótkie wiadomości tekstowe, usługi wiadomości multimedialnych oraz inne podobne zastosowania; marketingowe wiadomości elektroniczne są zabronione, chyba że uprzednio uzyskano na nie

919 Dyrektywa Parlamentu Europejskiego i Rady 2009/136/WE z dnia 25 listopada 2009 r. zmieniająca dyrektywę 2002/22/WE w sprawie usługi powszechnej i związanych z sieciami i usługami łączności elektronicznej praw użytkowników, dyrektywę 2002/58/WE dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy między organami krajowymi odpowiedzialnymi za egzekwowanie przepisów prawa w zakresie ochrony konsumentów, Dz.U. L 337 z 18.12.2009.

zgodę. Bez takiej zgody marketingowe wiadomości elektroniczne można kierować jedynie do dotychczasowych klientów, jeżeli ci udostępnili swój adres e-mail i nie zgłosili sprzeciwu.

- Na państwa członkowskie nałożono obowiązek zapewnienia środków sądowych w odniesieniu do naruszeń zakazu przesyłania niezamówionych komunikatów[920].

- Wykorzystywanie plików cookie, czyli oprogramowania, które monitoruje i rejestruje czynności użytkownika komputera, nie jest już dozwolone bez zgody użytkownika komputera. Sposób wyrażenia i uzyskania zgody zapewniający wystarczającą ochronę należy uregulować bardziej szczegółowo w prawie krajowym[921].

W przypadku gdy naruszenie danych następuje w wyniku nieuprawnionego dostępu, utraty lub zniszczenia danych, należy niezwłocznie poinformować właściwy organ nadzorczy. Obowiązkowe jest informowanie abonentów w przypadkach, gdy mogą oni ponieść szkody w konsekwencji naruszenia ochrony danych[922].

W dyrektywie o zatrzymywaniu danych[923] zobowiązano dostawców usług łączności do zatrzymywania metadanych. Dyrektywa ta została jednak zniesiona wyrokiem TSUE (więcej informacji na ten temat w sekcji 8.3).

Perspektywa

W styczniu 2017 r. Komisja Europejska przyjęła nowy wniosek dotyczący rozporządzenia w sprawie prywatności i łączności elektronicznej, uchylającego dyrektywę o prywatności i łączności elektronicznej. Celem tego aktu również byłyby ochrona „podstawowych praw i wolności osób fizycznych i prawnych w odniesieniu do świadczenia usług łączności elektronicznej i korzystania z takich usług,

920 Zob. zmieniona dyrektywa, art. 13.

921 Zob. tamże, art. 5; zob. także Grupa Robocza Art. 29 (2012), *Opinion 04/2012 on Cookie Consent Exemption*, WP 194, Bruksela, 7 czerwca 2012 r.

922 Zob. także Grupa Robocza Art. 29 (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments*, WP 184, Bruksela, 5 kwietnia 2011 r.

923 Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE, Dz.U. L 105 z 13.4.2006.

w szczególności prawa do poszanowania życia prywatnego i komunikowania się oraz prawa do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych", a jednocześnie zagwarantowanie swobodnego przepływu danych i usług związanych z łącznością elektroniczną w Unii[924]. Podczas gdy ogólne rozporządzenie o ochronie danych odnosi się przede wszystkim do art. 8 Karty praw podstawowych UE, przedmiotowe rozporządzenie ma na celu wdrożenie do prawa wtórnego UE art. 7 karty.

Rozporządzenie dostosowałoby przepisy poprzedniej dyrektywy do nowych technologii i realiów rynku oraz tworzyłoby całościowe i spójne ramy wraz z ogólnym rozporządzeniem o ochronie danych. W tym sensie rozporządzenie w sprawie prywatności i łączności elektronicznej stanowiłoby *lex specialis* w stosunku do ogólnego rozporządzenia o ochronie danych, zawężając jego zakres do danych pochodzących z łączności elektronicznej, będących danymi osobowymi. Nowe rozporządzenie obejmuje przetwarzanie „danych pochodzących z łączności elektronicznej", w tym treści łączności elektronicznej i metadane, które niekoniecznie stanowią dane osobowe. Terytorialny zakres stosowania ogranicza się do UE – nawet wówczas, gdy dane pozyskane w Unii są przetwarzane poza jej granicami – i obejmuje również dostawców usług OTT, czyli usługodawców dostarczających treści, usługi lub aplikacje za pośrednictwem Internetu, bez bezpośredniego udziału operatora sieci lub dostawcy usług internetowych. Do takich dostawców należą między innymi Skype (rozmowy głosowe i wideo), WhatsApp (komunikator), Google (wyszukiwarka), Spotify (muzyka) czy Netflix (treści wideo). Do nowego rozporządzenia miałyby zastosowanie mechanizmy egzekwowania przewidziane w ogólnym rozporządzeniu o ochronie danych.

Rozporządzenie w sprawie prywatności i łączności elektronicznej ma zostać przyjęte do 25 maja 2018 r., kiedy to w 28 państwach członkowskich w życie wejdzie ogólne rozporządzenie o ochronie danych. Jest to jednak uzależnione od zgody zarówno Parlamentu Europejskiego, jak i Rady[925].

924 Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej i uchylającego dyrektywę 2002/58/WE (rozporządzenie w sprawie prywatności i łączności elektronicznej), COM(2017) 10 final, art. 1.

925 Więcej informacji zob. Komisja Europejska (2017), Komisja proponuje wprowadzenie wysokiego poziomu ochrony prywatności i danych osobowych w łączności elektronicznej i aktualizuje przepisy ochrony danych w instytucjach UE, komunikat prasowy, 10 stycznia 2017 r.

9.2. Dane o zatrudnieniu

Najważniejsze kwestie

- W zaleceniu RE w sprawie danych o zatrudnieniu zawarto szczegółowe zasady dotyczące ochrony danych w kontekście stosunków pracy.
- W ogólnym rozporządzeniu o ochronie danych konkretnie o stosunkach pracy mowa jest jedynie w kontekście przetwarzania danych szczególnie chronionych.
- Ważność zgody (która musi mieć dobrowolny charakter) jako podstawy prawnej przetwarzania danych o pracownikach może budzić wątpliwości ze względu na nierównowagę ekonomiczną między pracodawcą a pracownikami. Należy starannie ocenić okoliczności udzielenia zgody.

Przetwarzanie danych w kontekście zatrudnienia regulują ogólne unijne przepisy z zakresu ochrony danych. Jedno z rozporządzeń[926] skupia się jednak konkretnie na ochronie danych przetwarzanych przez instytucje UE w kontekście zatrudnienia (między innymi). W ogólnym rozporządzeniu o ochronie danych o stosunkach pracy jest mowa w art. 9 ust. 2, w którym stwierdzono, że można przetwarzać dane osobowe podczas wypełniania przez administratora lub osobę, której dane dotyczą, obowiązków i wykonywania szczególnych praw w dziedzinie zatrudnienia.

Zgodnie z ogólnym rozporządzeniem o ochronie danych pracownikowi należy zapewnić możliwość jednoznacznego stwierdzenia, które dane są przedmiotem wyrażanej dobrowolnie zgody na przetwarzanie/przechowywanie, oraz poznania celów ich przechowywania. Zanim pracownicy wyrażą zgodę, powinno się ich ponadto informować o przysługujących im prawach oraz o okresie przechowywania. W sytuacji, gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych będzie skutkowało wysokim ryzykiem dla praw i wolności osób fizycznych, pracodawca musi poinformować pracownika o takim naruszeniu. W myśl art. 88 rozporządzenia państwa członkowskie mogą przyjąć bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w kontekście zatrudnienia.

926 Rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych, Dz.U. L 8 z 12.1.2001.

Przykład: W sprawie *Worten*[927] dane obejmowały ewidencję czasu pracy, zawierającą dzienne okresy czasu pracy i odpoczynku, które stanowią dane osobowe. Prawo krajowe może nakładać na pracodawcę obowiązek udostępnienia ewidencji czasu pracy krajowym organom uprawnionym do kontroli warunków pracy. Umożliwiłoby to tym organom natychmiastowy dostęp do odnośnych danych osobowych. Dostęp do danych osobowych jest im jednak niezbędny do kontrolowania przestrzegania przepisów z zakresu warunków pracy[928].

Jeżeli chodzi o prawo **RE**, zalecenie w sprawie danych o zatrudnieniu opublikowano w 1989 r. i zaktualizowano w 2015 r.[929]. Zalecenie to odnosi się do przetwarzania danych osobowych do celów zatrudnienia zarówno w sektorze prywatnym, jak i publicznym. Przetwarzanie danych musi odbywać się z poszanowaniem określonych zasad i ograniczeń, na przykład zasady przejrzystości oraz konsultacji z przedstawicielami pracowników przed wdrożeniem w zakładzie systemów monitorujących. W zaleceniu stwierdzono ponadto, że pracodawcy powinni stosować środki zapobiegawcze, takie jak filtry, zamiast monitorować korzystanie przez pracowników z Internetu.

Przegląd najczęstszych problemów związanych z ochroną danych w kontekście zatrudnienia znajduje się w dokumencie roboczym Grupy Roboczej Art. 29[930]. Grupa robocza przeanalizowała znaczenie zgody jako podstawy prawnej przetwarzania danych o zatrudnieniu[931]. Stwierdziła ona, że nierównowaga ekonomiczna między wnioskującym o zgodę pracodawcą a udzielającym jej pracownikiem często budzi wątpliwości, czy zgody udzielono dobrowolnie, czy też nie. Przy ocenie ważności zgody w kontekście zatrudnienia należy zatem starannie rozważyć okoliczności, w których wyrażenie zgody służy za podstawę prawną przetwarzania danych.

Częsty problem dotyczący ochrony danych w typowym współczesnym środowisku pracy wiąże się z zakresem uzasadnionego monitorowania komunikacji

927 TSUE, C-342/12, *Worten – Equipamentos para o Lar SA przeciwko Autoridade para as Condições de Trabalho (ACT)*, 30 maja 2013 r., pkt 19.

928 Tamże, pkt 43.

929 Rada Europy, Komitet Ministrów (2015), Zalecenie Rec(2015)5 dla państw członkowskich na temat ochrony danych osobowych wykorzystywanych dla celów zatrudnienia, kwiecień 2015 r.

930 Grupa Robocza Art. 29 (2017), *Opinion 2/2017 on data processing at work*, WP 249, Bruksela, 8 czerwca 2017 r.

931 Grupa Robocza Art. 29 (2005), *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995*, WP 114, Bruksela, 25 listopada 2005 r.

elektronicznej pracowników w miejscu pracy. Często twierdzi się, że problem ten można łatwo rozwiązać przez zakaz prywatnego wykorzystania środków komunikacji w pracy. Taki ogólny zakaz mógłby jednak okazać się nieproporcjonalny i nierealistyczny. Szczególnie interesujące w tym kontekście są wyroki ETPC w sprawach *Copland przeciwko Zjednoczonemu Królestwu* i Bărbulescu przeciwko Rumunii.

Przykład: W sprawie *Copland przeciwko Zjednoczonemu Królestwu*[932] potajemnie monitorowano korzystanie przez pracownicę uczelni z telefonu, poczty elektronicznej i Internetu w celu ustalenia, czy nie korzysta ona w nadmiernym stopniu z urządzeń uczelni do celów osobistych. ETPC uznał, że rozmowy telefoniczne z miejsca pracy wchodzą w zakres pojęć życia prywatnego i korespondencji. Dlatego też takie rozmowy i wiadomości e-mail wysyłane z miejsca pracy, jak również informacje pochodzące z monitorowania korzystania z Internetu do celów osobistych, są chronione na mocy art. 8 EKPC. W przypadku skarżącej nie istniały przepisy regulujące okoliczności, w których pracodawcy mogliby monitorować korzystanie przez pracowników z telefonu, poczty elektronicznej i Internetu. Ingerencja była zatem niezgodna z prawem. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Bărbulescu przeciwko Rumunii*[933] skarżący został zwolniony przez swojego pracodawcę za to, że korzystał z sieci internetowej swojego przedsiębiorstwa w godzinach pracy z naruszeniem wewnętrznego regulaminu. Pracodawca monitorował jego połączenia. Zapisy sporządzone w trakcie wewnętrznych procedur wykazały, że wymieniał on wiadomości o charakterze ściśle osobistym. Stwierdzając możliwość zastosowania art. 8, ETPC nie rozstrzygnął ostatecznie, czy w świetle restrykcyjnych regulacji pracodawcy skarżący mógł żywić rozsądne oczekiwanie odnośnie do życia prywatnego, tym niemniej stwierdził, że instrukcje pracodawcy nie mogą ograniczać do zera korzystania z prywatnego życia społecznego w miejscu pracy.

Co do istoty sprawy, układającym się państwom należało przyznać szeroki margines oceny przy określaniu konieczności przyjęcia ram prawnych regulujących warunki, w ramach których pracodawca może kształtować zasady elektronicznej lub innej komunikacji swoich pracowników, niemającej

932 ETPC, *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 3 kwietnia 2007 r.

933 ETPC, *Bărbulescu przeciwko Rumunii* [WI], nr 61496/08, 5 września 2017 r., pkt 121.

charakteru służbowego, w miejscu pracy. Organy krajowe musiały jednak zapewnić, że wprowadzeniu przez pracodawcę środków monitorowania korespondencji i innej komunikacji, niezależnie od ich zakresu i trwania, towarzyszą odpowiednie i wystarczające zabezpieczenia przed nadużyciami. Proporcjonalność i gwarancje proceduralne chroniące przed arbitralnością miały kluczowe znaczenie, a ETPC zidentyfikował szereg czynników, które należało uwzględnić w rozpatrywanych okolicznościach. Należały do nich między innymi zakres monitoringu wykonywanego przez pracodawcę i stopień ingerencji w prywatność pracownika; konsekwencje monitoringu dla pracownika; oraz to, czy miał on do dyspozycji odpowiednie gwarancje. Ponadto władze krajowe musiały się upewnić, że pracownik, którego komunikacje były przedmiotem monitoringu, mógł skorzystać ze środka ochrony prawnej przed organem sądowym mającym kompetencje do rozstrzygania, przynajmniej co do istoty, czy wskazane kryteria zostały spełnione, a także czy kwestionowane środki były zgodne z prawem.

W przedmiotowej sprawie ETPC stwierdził naruszenie art. 8, ponieważ organy krajowe nie zapewniły w sposób odpowiedni ochrony prawa skarżącego do poszanowania jego życia prywatnego i korespondencji, a także, w rezultacie, nie zapewniły słusznej równowagi między wchodzącymi w grę interesami.

Zgodnie z zaleceniem RE w sprawie zatrudnienia dane osobowe gromadzone w celach związanych z zatrudnieniem należy uzyskać bezpośrednio od danego pracownika.

Dane osobowe gromadzone w ramach rekrutacji muszą ograniczać się do informacji niezbędnych do oceny przydatności kandydatów oraz ich potencjału zawodowego.

W zaleceniu mowa jest także o subiektywnych ocenach wyników lub potencjału poszczególnych pracowników. Dane subiektywne muszą opierać się na rzetelnych i uczciwych ocenach oraz nie mogą być formułowane w sposób obraźliwy. Wymagają tego zasady rzetelnego przetwarzania danych i prawidłowości danych.

Szczególnym aspektem prawa o ochronie danych w stosunkach między pracodawcą a pracownikiem jest rola przedstawicieli pracowników. Przedstawiciele ci mogą otrzymywać dane osobowe pracowników wyłącznie w zakresie, w jakim jest to niezbędne, aby umożliwić im reprezentowanie ich interesów, lub gdy takie dane są im potrzebne do wypełniania lub nadzorowania zobowiązań wynikających z układów zbiorowych.

Dane osobowe szczególnie chronione zgromadzone w celach związanych z zatrudnieniem mogą być przetwarzane jedynie w szczególnych przypadkach i z zastosowaniem zabezpieczeń przewidzianych w prawie krajowym. Pracodawcy mogą pytać pracowników lub kandydatów do pracy o ich stan zdrowia lub przeprowadzać badania medyczne wyłącznie wówczas, gdy jest to konieczne w celu: określenia ich przydatności do pracy; spełnienia wymagań medycyny prewencyjnej; zabezpieczenia interesów życiowych osoby, której dane dotyczą, bądź innych pracowników i osób; przyznania świadczeń społecznych; lub gdy zażąda tego sąd. Dane dotyczące zdrowia nie mogą być gromadzone ze źródeł innych niż od danego pracownika z wyjątkiem przypadków, gdy uzyskano wyraźną i świadomą zgodę bądź gdy przewiduje to prawo krajowe.

Na mocy zalecenia w sprawie zatrudnienia pracowników należy informować o celu przetwarzania ich danych osobowych, rodzaju przechowywanych danych osobowych, podmiotach, którym te dane są regularnie przekazywane, oraz celu i podstawie prawnej takiego przekazywania. Dostęp do łączności elektronicznej jest w miejscu pracy dopuszczalny tylko ze względów bezpieczeństwa lub innych uzasadnionych powodów, przy czym pracodawca może go uzyskać wyłącznie po poinformowaniu pracowników o takiej ewentualności.

Pracownicy muszą mieć prawo dostępu do swoich danych o zatrudnieniu, jak też ich sprostowania lub usunięcia. Jeżeli są przetwarzane dane subiektywne, pracownicy muszą ponadto mieć prawo do zakwestionowania subiektywnych opinii. Prawa te mogą jednak zostać czasowo ograniczone do celów wewnętrznych dochodzeń. Jeżeli pracownikowi nie umożliwiono dostępu do danych osobowych o zatrudnieniu, ich sprostowania lub usunięcia, prawo krajowe musi zapewniać odpowiednie procedury odwołania się od takiej odmowy.

9.3. Dane dotyczące zdrowia

Najważniejsza kwestia

- Dane medyczne należą do kategorii danych wrażliwych, w związku z tym przysługuje im szczególna ochrona.

Dane osobowe o stanie zdrowia osoby, której dotyczą, są zakwalifikowane jako dane szczególnie chronione na mocy art. 9 ust. 1 ogólnego rozporządzenia

o ochronie danych i na mocy art. 6 zaktualizowanej konwencji nr 108. W związku z tym zasady przetwarzania danych dotyczących zdrowia są bardziej rygorystyczne niż w przypadku danych innych niż szczególnie chronione. Ogólne rozporządzenie o ochronie danych przewiduje zakaz przetwarzania „danych osobowych dotyczących zdrowia" (rozumianych jako „wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą"[934]) oraz danych genetycznych i biometrycznych, chyba że zastosowanie ma art. 9 ust. 2. Oba rodzaje danych ujęto na liście „szczególnych kategorii danych"[935].

Przykład: W sprawie *Z przeciwko Finlandii*[936] były mąż skarżącej, który był zarażony wirusem HIV, dopuścił się przestępstw seksualnych. Został on następnie skazany za zabójstwo, gdyż świadomie narażał swoje ofiary na ryzyko zakażenia HIV. Sąd krajowy utajnił pełne brzmienie wyroku i akta sprawy na okres 10 lat mimo wniosków skarżącej o dłuższy okres poufności. Wnioski te zostały odrzucone przez sąd apelacyjny, którego wyrok zawierał pełne nazwiska zarówno skarżącej, jak i jej byłego męża. ETPC uznał, że ingerencji tej nie można uznać za konieczną w demokratycznym społeczeństwie, ponieważ ochrona danych medycznych ma fundamentalne znaczenie dla korzystania z prawa do poszanowania życia prywatnego i rodzinnego, w szczególności w odniesieniu do informacji na temat zakażenia HIV ze względu na związane z tym piętno w wielu społeczeństwach. W związku z tym Trybunał uznał, że umożliwienie dostępu do informacji o tożsamości i stanie zdrowia skarżącej zgodnie z wyrokiem sądu apelacyjnego po zaledwie 10 latach od wydania wyroku naruszałoby art. 8 EKPC.

W **prawie UE** art. 9 ust. 2 lit. h) ogólnego rozporządzenia o ochronie danych dopuszcza przetwarzanie danych medycznych wówczas, gdy jest to niezbędne do celów profilaktyki zdrowotnej, diagnozy medycznej, zapewnienia opieki zdrowotnej bądź leczenia lub zarządzania usługami opieki zdrowotnej. Przetwarzanie danych jest jednak dopuszczalne tylko wtedy, gdy przetwarza je pracownik służby zdrowia

934 Ogólne rozporządzenie o ochronie danych, motyw 35.

935 Tamże, art. 2.

936 ETPC, *Z przeciwko Finlandii*, nr 22009/93, 25 lutego 1997 r., pkt 94 i 112; zob. także ETPC, *M.S. Przeciwko Szwecji*, nr 20837/92, 27 sierpnia 1997 r.; ETPC, *L.L. przeciwko Francji*, nr 7508/02, 10 października 2006 r.; ETPC, *I przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.; ETPC, *K.H. i in. przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.; ETPC, *Szuluk przeciwko Zjednoczonemu Królestwu*, nr 36936/05, 2 czerwca 2009 r.

podlegający obowiązkowi zachowania tajemnicy zawodowej lub inna osoba podlegająca równoważnemu obowiązkowi.

W **prawie RE** w zaleceniu RE w sprawie danych medycznych z 1997 r. do przetwarzania danych w dziedzinie medycyny zastosowano w sposób bardziej szczegółowy zasady zawarte w konwencji nr 108[937]. Proponowane przepisy są zgodne z zapisami ogólnego rozporządzenia o ochronie danych w odniesieniu do uzasadnionych celów przetwarzania danych medycznych, obowiązków w zakresie tajemnicy zawodowej, które należy nałożyć na osoby wykorzystujące dane dotyczące zdrowia, jak też praw osób, których dane dotyczą, do przejrzystości i dostępu, sprostowania oraz usunięcia danych. Ponadto dane medyczne przetwarzane zgodnie z prawem przez pracowników służby zdrowia nie mogą zostać przekazane organom ścigania, chyba że zapewniono „wystarczające zabezpieczenia, aby zapobiec ujawnieniu niezgodnemu z poszanowaniem [...] życia prywatnego zagwarantowanym na mocy art. 8 EKPC"[938]. Przepisy krajowe muszą ponadto być „formułowane wystarczająco precyzyjnie oraz zapewniać odpowiednią ochronę przed arbitralnością"[939].

Dodatkowo zalecenie w sprawie danych medycznych zawiera szczególne przepisy dotyczące danych medycznych dzieci nienarodzonych i osób niezdolnych do wyrażenia zgody oraz przetwarzania danych genetycznych. Za powód do przechowywania danych, gdy nie są one już potrzebne, wyraźnie uznano badania naukowe, choć zazwyczaj wymagana jest anonimizacja. W art. 12 zalecenia w sprawie danych medycznych zaproponowano szczegółowe regulacje dotyczące sytuacji, w których naukowcy potrzebują danych osobowych i dane zanonimizowane są niewystarczające.

Odpowiednim sposobem zaspokojenia potrzeb naukowych, a zarazem ochrony interesów pacjentów może być pseudonimizacja. Koncepcję pseudonimizacji w kontekście ochrony danych wyjaśniono bardziej szczegółowo w sekcji 2.1.1.

Do przetwarzania danych w dziedzinie medycyny odnosi się też zalecenie RE z 2016 r. w sprawie danych uzyskanych w wyniku testów genetycznych[940].

937 Rada Europy, Komitet Ministrów (1997), Recommendation Rec(97)5 to member states on the protection of medical data, 13 lutego 1997 r. Uwaga: Zalecenie znajduje się obecnie na etapie przeglądu.

938 ETPC, *Avilkina i in. przeciwko Rosji*, nr 1585/09, 6 czerwca 2013 r., pkt 53. Zob. także ETPC, *Biriuk przeciwko Litwie*, nr 23373/03, 25 listopada 2008 r.

939 ETPC, *L.H. przeciwko Łotwie*, nr 52019/07, 29 kwietnia 2014 r., pkt 59.

940 Rada Europy, Komitet Ministrów (2016), Recommendation Rec(2016)8 to member states on the processing of personal health-related data for insurance purposes, including data resulting from genetic tests, 26 października 2016 r.

Zalecenie to jest niezwykle ważne w dziedzinie e-zdrowia, w której technologie informacyjno-komunikacyjne (ICT) służą do usprawnienia świadczenia opieki zdrowotnej. Przykładem jest przesyłanie między dostawcami usług zdrowotnych wyników testów pacjenta na rodzicielstwo. Zalecenie to ma na celu ochronę praw osób, których dane osobowe są przetwarzane do celów ubezpieczenia przed ryzykiem związanym ze zdrowiem, integralnością cielesną, wiekiem bądź śmiercią danej osoby. Ubezpieczyciele muszą uzasadnić przetwarzanie danych dotyczących zdrowia i musi ono być proporcjonalne do charakteru i wagi rozpatrywanego ryzyka. Przetwarzanie takich danych osobowych wymaga zgody osoby, której dane dotyczą. Ubezpieczyciele powinni ponadto zapewniać zabezpieczenia w zakresie przechowywania danych dotyczących zdrowia.

Badania kliniczne, czyli udokumentowane próby nowych leków na pacjentach, mają poważne implikacje dla ochrony danych. Zagadnienia badań klinicznych produktów leczniczych przeznaczonych do stosowania przez człowieka uregulowano w rozporządzeniu (UE) Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE (rozporządzenie w sprawie badań klinicznych)[941]. Rozporządzenie w sprawie badań klinicznych obejmuje przede wszystkim następujące elementy:

- usprawniona procedura składania wniosków za pośrednictwem portalu UE[942];
- terminy oceny wniosku o pozwolenie na badanie kliniczne[943];
- uwzględnienie w procedurze oceny komisji etycznej, zgodnie z przepisami państw członkowskich (i europejskim prawem określającym terminy oceny)[944];
- zwiększona przejrzystość badań klinicznych i ich wyników[945].

W ogólnym rozporządzeniu o ochronie danych stwierdzono, że do celów wyrażenia zgody na udział w badaniach naukowych podczas prób klinicznych zastosowanie ma rozporządzenie (UE) nr 536/2014[946].

941 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE (rozporządzenie w sprawie badań klinicznych), Dz.U. L 158 z 27.5.2014.

942 Rozporządzenie w sprawie badań klinicznych, art. 5 ust. 1.

943 Tamże, art. 5 ust. 2–5.

944 Tamże, art. 2 ust. 2 pkt 11.

945 Tamże, art. 9 ust. 1 i motyw 67.

946 Ogólne rozporządzenie o ochronie danych, motywy 156 i 161.

Na szczeblu UE istnieje wiele inicjatyw legislacyjnych i innych w sprawie danych osobowych w sektorze ochrony zdrowia[947].

Elektroniczne karty zdrowia

W myśl definicji elektroniczna karta zdrowia oznacza „pełną ewidencję medyczną lub podobną dokumentację przeszłego i obecnego stanu zdrowia fizycznego i psychicznego osoby, przedstawioną w formie elektronicznej i umożliwiającą łatwą dostępność tych danych do leczenia lub innych ściśle związanych z tym celów"[948]. Elektroniczne karty zdrowia to elektroniczne wersje historii choroby pacjentów, które mogą obejmować dane kliniczne dotyczące tych osób, na przykład informacje o przebytych chorobach, problemach i schorzeniach, lekach i terapii oraz wyniki i raporty z badań i testów laboratoryjnych. Dostęp do takiej elektronicznej dokumentacji, która może obejmować całe karty zdrowia bądź zaledwie wyciągi z dokumentacji lub kartoteki, mogą uzyskać lekarz podstawowej opieki zdrowotnej, farmaceuta i inni pracownicy służby zdrowia. Koncepcja „e-zdrowia" również dotyczy takiej dokumentacji medycznej.

Przykład: Niejaki A wykupił polisę ubezpieczeniową w spółce B, będącej ubezpieczycielem. Spółka ta uzyska od A pewne informacje dotyczące zdrowia, na przykład problemów zdrowotnych bądź chorób, z którymi się boryka. Ubezpieczyciel powinien przechowywać dane osobowe A dotyczące jego zdrowia oddzielnie od innych danych. Musi również przechowywać te dane oddzielnie od innych danych osobowych. Oznacza to, że wyłącznie osoba rozpatrująca sprawę A będzie miała dostęp do danych dotyczących jego zdrowia.

Niemniej jednak elektroniczna dokumentacja zdrowotna wiąże się z pewnymi problemami dotyczącymi ochrony danych, takimi jak dostępność, właściwe przechowywanie i dostęp osoby, której dane dotyczą.

Oprócz podjęcia zagadnienia elektronicznych kart zdrowia 10 kwietnia 2014 r. Komisja Europejska opublikowała Zieloną księgę w sprawie mobilnego zdrowia („mHealth"), uznając, że m-zdrowie jest nową, coraz szybciej rozwijającą się dziedziną, która może odegrać rolę w przemianach w opiece zdrowotnej, a także

947 EIOD (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', Bruksela, 27 marca 2013 r.

948 Zalecenie Komisji z dnia 2 lipca 2008 r. w sprawie transgranicznej interoperacyjności systemów elektronicznych kart zdrowia, pkt 3 lit. c).

podnieść jej jakość i wydajność. Pojęcie m-zdrowia obejmuje działalność w obszarze medycyny i zdrowia publicznego wykonywaną przy użyciu urządzeń mobilnych, takich jak telefony komórkowe, urządzenia do monitorowania pacjentów, osobiści asystenci cyfrowi i inne urządzenia bezprzewodowe (na przykład aplikacje związane z dobrym samopoczuciem), które mogą łączyć się z wyrobami medycznymi bądź czujnikami[949]. W omawianym dokumencie nakreślono rodzaje ryzyka dla prawa do ochrony danych osobowych, z jakimi może się wiązać rozwój dziedziny m-zdrowia, oraz stwierdzono, że z uwagi na wrażliwy charakter danych dotyczących zdrowia rozwiązania w dziedzinie m-zdrowia powinny być wyposażone w specjalne, odpowiednie do tych celów zabezpieczenia, aby ograniczyć ryzyko. Do takich zabezpieczeń należy np. szyfrowanie danych pacjentów i właściwe mechanizmy uwierzytelniania pacjenta. Aby budować zaufanie do narzędzi m-zdrowia, niezbędna jest ich zgodność z zasadami ochrony danych osobowych, w tym przestrzeganie obowiązku informowania osoby, której dane dotyczą, zapewnienie bezpieczeństwa danych i zgodne z prawem przetwarzanie danych osobowych[950]. W związku z tym przedstawiciele tego sektora opracowali kodeks postępowania, który uwzględnia wkład szerokiego grona zainteresowanych stron, w tym przedstawicieli dysponujących wiedzą fachową z dziedzin ochrony danych, samoregulacji i współregulacji, ICT oraz opieki zdrowotnej[951]. W czasie opracowywania niniejszego podręcznika projekt kodeksu postępowania przedłożony Grupie Roboczej Art. 29 w celu przedstawienia uwag oczekiwał na zatwierdzenie.

9.4. Przetwarzanie danych do celów badań i do celów statystycznych

Najważniejsze kwestie

- Danych zgromadzonych do celów statystycznych oraz do celów badań naukowych lub historycznych nie wolno wykorzystywać do żadnych innych celów.
- Dane zgromadzone zgodnie z prawem w dowolnym celu mogą później zostać wykorzystane do celów statystycznych bądź do celów badań naukowych lub historycznych pod warunkiem, że przewidziano odpowiednie zabezpieczenia. W tym celu należy przewidzieć w szczególności anonimizację lub pseudonimizację danych przed przekazaniem ich osobom trzecim.

949 Komisja Europejska (2014), *Zielona księga w sprawie mobilnego zdrowia („mHealth")*, COM(2014) 219 final, Bruksela, 10 kwietnia 2014 r.

950 Tamże, s. 8.

951 Draft Code of Conduct on privacy for mobile health applications, 7 czerwca 2016 r.

Prawo UE dopuszcza przetwarzanie danych do celów statystycznych oraz do celów badań naukowych lub historycznych pod warunkiem zastosowania odpowiednich zabezpieczeń praw i wolności osób, których dane dotyczą. Może do nich należeć pseudonimizacja[952]. Prawo Unii lub prawo krajowe mogą przewidzieć określone wyjątki od praw osób, których dane dotyczą, jeżeli jest prawdopodobne, że prawa te uniemożliwią lub poważnie utrudnią realizację uzasadnionych celów badania[953]. Możliwe jest wprowadzenie odstępstw od prawa dostępu osoby, której dane dotyczą, prawa sprostowania danych, ograniczenia ich przetwarzania oraz prawa sprzeciwu.

Choć dane zgromadzone przez administratora zgodnie z prawem w jakimkolwiek celu mogą zostać przez niego ponownie wykorzystane do własnych celów statystycznych bądź celów badań naukowych lub historycznych, zanim zostałyby przekazane osobie trzeciej do celów statystycznych bądź do celów badań naukowych lub historycznych, musiałyby zostać zanonimizowane bądź na przykład spseudonimizowane – w zależności od sytuacji – chyba że osoba, której dane dotyczą, wyraziła zgodę na ponowne wykorzystanie w tych celach lub że taką możliwość wyraźnie przewiduje prawo krajowe. Dane spseudonimizowane pozostają objęte ogólnym rozporządzeniem o ochronie danych, w przeciwieństwie do danych anonimowych[954].

Jeżeli chodzi o ogólne przepisy dotyczące ochrony danych, rozporządzenie zapewnia zatem badaniom szczególne traktowanie, aby uniknąć ograniczania rozwoju badań oraz osiągnąć przewidziany w art. 179 TFUE cel, jakim jest utworzenie europejskiej przestrzeni badawczej. W akcie tym przewidziano szeroką interpretację przetwarzania danych osobowych do celów badań naukowych, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. W rozporządzeniu uznano też znaczenie łączenia danych z rejestrów do celów badań naukowych oraz dostrzeżono, że w momencie zebrania danych może nie być możliwe zidentyfikowanie w pełni późniejszego celu przetwarzania danych osobowych do celów badań naukowych[955]. Z tego względu rozporządzenie dopuszcza przetwarzanie danych do omówionych celów bez zgody osoby, której dane dotyczą, pod warunkiem że są stosowane odpowiednie zabezpieczenia.

952 Ogólne rozporządzenie o ochronie danych, art. 89 ust. 1.

953 Tamże, art. 89 ust. 2.

954 Tamże, motyw 26.

955 Tamże, motywy 33, 157 i 159.

Ważnym przykładem wykorzystania danych do celów statystycznych jest statystyka publiczna. Statystyki są uzyskiwane przez krajowe i unijne urzędy statystyczne zgodnie z unijnymi i krajowymi przepisami w zakresie statystyki publicznej. W myśl tych uregulowań obywatele i przedsiębiorstwa są zazwyczaj zobowiązani do ujawniania danych właściwym organom statystycznym. Urzędnicy pracujący w urzędach statystycznych są związani specjalnym obowiązkiem zachowania tajemnicy zawodowej. Trzeba go skrupulatnie przestrzegać, gdyż jest on warunkiem wysokiego poziomu zaufania obywateli, który jest niezbędny, aby dane były udostępniane organom statystycznym[956].

Rozporządzenie (WE) nr 223/2009 w sprawie statystyki europejskiej (rozporządzenie w sprawie statystyki europejskiej) zawiera podstawowe przepisy dotyczące ochrony danych w związku ze statystyką publiczną, dlatego też można je uznać za istotne także z punktu widzenia przepisów o statystyce publicznej na szczeblu krajowym[957]. W rozporządzeniu utrzymano zasadę, że dla urzędowych działań statystycznych niezbędna jest wystarczająco precyzyjna podstawa prawna[958].

Przykład: W sprawie *Heinz Huber przeciwko Bundesrepublik Deutschland*[959] austriacki przedsiębiorca zamieszkały w Niemczech zaskarżył gromadzenie i przechowywanie danych osobowych cudzoziemców przez niemieckie organy w centralnym rejestrze (AZR) również do celów statystycznych, twierdząc, że narusza to jego prawa wynikające z dyrektywy o ochronie danych. Zważywszy że dyrektywa 95/46 ma zapewniać jednolity poziom ochrony we wszystkich państwach członkowskich, TSUE uznał, że aby zagwarantować wysoki poziom ochrony w UE, pojęcie konieczności w rozumieniu art. 7 lit. e) dyrektywy nie może mieć różnego zakresu

956 Tamże, art. 90.

957 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009 z dnia 11 marca 2009 r. w sprawie statystyki europejskiej oraz uchylające rozporządzenie Parlamentu Europejskiego i Rady (WE, Euratom) nr 1101/2008 w sprawie przekazywania do Urzędu Statystycznego Wspólnot Europejskich danych statystycznych objętych zasadą poufności, rozporządzenie Rady (WE) nr 322/97 w sprawie statystyk Wspólnoty oraz decyzję Rady 89/382/EWG, Euratom w sprawie ustanowienia Komitetu ds. Programów Statystycznych Wspólnot Europejskich, Dz.U. L 87 z 31.3.2009, zmienione rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 2015/759 z dnia 29 kwietnia 2015 r. zmieniającym rozporządzenie (WE) nr 223/2009 w sprawie statystyki europejskiej, Dz.U. L 123 z 19.5.2015.

958 Zasada ta ma zostać bardziej szczegółowo sformułowana w kodeksie praktyk Eurostatu , który zgodnie z art. 11 rozporządzenia w sprawie statystyki europejskiej zawiera wskazówki etyczne dotyczące sposobu realizowania działań statystyki publicznej, w tym właściwego sposobu wykorzystania danych osobowych.

959 TSUE, C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r., zob. zwłaszcza pkt 68.

w poszczególnych państwach członkowskich. Jest to zatem autonomiczne pojęcie prawa UE, którego wykładnia musi w pełni odpowiadać celowi dyrektywy 95/46. Trybunał zauważył, że do celów statystycznych wystarczy przetwarzanie informacji anonimowych, i orzekł, że niemiecki rejestr nie był zgodny z wymogiem konieczności przewidzianym w art. 7 lit. e) dyrektywy.

Jeżeli chodzi o prawo **RE**, dalsze przetwarzanie danych osobowych do celów badań naukowych lub historycznych bądź do celów statystycznych jest możliwe wówczas, gdy leży to w interesie publicznym, przy czym musi być objęte odpowiednimi zabezpieczeniami[960]. Prawa osób, których dane dotyczą, mogą zostać ograniczone również w przypadku przetwarzania danych do celów statystycznych, pod warunkiem że w oczywisty sposób brak jest ryzyka naruszenia ich praw i wolności[961].

Wydane w 1997 r. zalecenie w sprawie danych statystycznych dotyczy sporządzania statystyk w sektorach publicznym i prywatnym[962].

Danych zgromadzonych przez administratora do celów statystycznych nie wolno wykorzystywać do żadnych innych celów. Dane, które zgromadzono do celów innych niż statystyczne, można później wykorzystać do celów statystycznych. W zaleceniu w sprawie danych statystycznych zezwala się również na przekazywanie danych osobom trzecim, jeżeli następuje to tylko w celach statystycznych. W takich przypadkach strony powinny uzgodnić w formie pisemnej zakres uzasadnionego dalszego wykorzystania do celów statystycznych. Jako że takie porozumienie nie może zastąpić zgody osoby, której dane dotyczą – jeżeli jest wymagana – w prawie krajowym muszą zostać dodatkowo ustanowione odpowiednie zabezpieczenia w celu minimalizacji ryzyka niewłaściwego wykorzystania danych osobowych, takie jak obowiązek anonimizacji lub pseudonimizacji danych przed ich ujawnieniem.

Na osoby zajmujące się zawodowo badaniami statystycznymi należy nałożyć na mocy prawa krajowego specjalne obowiązki zachowania tajemnicy zawodowej, co jest powszechne w przypadku statystyki publicznej. Obowiązki te należy rozszerzyć także na ankieterów i inne osoby zajmujące się zbieraniem danych osobowych,

960 Zaktualizowana konwencja nr 108, art. 5 ust. 4 lit. b).

961 Tamże, art. 11 ust. 2.

962 Rada Europy, Komitet Ministrów (1997), Recommendation Rec(97)18 to Member States on the protection of personal data collected and processed for statistical purposes, 30 września 1997 r.

jeżeli uczestniczą oni w gromadzeniu danych od osób, których dane dotyczą, lub innych osób.

Jeżeli badanie statystyczne z wykorzystaniem danych osobowych nie jest wymagane prawem, może być konieczne wyrażenie zgody przez osoby, których dane dotyczą, na wykorzystanie ich danych, aby było ono zgodne z prawem, lub trzeba im co najmniej umożliwić wyrażenie sprzeciwu. Jeżeli dane osobowe do celów statystycznych są gromadzone przez ankieterów, respondentów należy wyraźnie poinformować, czy ujawnianie danych jest obowiązkowe na mocy prawa krajowego, czy też nie.

W przypadku gdy badań statystycznych nie można przeprowadzić z użyciem danych anonimowych i niezbędne jest wykorzystanie danych osobowych, dane zgromadzone w tym celu należy zanonimizować, gdy tylko będzie to możliwe. Wyniki badań statystycznych nie mogą co najmniej umożliwiać identyfikacji żadnych osób, których dane dotyczą, chyba że w sposób oczywisty nie stwarza to zagrożenia.

Po zakończeniu analizy statystycznej wykorzystane dane osobowe należy usunąć lub zanonimizować. W tym przypadku w zaleceniu w sprawie danych statystycznych sugeruje się, aby dane identyfikacyjne były przechowywane oddzielnie od pozostałych danych osobowych. Oznacza to na przykład, że klucz kryptograficzny lub listę identyfikujących synonimów należy przechowywać oddzielnie od innych danych.

9.5. Dane finansowe

Najważniejsze kwestie

- Chociaż dane finansowe nie są danymi szczególnie chronionymi w rozumieniu zaktualizowanej konwencji nr 108 lub ogólnego rozporządzenia o ochronie danych, ich przetwarzanie wymaga szczególnych zabezpieczeń w celu zapewnienia prawidłowości i bezpieczeństwa danych.
- Elektroniczne systemy płatnicze muszą cechować się wbudowaną ochroną danych, czyli uwzględnieniem ochrony prywatności już w fazie projektowania i domyślną ochroną danych.
- Szczególne problemy związane z ochroną danych w tym obszarze wynikają z potrzeby wdrożenia odpowiednich mechanizmów uwierzytelnienia.

Przykład: W sprawie *Michaud przeciwko Francji*[963] skarżący, który był francuskim prawnikiem, zakwestionował ciążący na nim na mocy prawa francuskiego obowiązek zgłaszania podejrzeń dotyczących możliwego prania pieniędzy przez jego klientów. ETPC zauważył, że wymaganie od prawników, aby przekazywali organom administracyjnym informacje dotyczące innej osoby, w których posiadanie weszli wskutek kontaktów z tą osobą na gruncie zawodowym, stanowi ingerencję w prawo prawników do poszanowania ich korespondencji i życia prywatnego na mocy art. 8 EKPC, gdyż pojęcie to obejmuje działania o charakterze zawodowym lub biznesowym. Ingerencja ta jest jednak zgodna z prawem i służy uzasadnionemu celowi, a mianowicie ochronie porządku oraz zapobieganiu przestępstwom. Jako że prawnicy podlegają obowiązkowi zgłaszania swoich podejrzeń tylko w bardzo ograniczonej liczbie przypadków, ETPC uznał, że zobowiązanie to jest proporcjonalne, i stwierdził, że nie doszło do naruszenia art. 8.

Przykład: W sprawie *M.N. i in. przeciwko San Marino*[964] skarżący, obywatel Włoch, zawarł umowę powierniczą z przedsiębiorstwem objętym dochodzeniem. Oznaczało to, że przeszukano i zajęto kopie dokumentacji (elektronicznej) spółki. Skarżący złożył skargę do sądu w San Marino, w której stwierdził, że nie ma związku między nim a domniemanymi przestępstwami. Sąd uznał jednak jego skargę za niedopuszczalną, ponieważ nie był on „zainteresowaną osobą". ETPC uznał, że jeśli chodzi o ochronę sądową skarżący znajdował się w znacznie bardziej niekorzystnej sytuacji niż „zainteresowana osoba", a mimo to jego dane zostały objęte operacjami przeszukania i zajęcia. Z tego względu Trybunał stwierdził naruszenie art. 8.

Przykład: W sprawie *G.S.B. przeciwko Szwajcarii*[965] dane rachunku bankowego skarżącego przesłano do amerykańskich organów podatkowych na podstawie umowy o współpracy administracyjnej zawartej między Szwajcarią a USA. ETPC uznał, że przekazanie danych nie naruszało art. 8 EKPC, ponieważ ingerencja w prawo skarżącego do prywatności była przewidziana przez ustawę, służyła uzasadnionemu celowi oraz była proporcjonalna w świetle interesu publicznego dochodzącego do głosu w tej sprawie.

963 ETPC, *Michaud przeciwko Francji*, nr 12323/11, 6 grudnia 2012 r. Zob. także ETPC, *Niemietz przeciwko Niemcom*, nr 13710/88, 16 grudnia 1992 r., pkt 29; oraz ETPC, *Halford przeciwko Zjednoczonemu Królestwu*, nr 20605/92, 25 czerwca 1997 r., pkt 42.

964 ETPC, *M.N. i in. przeciwko San Marino*, nr 28005/12, 7 lipca 2015 r.

965 ETPC, *G.S.B. przeciwko Szwajcarii*, nr 28601/11, 22 grudnia 2015 r.

RE określiła zasady stosowania ogólnych ram prawnych ochrony danych zapisanych w konwencji nr 108 w kontekście płatności w zaleceniu Rec(90)19 z 1990 r.[966]. W zaleceniu tym sprecyzowano zakres zgodnego z prawem gromadzenia i wykorzystywania danych w kontekście płatności, zwłaszcza z użyciem kart płatniczych. Dodatkowo zawiera ono szczegółowe zalecenia dla ustawodawców krajowych odnoszące się do regulacji dotyczących ujawniania danych o płatnościach osobom trzecim, terminów przechowywania danych, przejrzystości, bezpieczeństwa danych i transgranicznego przepływu danych, jak też nadzoru oraz środków prawnych. RE opracowała też opinię w sprawie przekazywania danych podatkowych[967], w której przedstawiła zalecenia oraz kwestie, które należy uwzględnić przy przekazywaniu takich danych.

ETPC dopuszcza przekazywanie danych finansowych – zwłaszcza danych rachunku bankowego danej osoby – w ramach art. 8 EKPC, jeżeli przekazanie danych jest przewidziane przez ustawę, służy uzasadnionemu celowi i jest proporcjonalne do interesu publicznego dochodzącego do głosu w danej sprawie[968].

Jeżeli chodzi o **prawo UE**, elektroniczne systemy płatności, w których przetwarza się dane osobowe, muszą być zgodne z ogólnym rozporządzeniem o ochronie danych. Z tego względu takie systemy muszą uwzględniać ochronę danych w fazie projektowania oraz zapewniać domyślną ochronę danych. Uwzględnienie ochrony danych w fazie projektowania oznacza, że administrator ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapewnić przestrzeganie zasad ochrony danych. Domyślna ochrona danych zakłada, że administrator musi zagwarantować, by domyślnie przetwarzane były tylko te dane osobowe, które są niezbędne do określonego celu (zob. sekcja 4.4). W sprawie danych finansowych, TSUE uznał, że przekazywane dane podatkowe mogą stanowić dane osobowe[969]. Grupa Robocza Art. 29 wydała powiązane wytyczne dla państw członkowskich, w których omówiła między innymi kryteria zapewniania zgodności z przepisami z zakresu ochrony danych odnoszące się do zautomatyzowanej wymiany danych osobowych do celów

966 Rada Europy, Komitet Ministrów (1990), Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations, 13 września 1990 r.

967 Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108(2014), Opinion on the implication for data protection of mechanisms for automatic inter-state exchanges of data for administrative and tax purposes, 4 czerwca 2014 r.

968 ETPC, *G.S.B. przeciwko Szwajcarii*, nr 28601/11, 22 grudnia 2015 r.

969 TSUE, C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 1 października 2015 r., pkt 29.

podatkowych[970]. Ponadto uchwalono szereg aktów prawnych dotyczących regulacji rynków instrumentów finansowych oraz działalności instytucji kredytowych i firm inwestycyjnych[971]. Inne akty prawne pomagają w zwalczaniu wykorzystywania informacji wewnętrznych i manipulacji na rynku[972]. Najważniejszymi obszarami, które wywierają wpływ na ochronę danych, są:

- zatrzymywanie zapisów dotyczących transakcji finansowych;
- przekazywanie danych osobowych do państw trzecich;
- rejestrowanie rozmów telefonicznych lub komunikacji elektronicznej, w tym uprawnienia właściwych organów do żądania rejestrów połączeń telefonicznych i przesyłu danych;
- ujawnianie danych osobowych, w tym publikacja sankcji;
- uprawnienia nadzorcze i dochodzeniowe właściwych organów, w tym do kontroli na miejscu oraz wejścia na teren prywatny w celu zajęcia dokumentów;
- mechanizmy zgłaszania naruszeń, tj. zasady sygnalizowania nieprawidłowości; oraz
- współpraca między właściwymi organami państw członkowskich oraz Europejskim Urzędem Nadzoru Giełd i Papierów Wartościowych (ESMA).

970 Grupa Robocza Art. 29 (2015), *Statement of the WP 29 on automatic inter-state exchanges of personal data for tax purposes*, WP 230.

971 Dyrektywa Parlamentu Europejskiego i Rady 2014/65/UE z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniająca dyrektywę 2002/92/WE i dyrektywę 2011/61/UE, Dz.U. L 173 z 12.6.2014; rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 600/2014 z dnia 15 maja 2014 r. w sprawie rynków instrumentów finansowych oraz zmieniające rozporządzenie (EU) nr 648/2012, Dz.U. L 173 z 12.6.2014; dyrektywa Parlamentu Europejskiego i Rady 2013/36/UE z dnia 26 czerwca 2013 r. w sprawie warunków dopuszczenia instytucji kredytowych do działalności oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi, zmieniająca dyrektywę 2002/87/WE i uchylająca dyrektywy 2006/48/WE oraz 2006/49/WE, Dz.U. L 176 z 27.6.2013.

972 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 596/2014 z dnia 16 kwietnia 2014 r. w sprawie nadużyć na rynku (rozporządzenie w sprawie nadużyć na rynku) oraz uchylające dyrektywę 2003/6/WE Parlamentu Europejskiego i Rady i dyrektywy Komisji 2003/124/WE, 2003/125/WE i 2004/72/WE, Dz.U. L 173 z 12.6.2014.

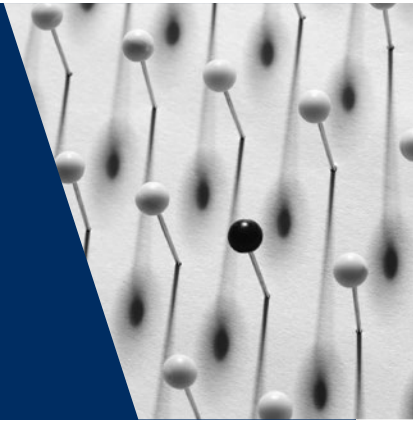
W tej dziedzinie występują także inne konkretnie wskazane zagadnienia, w tym gromadzenie danych na temat sytuacji finansowej osób, których dane dotyczą[973], bądź płatności transgraniczne przy wykorzystaniu przelewów bankowych, które muszą ze swojej natury prowadzić do przepływu danych osobowych[974].

973 Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1060/2009 z dnia 16 września 2009 r. w sprawie agencji ratingowych, Dz.U. L 302 z 17.11.2009, ostatnio zmienione dyrektywą Parlamentu Europejskiego i Rady 2014/51/UE z dnia 16 kwietnia 2014 r. zmieniającą dyrektywy 2003/71/WE i 2009/138/WE oraz rozporządzenia (WE) nr 1060/2009, (UE) nr 1094/2010 i (UE) nr 1095/2010 w zakresie uprawnień Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Ubezpieczeń i Pracowniczych Programów Emerytalnych) oraz Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Giełd i Papierów Wartościowych), Dz.U. L 153 z 22.5.2014; rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 462/2013 z dnia 21 maja 2013 r. zmieniające rozporządzenie (WE) nr 1060/2009 w sprawie agencji ratingowych, Dz.U. L 146 z 31.5.2013.

974 Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE, Dz.U. L 319 z 5.12.2007, zmieniona dyrektywą Parlamentu Europejskiego i Rady 2009/111/WE z dnia 16 września 2009 r. zmieniającą dyrektywy 2006/48/WE, 2006/49/WE i 2007/64/WE w odniesieniu do banków powiązanych z centralnymi instytucjami, niektórych pozycji funduszy własnych, dużych ekspozycji, uzgodnień w zakresie nadzoru oraz zarządzania w sytuacji kryzysowej, Dz.U. L 302 z 17.11.2009.

10

Współczesne wyzwania związane z ochroną danych osobowych



Epoka cyfrowa, zwana też epoką technologii informacyjnej, charakteryzuje się powszechnym korzystaniem z komputerów, Internetu i technologii cyfrowych. Wiąże się to z gromadzeniem i przetwarzaniem ogromnych ilości danych, również danych osobowych. Zbieranie i przetwarzanie danych osobowych w zglobalizowanej gospodarce pociąga za sobą zwielokrotnienie transgranicznych przepływów danych. Takie przetwarzanie danych może być źródłem znacznych i dostrzegalnych korzyści na co dzień: wyszukiwarki ułatwiają dostęp do ogromnych zasobów informacji i wiedzy, usługi sieci społecznościowych umożliwiają ludziom z różnych zakątków świata komunikację, wyrażanie opinii i zwiększanie poparcia dla ważnych inicjatyw społecznych, środowiskowych i politycznych, natomiast firmy i konsumenci czerpią z zalet skutecznych i wydajnych technik marketingowych, które pobudzają rozwój gospodarki. Technologia i przetwarzanie danych osobowych to także narzędzia niezbędne organom państwowym do zwalczania przestępczości i terroryzmu. Wykorzystanie technologii dużych zbiorów danych (Big Data) – czyli zbieranie, przechowywanie i analiza dużych ilości informacji w celu identyfikowania wzorców i prognozowania zachowań – również „może być bardzo wartościowe dla społeczeństwa, gdyż zwiększa produktywność, poprawia skuteczność działania sektora publicznego i sprzyja udziałowi obywateli w życiu społecznym”[975].

Mimo licznych korzyści epoka cyfrowa rodzi też wyzwania związane z ochroną prywatności i danych, ponieważ umożliwia gromadzenie i przetwarzanie ogromnych ilości danych osobowych w coraz bardziej nieprzejrzysty i złożony sposób. Postęp technologiczny doprowadził do rozwinięcia ogromnych zbiorów danych, które

975 Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasburg, 23 stycznia 2017 r.

można z łatwością ze sobą zestawiać oraz dalej analizować w celu identyfikacji wzorców lub podejmowania decyzji na podstawie algorytmów, co zapewnia niespotykany do tej pory wgląd w zachowanie ludzi i ich życie prywatne[976].

Nowe technologie dają ogromne możliwości i mogą być szczególnie niebezpieczne, gdy dostaną się w niepowołane ręce. O ogromnym wpływie tych technologii na prawa osób fizycznych świadczy na przykład potencjalne wykorzystywanie ich przez władze państwowe do masowej inwigilacji obywateli. W 2013 r. informacje ujawnione przez Edwarda Snowdena na temat szeroko zakrojonych programów niejawnego nadzoru komunikacji internetowej i telefonicznej przez agencje wywiadowcze w niektórych państwach wzbudziły ogromne obawy dotyczące zagrożeń, jakie inwigilacja niesie ze sobą w sferze prywatności, demokratycznych rządów i wolności wypowiedzi. Masowa inwigilacja i technologie umożliwiające przechowywanie i przetwarzanie danych osobowych w wymiarze globalnym oraz masowy dostęp do danych mogą uderzać w samą istotę prawa do prywatności[977]. Ponadto mogą niekorzystnie wpływać na kulturę polityczną, a także osłabiać demokrację, tłumić kreatywność i hamować innowacje[978]. Sama obawa przed ciągłym śledzeniem i analizowaniem zachowań i działań obywateli przez państwo może zniechęcać ich do wyrażania opinii na określone tematy oraz powodować nieufność i podejrzliwość[979]. Wyzwania te skłoniły szereg organów państwowych, ośrodków badawczych i organizacji społeczeństwa obywatelskiego do przeanalizowania potencjalnego wpływu nowych technologii na społeczeństwo. W 2015 r. Europejski Inspektor Ochrony Danych podjął kilka inicjatyw mających na celu ocenę etycznych implikacji dużych zbiorów danych i Internetu rzeczy. Przede wszystkim EIOD powołał grupę doradczą ds. etyki, która ma na celu rozpoczęcie „otwartej i opartej na wiedzy dyskusji na temat etyki cyfrowej, która pozwala UE realizować potencjał technologii na rzecz społeczeństwa i gospodarki, a jednocześnie wzmacniać prawa

976 Parlament Europejski (2017), Rezolucja w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw, P8_TA-PROV(2017)0076, Strasburg, 14 marca 2017 r.

977 Zob. ONZ, Zgromadzenie Ogólne, *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 września 2014 r., pkt 59. Zob. także ETPC, *Factsheet on Mass surveillance*, lipiec 2017 r.

978 EIOD (2015), *Sprostanie wyzwaniom związanym z dużymi zbiorami danych*, Opinia 7/2015, Bruksela, 19 listopada 2015 r.

979 TSUE, sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r., pkt 37.

i swobody osób, w szczególności ich prawa do poszanowania prywatności i ochrony danych”[980].

Przetwarzanie danych osobowych to również potężne narzędzie w rękach przedsiębiorstw. Obecnie w wyniku przetwarzania danych można uzyskać szczegółowe informacje o stanie zdrowia lub sytuacji finansowej, które następnie służą przedsiębiorstwom do podejmowania istotnych decyzji dotyczących osób fizycznych, na przykład ustalania wysokości pobieranej od nich składki na ubezpieczenie zdrowotne czy oceny ich zdolności kredytowej. Techniki przetwarzania danych wykorzystywane przez polityków bądź przedsiębiorstwa z myślą o wpłynięciu na wyniki wyborów – przykładowo poprzez „mikrotargetowanie” komunikacji wyborców – mogą również oddziaływać na procesy demokratyczne. Innymi słowy, podczas gdy prywatność była pierwotnie postrzegana jako prawo do ochrony osób fizycznych przed nieuzasadnioną ingerencją ze strony organów publicznych, współcześnie zagrożeniem dla niej mogą być również podmioty prywatne. Rodzi to pytania o wykorzystanie technologii i analityki predykcyjnej przy podejmowaniu decyzji dotyczących życia codziennego ludzi i sprawia, że potrzeba zapewnienia, by przetwarzanie danych osobowych w każdej sytuacji odbywało się z poszanowaniem wymogów w zakresie praw podstawowych, jest jeszcze bardziej paląca.

Ochrona danych nierozerwalnie łączy się ze zmianami technologicznymi, społecznymi i politycznymi. Niemożliwe byłoby zatem sporządzenie kompletnej listy wyzwań, z jakimi przyjdzie nam się zmierzyć w przyszłości. W niniejszym rozdziale omówiono bliżej wybrane zagadnienia dotyczące dużych zbiorów danych, internetowych sieci społecznościowych i jednolitego rynku treści cyfrowych UE. Nie służy on wyczerpującej analizie tych obszarów z perspektywy ochrony danych osobowych, a podkreśleniu rozlicznych możliwych interakcji między nowymi bądź zmodyfikowanymi działaniami człowieka a ochroną danych.

980 EIOD, Decyzja z dnia 3 grudnia 2015 r. ustanawiająca zewnętrzną grupę doradczą ds. etycznych wymiarów ochrony danych („grupę doradczą ds. etyki”), 3 grudnia 2015 r., motyw 5.

10.1. Duże zbiory danych, algorytmy i sztuczna inteligencja

Najważniejsze kwestie

- Rewolucyjne innowacje w dziedzinie technologii informacyjno-komunikacyjnych (ICT) kształtują nowy obraz świata, w którym relacje społeczne, działalność gospodarcza oraz usługi sektora prywatnego i publicznego są wzajemnie połączone cyfrowo, przez co generują coraz większe ilości danych, często danych osobowych.
- Rządy, przedsiębiorstwa i obywatele funkcjonują w gospodarce w coraz większej mierze zależnej od danych, w której dane same w sobie stanowią wartościowe zasoby.
- Koncepcja dużych zbiorów danych (Big Data) odnosi się zarówno do samych danych, jak i do analiz danych.
- Dane osobowe przetwarzane w ramach analizy dużych zbiorów są objęte prawodawstwem UE i RE.
- Odstępstwa od przepisów i praw w zakresie ochrony danych dopuszcza się wyłącznie w przypadku wybranych praw i konkretnych sytuacji, gdy wykonanie prawa byłoby niemożliwe bądź wymagałoby od administratorów danych niewspółmiernego wysiłku.
- W pełni zautomatyzowane podejmowanie decyzji jest co do zasady zabronione, z wyjątkiem określonych przypadków.
- Świadomość osób fizycznych i oddanie w ich ręce kontroli nad danymi są kluczowe dla skutecznego wykonywania praw.

W świecie coraz bardziej zależnym od technologii cyfrowych wszystkie działania pozostawiają ślady cyfrowe, które można zgromadzić, przetworzyć i ocenić bądź przeanalizować. Nowe technologie informacyjno-komunikacyjne powodują, że ilość gromadzonych i rejestrowanych danych stale rośnie[981]. Do niedawna żadna technologia nie była w stanie analizować i oceniać masowych ilości danych ani wyciągać rzeczowych wniosków na ich podstawie. Danych było po prostu zbyt wiele, by można je było ocenić, oraz były one zbyt złożone, nieustrukturyzowane i dynamiczne, by umożliwić identyfikację tendencji i przyzwyczajeń.

981 Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ku gospodarce opartej na danych", COM(2014) 442 final, Bruksela, 2 lipca 2014 r.

10.1.1. Duże zbiory danych, algorytmy i sztuczna inteligencja – definicje

Duże zbiory danych (big data)

Termin „big data" to popularny zwrot, który w zależności od kontekstu może opisywać różne zjawiska. Zazwyczaj odnosi się do „rosnących możliwości technologicznych w zakresie gromadzenia, przetwarzania i wyciągania nowych i predykcyjnych wniosków z dużych ilości danych o różnej szybkości przetwarzania i dużej różnorodności"[982]. Pojęcie dużych zbiorów danych obejmuje zatem zarówno same dane, jak i analizy danych.

Dane te pochodzą z rozmaitych źródeł, wśród których można wymienić ludzi i ich dane osobowe, maszyny lub czujniki, informacje dotyczące klimatu, obrazy satelitarne, zdjęcia i filmy w postaci cyfrowej i sygnały GPS. Dużą część danych i informacji stanowią jednak dane osobowe – mogą one obejmować wszelkie informacje takie jak nazwiska, zdjęcia, adresy e-mail, dane rachunków bankowych, dane GPS, wpisy w sieciach społecznościowych, informacje medyczne lub adresy IP komputerów[983].

Koncepcja dużych zbiorów danych odnosi się też do **przetwarzania**, analizy i oceny masowych ilości danych i dostępnych informacji, np. z myślą o zgromadzeniu przydanych informacji na potrzeby analiz dużych zbiorów danych. Oznacza to, że zbierane dane i informacje można wykorzystać do celów innych niż pierwotnie przewidziane, np. do analizy trendów statystycznych lub świadczenia bardziej zindywidualizowanych usług, takich jak reklamy. W obszarach, w których są dostępne technologie umożliwiające zbieranie, przetwarzanie i ocenę dużych zbiorów danych, połączyć i przeanalizować można dowolny rodzaj informacji: transakcje finansowe, zdolność kredytową, informacje o leczeniu, spożyciu prywatnym, działalności zawodowej, dane śledzenia i informacje o obranych trasach, korzystaniu z Internetu, kartach elektronicznych i smartfonach, oraz dane z monitoringu wizyjnego lub

982 Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 2; Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ku gospodarce opartej na danych", COM(2014) 442 final, Bruksela, 2 lipca 2014 r., s. 4; Międzynarodowy Związek Telekomunikacyjny (2015), Recommendation Y.3600. Big Data – Cloud computing based requirements and capabilities.

983 Komisja Europejska, Reforma ochrony danych w UE a duże zbiory danych, zestawienie informacji; Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 2.

monitorowania komunikacji. Analizy dużych zbiorów danych nadają danym nowy wymiar ilościowy, który można ocenić i wykorzystać w czasie rzeczywistym na przykład po to, aby dostarczać konsumentom spersonalizowane usługi.

Algorytmy i sztuczna inteligencja

Sztuczna inteligencja (AI) odnosi się do inteligencji maszyn działających w charakterze „inteligentnych agentów". Jako inteligentni agenci określone urządzenia mogą – z pomocą oprogramowania – postrzegać otoczenie i podejmować działania na podstawie algorytmów. O sztucznej inteligencji mówi się wówczas, gdy maszyna imituje funkcje „kognitywne" – takie jak uczenie się i rozwiązywanie problemów – typowo kojarzone z ludźmi[984]. Aby podobnie do ludzi podejmować decyzje, współczesne technologie i oprogramowanie korzystają z algorytmów, za pomocą których urządzenia podejmują „zautomatyzowane decyzje". Najprościej mówiąc, algorytm to procedura określająca krok po kroku sposób obliczania, przetwarzania danych, oceny i zautomatyzowanego wnioskowania i podejmowania decyzji.

Podobnie jak duże zbiory danych, sztuczna inteligencja i zautomatyzowane podejmowanie decyzji, które AI umożliwia, wymagają zestawienia i przetworzenia dużych ilości danych. Źródłem tych danych może być samo urządzenie (temperatura hamulców, stan paliwa itp.) lub jego otoczenie. Przykładowo proces profilowania może opierać się na zautomatyzowanym podejmowaniu decyzji na podstawie wstępnie definiowanych wzorców lub czynników.

Przykład: Profilowanie i reklamy ukierunkowane

Profilowanie na podstawie dużych zbiorów danych polega na identyfikowaniu wzorców odzwierciedlających „cechy osobowości" – na przykład gdy sprzedawcy internetowi sugerują kupującym produkty, które również mogą im się spodobać, na podstawie informacji o produktach umieszczonych przez nich w koszyku. Im więcej danych, tym precyzyjniejszy obraz się rysuje. Smartfon jest na przykład swoistym rozbudowanym kwestionariuszem, uzupełnianym przez użytkownika – świadomie i nieświadomie – z każdym użyciem.

984 Stuart Russel i Peter Norvig, *Artificial Intelligence: A Modern Approach (2nd ed.)*, 2003, Upper Saddle River, New Jersey: Prentice Hall, s. 27, 32–58, 968–972; Stuart Russel i Peter Norvig, *Artificial Intelligence: A Modern Approach (3rd ed.)*, 2009, Upper Saddle River, New Jersey: Prentice Hall, s. 2.

Współczesna psychografia – dziedzina zajmująca się badaniem osobowości – wykorzystuje metodę OCEAN do ustalania, z jakim typem osobowości ma się do czynienia. „Wielka piątka" czynników osobowości obejmuje otwartość (na nowe doświadczenia, ang. *openness*), sumienność (skłonność do perfekcjonizmu, ang. *conscientiousness*), ekstrawersję (towarzyskość, ang. *extraversion*), ugodowość (nastawienie do ludzi, ang. *agreeableness*) i neurotyczność (podatność na negatywne stany emocjonalne, ang. *neuroticism*). Informacje te pozwalają sprofilować daną osobę, poznać jej potrzeby i obawy, przewidzieć zachowania itp. Uzupełniają je inne informacje o danej osobie zebrane z dostępnych źródeł – od brokerów informacji, sieci społecznościowych (w tym „polubienia" pod wpisami i opublikowane zdjęcia) po muzykę odtwarzaną w Internecie czy dane GPS i dane śledzenia.

Ogromna liczba profili tworzonych za pomocą technik analizy dużych zbiorów danych jest następnie porównywana w celu identyfikacji podobnych wzorców i grup osobowości. Informacje o zachowaniach i postawach właściwych dla określonych typów temperamentu są zatem odwracane. Dostęp do dużych zbiorów danych i ich wykorzystanie powodują odwrócenie testu osobowości w taki sposób, że informacje o zachowaniach i postawach służą do opisania osobowości danej osoby. Łącząc informacje o „polubieniach" w sieciach społecznościowych, dane śledzenia, informacje o odtworzonej muzyce lub obejrzanych filmach, można uzyskać jasny obraz charakteru danej osoby, co pozwala przedsiębiorstwom kierować do niej spersonalizowane reklamy lub informacje, dopasowane do jej „osobowości". Co najważniejsze, informacje te można przetwarzać w czasie rzeczywistym[985].

10.1.2. Osiągnięcie równowagi między zaletami dużych zbiorów danych a związanym z nimi ryzykiem

Współczesne techniki przetwarzania danych umożliwiają obsługę masowych ilości danych, szybkie importowanie nowych danych, przetwarzanie informacji w czasie rzeczywistym, tj. krótki czas odpowiedzi (nawet w przypadku złożonych żądań),

985 Techniki przetwarzania i nowe oprogramowanie analizują w czasie rzeczywistym informacje o upodobaniach danej osoby, produktach przeglądanych podczas zakupów w Internecie lub artykułach dodanych do koszyka, dzięki czemu mogą na podstawie zgromadzonych informacji „zaproponować" kolejne produkty, które mogą taką osobę zainteresować.

pozwalają na zgłaszanie wielu żądań jednocześnie oraz analizują różne typy informacji (zdjęcia, tekst lub liczby). Te innowacje technologiczne umożliwiają strukturyzowanie, przetwarzanie i analizę masowych ilości danych i informacji w czasie rzeczywistym[986]. Zwiększając wykładniczo ilość dostępnych i analizowanych danych, można osiągać wyniki, których nie da się uzyskać w drodze analiz zakrojonych na mniejszą skalę. Duże zbiory danych przyczyniły się do powstania nowego obszaru działalności, który może być źródłem nowych usług, zarówno dla przedsiębiorstw, jak i konsumentów. Do 2020 r. wartość danych osobowych obywateli UE ma potencjał wzrosnąć do niemal 1 bln EUR rocznie[987]. Z tego względu duże zbiory danych mogą być źródłem nowych **możliwości** wynikających z oceny masowych ilości danych i generowania na tej podstawie analiz społecznych, gospodarczych lub naukowych, z pożytkiem dla obywateli, a także podmiotów gospodarczych i agencji rządowych[988].

Analizy dużych zbiorów danych pozwalają zidentyfikować wzorce na podstawie różnych źródeł oraz zbiorów danych, umożliwiając wyciąganie wartościowych wniosków, na przykład w takich obszarach jak nauka i medycyna. Ma to zastosowanie na przykład w takich dziedzinach jak zdrowie, bezpieczeństwo żywności, inteligentne systemy transportu, efektywność energetyczna i urbanistyka. Analiza informacji w czasie rzeczywistym może posłużyć do usprawniania wdrażanych systemów. W przypadku badań połączenie dużych ilości danych i analiz statystycznych może być źródłem nowych informacji, zwłaszcza w dziedzinach, w których dotąd większość danych analizowano ręcznie. Otwiera to drzwi do opracowywania nowych metod leczenia, dostosowanych do poszczególnych pacjentów, a opartych na porównaniu masowych ilości dostępnych informacji. Przedsiębiorstwa upatrują

986 Oprogramowanie do przetwarzania dużych zbiorów danych jest nadal na wczesnym etapie rozwoju. W ostatnim czasie opracowano jednak programy analityczne, zwłaszcza narzędzia umożliwiające analizowanie w czasie rzeczywistym masowych ilości danych i informacji o działaniach osób fizycznych. Możliwość analizowania i przetwarzania dużych zbiorów danych w sposób ustrukturyzowany pozwoliła na rozwinięcie nowych sposobów profilowania oraz tworzenia reklam ukierunkowanych. Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ku gospodarce opartej na danych", COM(2014) 442 final, Bruksela, 2 lipca 2014 r.; Komisja Europejska, Reforma ochrony danych w UE a duże zbiory danych, zestawienie informacji; Rada Europy, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 2.

987 Komisja Europejska, Reforma ochrony danych w UE a duże zbiory danych, zestawienie informacji.

988 Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności (2014), Resolution on Big Data; Komisja Europejska, Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów „Ku gospodarce opartej na danych", COM(2014) 442 final, Bruksela, 2 lipca 2014 r., s. 2; Komisja Europejska, Reforma ochrony danych w UE a duże zbiory danych, zestawienie informacji; Rada Europy, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 1.

w analizach dużych zbiorów danych szansy na zdobycie przewagi nad konkurencją, potencjalne oszczędności i utworzenie nowych obszarów działalności dzięki bezpośredniej, zindywidualizowanej obsłudze klienta. Agencje rządowe liczą na udoskonalenie funkcjonowania wymiaru sprawiedliwości. W opracowanej przez Komisję strategii jednolitego rynku cyfrowego dla Europy uznano potencjał opartych na danych technologii, usług i dużych zbiorów danych jako czynnika wspomagającego wzrost gospodarczy, innowacje i cyfryzację w UE[989].

Duże zbiory danych pociągają za sobą jednak również **ryzyko**, związane z ich charakterystycznymi atrybutami: ilością, różnorodnością i prędkością. Ilość dotyczy wolumenu przetwarzanych danych, różnorodność odnosi się do liczby różnych rodzajów danych, natomiast prędkość – do szybkości ich przetwarzania. Szczególne obawy związane z ochroną danych rodzą przypadki wykorzystania takich analiz dużych zbiorów danych z myślą o pozyskaniu nowych i predykcyjnych informacji na potrzeby podejmowania decyzji dotyczących osób fizycznych lub grup osób[990]. Ryzyko dla ochrony danych i prywatności związane z dużymi zbiorami danych podkreślono w opiniach EIOD i Grupy Roboczej Art. 29, rezolucjach Parlamentu Europejskiego oraz dokumentach dotyczących polityki opracowanych przez Radę Europy[991].

Ryzyko to może obejmować niewłaściwe posługiwanie się dużymi zbiorami danych przez osoby dysponujące dostępem do masowych ilości informacji, polegające na manipulacji, dyskryminacji bądź represji skierowanych przeciwko poszczególnym osobom lub grupom społecznym[992]. Gdy dochodzi do zbierania, przetwarzania i oceny danych osobowych lub informacji na masową skalę, wykorzystanie ich może prowadzić do przypadków poważnego naruszenia praw podstawowych i wolności, które nie ogranicza się do prawa do prywatności. Nie jest możliwe precyzyjne określenie zakresu potencjalnego wpływu na prywatność i dane osobowe.

989 Rezolucja Parlamentu Europejskiego z dnia 14 marca 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw (2016/2225/(INI)).

990 Rada Europy, Komitet Konsultacyjnya ds. Konwencji nr 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 2.

991 Zob. na przykład EIOD (2015), *Sprostanie wyzwaniom związanym z dużymi zbiorami danych*, opinia 7/2015, Bruksela, 19 listopada 2015 r.; EIOD (2016), *Coherent enforcement of fundamental rights in the age of Big Data*, Opinia 8/2016, 23 września 2016 r.; Parlament Europejski (2016), Rezolucja w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw, P8_TA-PROV(2017)0076, Strasburg, 14 marca 2017 r.; Rada Europy, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasburg, 23 stycznia 2017 r.

992 Międzynarodowa Konferencja Rzeczników Ochrony Danych Osobowych i Prywatności (2014), Resolution on Big Data.

Parlament Europejski stwierdził, że nie istnieje metodologia, która umożliwiłaby przeprowadzenie opartej na faktach oceny całkowitego wpływu dużych zbiorów danych, istnieją jednak dowody wskazujące na to, że analiza dużych zbiorów danych może mieć istotne oddziaływanie horyzontalne zarówno w sektorze publicznym, jak i prywatnym[993].

Ogólne rozporządzenie o ochronie danych zawiera postanowienia dotyczące prawa niepodlegania zautomatyzowanemu podejmowaniu decyzji, w tym profilowaniu[994]. Problem z prywatnością pojawia się wtedy, gdy wykonywanie prawa sprzeciwu wymaga interwencji człowieka, umożliwiającej osobom, których dane dotyczą, wyrażenie własnego stanowiska i zakwestionowanie decyzji[995]. Może to rodzić wyzwania w zakresie zapewniania odpowiedniego poziomu ochrony danych osobowych, na przykład w sytuacji gdy nie jest możliwa interwencja człowieka, bądź gdy algorytmy są zbyt złożone, a ilość danych zbyt duża, by było możliwe przedstawienie osobom fizycznym uzasadnienia poszczególnych decyzji lub wcześniejsze powiadomienie takich osób w celu uzyskania ich zgody. Przykładem wykorzystania sztucznej inteligencji do zautomatyzowanego podejmowania decyzji są ostatnie zmiany w rozpatrywaniu wniosków o kredyty hipoteczne oraz procesach rekrutacyjnych. Wnioskodawców i kandydatów ocenia się na podstawie określonych parametrów lub czynników i w przypadku niezgodności wnioski są odrzucane.

10.1.3. Zagadnienia związane z ochroną danych

Jeśli chodzi o ochronę danych, główne obawy dotyczą z jednej strony ilości i różnorodności przetwarzanych danych osobowych, zaś z drugiej strony – samego przetwarzania i jego wyników. Wprowadzenie złożonych algorytmów i oprogramowania, które mają przekształcić masowe ilości danych w zasoby stanowiące podstawę podejmowania decyzji, ma wpływ zwłaszcza na poszczególne osoby i grupy – przede wszystkim w przypadku profilowania lub oznaczania (ang. *labelling*) – w związku z czym jest źródłem wielu problemów związanych z ochroną danych[996].

993 Rezolucja Parlamentu Europejskiego z dnia 14 marca 2017 r. w sprawie wpływu technologii dużych zbiorów danych na prawa podstawowe: prywatność, ochrona danych, niedyskryminacja, bezpieczeństwo i ściganie przestępstw (2016/2225/(INI)).

994 Ogólne rozporządzenie o ochronie danych, art. 22.

995 Tamże, art. 22 ust. 3.

996 Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of Big Data, 23 stycznia 2017 r., s. 2.

Określenie administratorów i podmiotów przetwarzających oraz ich odpowiedzialność

Duże zbiory danych i sztuczna inteligencja rodzą pytania o identyfikację administratorów i podmiotów przetwarzających oraz ich odpowiedzialność: kto jest właścicielem danych, gdy gromadzi się i przetwarza tak duże ich ilości? Kto jest administratorem danych, gdy są one przetwarzane przez inteligentne maszyny i oprogramowanie? Jakie dokładnie są obowiązki każdego podmiotu zaangażowanego w przetwarzanie? W jakim celu można wykorzystać duże zbiory danych?

Kwestia odpowiedzialności w kontekście sztucznej inteligencji będzie stanowić jeszcze większe wyzwanie, gdy technologia AI podejmie decyzję opartą na przetwarzaniu danych, które sama opracuje. Ogólne rozporządzenie o ochronie danych wprowadza ramy prawne odpowiedzialności administratora danych i podmiotu przetwarzającego. Niezgodne z prawem przetwarzanie danych osobowych powoduje odpowiedzialność po stronie administratora danych lub podmiotu przetwarzającego[997]. Sztuczna inteligencja i zautomatyzowane podejmowanie decyzji prowokują pytania o to, kto odpowiada za naruszenia mające wpływ na prywatność osób, których dane dotyczą, gdy złożoność przetwarzania i ilość przetworzonych danych sprawiają, że przypisanie odpowiedzialności z całą pewnością konkretnemu podmiotowi jest niemożliwe. Gdy sztuczna inteligencja i algorytmy są uznawane za produkty, pojawia się kwestia odpowiedzialności osobistej, uregulowanej w ogólnym rozporządzeniu o ochronie danych, oraz odpowiedzialności za produkt, której ten akt nie reguluje[998]. W związku z tym konieczne byłoby przyjęcie przepisów w zakresie takiej odpowiedzialności, które wypełniłyby lukę między odpowiedzialnością osobistą a odpowiedzialnością za produkt w przypadku robotyki i technologii AI, w tym na przykład zautomatyzowanego podejmowania decyzji[999].

Wpływ na zasady ochrony danych

Opisane powyżej charakter, analiza i wykorzystanie dużych zbiorów danych utrudniają zastosowanie niektórych tradycyjnych, fundamentalnych zasad europejskiego

997 Ogólne rozporządzenie o ochronie danych, art. 77–79 i art. 82.

998 Parlament Europejski, European Civil Law Rules in Robotics, Directorate-General for Internal Policies, (październik 2016 r.), s. 14.

999 Wystąpienie Roberta Violi podczas seminarium medialnego poświęconego zagadnieniom europejskiego prawa w dziedzinie robotyki, które odbyło się w Parlamencie Europejskim, (SPEECH 16/02/2017); Komunikat prasowy Parlamentu Europejskiego na temat wezwania Komisji do opracowania wniosku dotyczącego zasad odpowiedzialności cywilnej w obszarze robotyki i sztucznej inteligencji.

prawa o ochronie danych[1000]. Wyzwania te dotyczą przede wszystkim zasad zgodności z prawem, minimalizacji danych, ograniczenia celu i przejrzystości.

Zgodnie z zasadą minimalizacji danych dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane. Model biznesowy dużych zbiorów danych może jednak stanowić antytezę tej zasady, ponieważ wymaga coraz większej ilości danych, często bez wskazania celów ich zebrania i przetwarzania.

Podobnie ma się sprawa w przypadku zasady ograniczenia celu, zgodnie z którą dane muszą być przetwarzane w konkretnych celach i nie mogą być przetwarzane w sposób niezgodny z pierwotnymi celami, chyba że takie przetwarzanie opiera się na podstawie prawnej – między innymi zgodzie osoby, której dane dotyczą (zob. sekcja 4.1.1).

Wreszcie duże zbiory danych podważają zasadę prawidłowości danych, ponieważ aplikacje oparte na tej technologii zazwyczaj zbierają dane z różnych źródeł bez możliwości sprawdzenia, czy takie dane są prawidłowe, i zapewnienia, by takie pozostały[1001].

Szczegółowe zasady i prawa

Co do zasady dane osobowe przetwarzane w ramach analiz dużych zbiorów danych pozostają objęte zakresem przepisów dotyczących ochrony danych. W prawie UE i RE ujęto jednak szczegółowe zasady lub odstępstwa, mające zastosowanie w szczególnych przypadkach do złożonych operacji przetwarzania danych za pomocą algorytmów.

W prawie RE zaktualizowana konwencja nr 108 przyznaje nowe prawa osobie, której dane dotyczą, w celu umożliwienia sprawowania skuteczniejszej kontroli nad swoimi danymi osobowymi w erze Big Data. Są to na przykład przewidziane w artykule 9 ust. 1 lit. a), c) i d) zaktualizowanej konwencji prawo do niepodlegania decyzji mającej znaczący wpływ na osobę opartej wyłącznie na zautomatyzowanym przetwarzaniu danych bez uwzględnienia jej stanowiska; prawo do uzyskania, na wniosek, wiedzy na temat argumentacji leżącej u podstaw przetwarzania danych,

1000 Rada Europy, *Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data*, T-PD(2017)01, Strasburg, 23 stycznia 2017 r.

1001 EIOD (2016), Skuteczne wdrażanie społeczeństwa cyfrowego i gospodarki cyfrowej, opinia 8/2016, 23 września 2016 r., s. 8.

gdy wyniki takiego przetwarzania mają wobec niej zastosowanie, oraz prawo do wniesienia sprzeciwu. Inne przepisy zaktualizowanej konwencji nr 108, w szczególności dotyczące przejrzystości i dodatkowych obowiązków, stanowią elementy uzupełniające mechanizmu ochrony ustanowionego przez zaktualizowaną konwencję nr 108 w celu sprostania wyzwaniom cyfrowym.

W prawie UE, oprócz przypadków wymienionych w art. 23 RODO należy zapewnić **przejrzystość** wszystkich operacji przetwarzania danych osobowych. Ma to szczególne znaczenie w kontekście usług internetowych i innych złożonych operacji zautomatyzowanego przetwarzania danych, na przykład wykorzystania algorytmów do podejmowania decyzji. W tym przypadku funkcje systemów przetwarzania danych muszą zapewnić osobom, których dane dotyczą, możliwość zrozumienia, co dzieje się z ich danymi. Aby zapewnić rzetelność i przejrzystość przetwarzania, w ogólnym rozporządzeniu o ochronie danych nałożono na administratorów wymóg podania osobie, której dane dotyczą, istotnych informacji o zasadach zautomatyzowanego podejmowania decyzji, w tym profilowania[1002]. W zaleceniu dotyczącym ochrony i promowania prawa do swobody wypowiedzi i prawa do życia prywatnego w odniesieniu do neutralności sieci Komitet Ministrów Rady Europy zalecił, by dostawcy usług internetowych „podawali użytkownikom jasne i pełne informacje, które należy udostępniać publicznie, o wszelkich praktykach zarządzania ruchem mogących mieć wpływ na dostęp użytkowników do treści, aplikacji lub usług lub ich rozpowszechnianie”[1003]. Sprawozdania na temat praktyk zarządzania ruchem internetowym, sporządzone przez właściwe ograny we wszystkich państwach członkowskich, powinny być opracowywane w sposób otwarty i przejrzysty oraz powinny być udostępniane nieodpłatnie szerokiemu gronu odbiorców[1004].

Administratorzy danych muszą **informować** osoby, których dane dotyczą – niezależnie od tego, czy dane pozyskano od nich czy też nie – nie tylko konkretnie o zebranych danych i ich przetwarzaniu (zob. sekcja 6.1.1), lecz także, w odpowiednich przypadkach, o istnieniu procesów zautomatyzowanego podejmowania decyzji, przekazując im „istotne informacje o zasadach ich podejmowania”[1005], celach i potencjalnych konsekwencjach takich procesów. Ogólne rozporządzenie o ochronie danych precyzuje ponadto (wyłącznie w przypadkach, gdy dane

1002 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 2 lit. f).

1003 Rada Europy, Komitet Ministrów (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 stycznia 2016 r., pkt 5.1.

1004 Tamże, pkt 5.2.

1005 Ogólne rozporządzenie o ochronie danych, art. 13 ust. 2 lit. f) i art. 14 ust. 2 lit. g).

osobowe nie zostały pozyskane od osoby, której dane dotyczą), że administrator nie ma obowiązku przekazywania takich informacji osobie, której dane dotyczą, jeżeli „udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku”[1006]. Niemniej jednak, jak podkreśliła Grupa Robocza Art. 29 w *Wytycznych dotyczących zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia (UE) 2016/679*, stopień złożoności operacji przetwarzania nie powinien sam w sobie uniemożliwiać administratorowi danych przekazania osobie, której dane dotyczą, jednoznacznych wyjaśnień co do celów przetwarzania danych oraz analiz[1007].

Prawa osób, których dane dotyczą, do **dostępu** do swoich danych osobowych, ich **sprostowania** i **usunięcia**, jak również prawo do **ograniczenia** przetwarzania nie przewidują podobnego wyjątku. Niemniej nałożony na administratora obowiązek poinformowania osoby, której dane dotyczą, o sprostowaniu lub usunięciu jej danych osobowych (zob. sekcja 6.1.4) również może zostać uchylony, jeżeli „okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku”[1008].

Osoby, których dane dotyczą, mają ponadto prawo do wniesienia **sprzeciwu**, zgodnie z art. 21 RODO (zob. sekcja 6.1.6) wobec wszelkiego przetwarzania ich danych osobowych, także w odniesieniu do analiz dużych zbiorów danych. Choć administratorzy danych mogą zostać zwolnieni z tego obowiązku, gdy wykażą, że istnieje nadrzędny, prawnie uzasadniony interes, takie wyłączenie nie jest możliwe, gdy przetwarzanie służy do celów marketingu bezpośredniego.

Administratorzy danych mogą powoływać się na szczególne przypadki wyjątków od tych praw, gdy przetwarzają dane osobowe do celów archiwalnych w interesie publicznym, do celów badań naukowych bądź historycznych lub do celów statystycznych[1009].

Jeśli chodzi o **profilowanie i zautomatyzowane podejmowanie decyzji**, RODO wprowadza szczególne zasady: W art. 22 ust. 1 przewidziano, że osoba, której dane dotyczą, „ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby

1006 Tamże, art. 14 ust. 5 lit. b).

1007 Grupa Robocza Art. 29, *Wytyczne dotyczące zautomatyzowanego podejmowania decyzji w indywidualnych przypadkach i profilowania do celów rozporządzenia 2016/679/UE*, WP 251, 3 października 2017 r., s. 14.

1008 Ogólne rozporządzenie o ochronie danych, art. 19.

1009 Tamże, art. 89 ust. 2 i 3.

skutki prawne". Jak podkreślono w wytycznych Grupy Roboczej Art. 29, artykuł ten przewiduje ogólny zakaz w pełni zautomatyzowanego podejmowania decyzji[1010]. Administratorzy danych mogą zostać spod niego wyłączeni tylko w trzech szczególnych przypadkach, tj. gdy decyzja taka jest: 1) niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, 2) dozwolona prawem Unii lub prawem krajowym lub 3) oparta na wyraźnej zgodzie[1011].

Indywidualna kontrola

Złożoność analiz dużych zbiorów danych oraz brak przejrzystości w tym zakresie mogą wymagać ponownego pochylenia się nad kwestiami indywidualnej kontroli nad danymi osobowymi. Wymaga to dostosowania pod kątem kontekstu społecznego i technologicznego oraz uwzględnienia braku wiedzy po stronie osób fizycznych. Z tego względu ochrona danych w kontekście dużych zbiorów danych powinna uwzględniać szerzej rozumianą kontrolę nad wykorzystaniem danych, zakładającą rozwinięcie indywidualnej kontroli tak, by stanowiła bardziej wielopłaszczyznowy proces wielu ocen wpływu czynników ryzyka związanych z wykorzystaniem danych[1012].

O jakości aplikacji wykorzystującej duże zbiory danych świadczy to, jak dobrze prognozuje potrzeby lub zachowania przykładowych osób (lub konsumentów). Obecne modele predykcyjne oparte na analizach dużych zbiorów danych są stale doskonalone. Wśród ostatnich dokonań można wymienić nie tylko wykorzystanie danych do klasyfikacji typów osobowości (tj. zachowań i postaw), lecz także analizowanie zachowań poprzez analizy wzorców głosowych i stopnia dynamiczności wpisywania komunikatów, jak również temperatury ciała. Wszystkie te informacje można wykorzystywać w czasie rzeczywistym, analizując je na tle wniosków płynących z oceny dużych zbiorów danych, na przykład po to, by podczas spotkania z przedstawicielem banku ustalić zdolność kredytową potencjalnego kredytobiorcy. Podstawą oceny osoby ubiegającej się o kredyt nie są wówczas fakty, a cechy zachowań, wywnioskowane na podstawie analizy i oceny informacji pochodzących z dużych zbiorów danych – na przykład czy mamy do czynienia z osobą o mocnym czy też słabym głosie, lub co mówi jej postawa czy temperatura ciała.

1010 Grupa Robocza Art. 29, *Guidelines on Automated Individual Decision-Making and profiling for the purposes of Regulation 2016/679*, WP 251, 3 października 2017 r., s. 9.

1011 Ogólne rozporządzenie o ochronie danych, art. 22 ust. 2.

1012 Rada Europy, Komitet Konsultacyjny ds. Konwencji nr 108, Guidelines on the protection of individuals with regard to the processing of personal data in a world of big data, T-PD(2017)01, Strasburg, 23 stycznia 2017 r.

Profilowanie i reklamy ukierunkowane niekoniecznie stanowią problem, pod warunkiem że ich odbiorcy są świadomi, że kieruje się do nich spersonalizowane reklamy. Problem z profilowaniem zaczyna się wtedy, gdy wykorzystuje się je do manipulowania osobami, tj. do wyszukiwania konkretnych typów osobowości lub grup osób na potrzeby kampanii politycznych. Przykładowo grupy niezdecydowanych wyborców mogą stać się odbiorcami komunikatów politycznych dostosowanych do ich „osobowości" i przekonań. Kolejnym problemem może być stosowanie profilowania w celu odmowy udzielenia dostępu do towarów i usług określonym osobom. Jednym z zabezpieczeń, które może ochronić przed nadużywaniem dużych zbiorów danych i danych osobowych, jest pseudonimizacja (zob. sekcja 2.1.1)[1013]. Sytuacje gdy dane osobowe są w pełni zanonimizowane, tj. nie ma w nich informacji zawierających ślady mogące umożliwić zidentyfikowanie osoby, której dane dotyczą, nie wchodzą w zakres ogólnego rozporządzenia o ochronie danych. W kontekście przetwarzania dużych zbiorów danych zgoda osób, których dane dotyczą, i osób fizycznych stanowi również niemałe wyzwanie w obszarze prawa o ochronie danych. Obejmuje to zgodę na otrzymywanie spersonalizowanych reklam i profilowanie, które można uzasadnić kwestiami związanymi z „doświadczeniami klienta", oraz zgodę na wykorzystywanie masowych ilości danych osobowych do doskonalenia i rozwijania opartych na informacjach narzędzi analitycznych. Świadomość przetwarzania dużych zbiorów danych lub jej brak rodzą szereg pytań dotyczących środków wykonywania praw przez osoby, których dane dotyczą, w świetle tego, że przetwarzanie dużych zbiorów danych może opierać się na algorytmach wykorzystujących zarówno informacje spseudonimizowane, jak i zanonimizowane. Dane spseudonimizowane wchodzą w zakres ogólnego rozporządzenia o ochronie danych, natomiast danych zanonimizowanych akt ten nie obejmuje. Indywidualna kontrola nad przetwarzaniem danych osobowych i świadomość, że takie przetwarzanie ma miejsce, są w kontekście analiz dużych zbiorów danych kluczowe: bez nich osoby, których dane dotyczą, nie miałyby jednoznacznego wglądu w to, kim są administrator danych i podmiot przetwarzający, a co za tym idzie – możliwości dochodzenia swoich praw.

1013 Tamże, s. 2.

10.2. Web 2.0 i 3.0: portale społecznościowe i Internet rzeczy

Najważniejsze kwestie

- Serwisy społecznościowe to internetowe platformy komunikacyjne umożliwiające osobom dołączenie do sieci podobnych użytkowników lub tworzenie takich sieci.
- Pojęcie Internet rzeczy oznacza podłączenie przedmiotów do Internetu, jak również wzajemne połączenia między samymi rzeczami.
- Zgoda osób, których dane dotyczą, to najpowszechniejsza podstawa prawna zgodnego z prawem przetwarzania danych przez administratorów danych w portalach społecznościowych.
- Użytkownicy takich serwisów są co do zasady chronieni na mocy „wyłączenia do użytku domowego", niemniej w określonych sytuacjach wyjątek ten może zostać zniesiony.
- Dostawców portali społecznościowych wyjątek ten nie chroni.
- Uwzględnienie ochrony prywatności już w fazie projektowania i domyślna ochrona danych są kluczowe dla zapewnienia ochrony danych w tym obszarze.

10.2.1. Web 2.0 i 3.0 – definicje

Sieci społecznościowe

Z założenia Internet miał być siecią wzajemnych połączeń między komputerami, służącą do przesyłania komunikatów. Początkowo możliwości wymiany danych za pomocą Internetu były ograniczone, a witryny internetowe umożliwiały użytkownikom jedynie bierne wyświetlanie zawartości[1014]. W erze Web 2.0 Internet stał się forum, na którym użytkownicy nawiązują relacje, współpracują i generują treści. Erę tę charakteryzuje ogromny sukces i powszechne korzystanie z sieci społecznościowych, które stanowią istotną część codziennego życia milionów ludzi.

Sieci społecznościowe (SNS) lub „media społecznościowe" można ogólnie określić jako „platformy komunikacyjne online umożliwiające osobom fizycznym

1014 Komisja Europejska (2016), *Advancing the Internet of Things in Europe*, SWD(2016) 110 final.

przystępowanie do lub tworzenie sieci użytkowników o wspólnych upodobaniach"[1015]. W celu dołączenia do sieci lub jej utworzenia osoby prosi się o podanie danych osobowych i założenie profilu. Dzięki portalom społecznościowym użytkownicy mogą tworzyć „treści" cyfrowe – od zdjęć i filmów po łącza do artykułów prasowych i osobiste wpisy, w których wyrażają swoje opinie. Te internetowe platformy komunikacyjne umożliwiają użytkownikom nawiązywanie interakcji i kontaktu z innymi użytkownikami. Co ważne, rejestracja w większości popularnych sieci społecznościowych jest bezpłatna. Dostawcy takich portali nie nakładają na użytkowników opłat za dołączenie do sieci, a większość przychodów czerpią z reklam ukierunkowanych. Dane osobowe ujawniane na co dzień w takich witrynach to dla reklamodawców potencjalne źródło ogromnych korzyści. Dostęp do informacji o wieku, płci, lokalizacji i zainteresowaniach użytkownika umożliwia im kierowanie reklam do „właściwych" odbiorców.

Komitet Ministrów Rady Europy przyjął Zalecenie w sprawie ochrony praw człowieka w odniesieniu do portali społecznościowych[1016], którego określona sekcja odnosi się do ochrony danych. Zalecenie to zostało uzupełnione w 2018 r. kolejnym Zaleceniem w sprawie ról i obowiązków pośredników usług internetowych[1017].

Przykład: Nora jest szczęśliwa, bo jej partner jej się oświadczył. Chce podzielić się dobrą nowiną z rodziną i przyjaciółmi. W tym celu postanawia opublikować emocjonalny wpis w sieci społecznościowej, w którym opisuje swoją radość, oraz zmienić status związku na „zaręczona". W kolejnych dniach po zalogowaniu na swoje konto Nora widzi reklamy sklepów z sukniami ślubnymi i kwiaciarni. Dlaczego?

Przy tworzeniu reklam w serwisie Facebook sprzedawcy sukien ślubnych i kwiatów wybrali określone parametry, by móc trafiać do osób takich jak Nora. Jeżeli profil sugeruje, że Nora jest zaręczoną kobietą mieszkającą w Paryżu, nieopodal lokalizacji sklepów z sukniami i kwiaciarni, które zamieściły reklamy, natychmiast widzi ona te reklamy.

1015 Grupa Robocza Art. 29 (2009), *Opinion 5/2009 on online social networking*, WP 163, 12 czerwca 2009 r., s. 4.

1016 Rada Europy, Komitet Ministrów, 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 kwietnia 2012 r.

1017 Rada Europy, Komitet Ministrów, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of internet intermediaries, 7 marca 2018 r.

Internet rzeczy

Internet rzeczy to kolejny krok w rozwoju Internetu: era Web 3.0. Technologia Internetu rzeczy umożliwia połączenie i interakcje między urządzeniami za pośrednictwem Internetu. Dzięki temu przedmioty i ludzie mogą być wzajemnie połączeni za pomocą sieci komunikacyjnych, informować o swoim statusie lub stanie otoczenia[1018]. Internet rzeczy i połączone urządzenia stały się rzeczywistością. Prognozuje się, że w najbliższych latach ta dziedzina znacznie się rozwinie – tworzone będą i dalej rozwijane inteligentne urządzenia, a w konsekwencji – inteligentne miasta, domy i przedsiębiorstwa.

Przykład: Technologia Internetu rzeczy ma szczególnie duży potencjał w dziedzinie opieki zdrowotnej. Istnieją już urządzenia, czujniki i aplikacje umożliwiające monitorowanie zdrowia pacjenta. Przycisk alarmowy do noszenia i inne bezprzewodowe czujniki umieszczone w różnych miejscach w mieszkaniu umożliwiają śledzenie dnia mieszkających samotnie osób starszych i generowanie alarmów, gdy coś poważnie zakłóci przebieg ich codziennych zajęć. Osoby w podeszłym wieku często korzystają na przykład z czujników upadku. Urządzenia te precyzyjnie ustalają, że doszło do upadku, i umożliwiają powiadomienie o nim lekarza lub rodziny danej osoby.

Przykład: Barcelona to jedno z najsłynniejszych inteligentnych miast. Od 2012 r. miasto to wdraża innowacyjne technologie, mające na celu utworzenie inteligentnego systemu transportu publicznego, gospodarki odpadami, parkowania i oświetlenia ulic. Przykładowo, aby usprawnić gospodarkę odpadami, miasto korzysta z inteligentnych kontenerów na śmieci. Umożliwiają one monitorowanie poziomu odpadów, co pozwala zoptymalizować trasę ich odbioru. Gdy kontenery są niemal pełne, za pośrednictwem sieci komunikacji mobilnej wysyłają sygnały odbierane przez aplikację firmy utylizacyjnej. Przedsiębiorstwo to może wówczas zaplanować optymalną trasę odbioru odpadów i w pierwszej kolejności opróżnić kontenery, które rzeczywiście tego wymagają, bądź odebrać odpady tylko z tych zbiorników.

1018 Komisja Europejska (2016), Dokument roboczy służb Komisji, *Advancing the Internet of Things in Europe*, SWD(2016) 110 , 19 kwietnia 2016 r.

10.2.2. Osiągnięcie równowagi między zaletami dużych zbiorów danych a związanym z nimi ryzykiem

Rozpowszechnienie i popularność sieci społecznościowych, jakie obserwowaliśmy w ostatnim dziesięcioleciu, sugerują, że serwisy te przynoszą **ogromne korzyści**. Przykładowo reklamy ukierunkowane (opisane w poniższym przykładzie) to szczególnie innowacyjny sposób przedsiębiorstw na dotarcie do odbiorców, dzięki któremu mogą kierować swoją ofertę do konkretnej grupy klientów. Konsumenci również mogą dostrzegać zalety wyświetlania reklam, które lepiej odnoszą się do ich potrzeb i są dla nich bardziej interesujące. Co jednak najważniejsze, sieci i media społecznościowe mogą wywierać pozytywny wpływ na społeczeństwo i sprzyjać wdrażaniu zmian. Dzięki nim użytkownicy mogą się komunikować, nawiązywać relacje, tworzyć grupy i organizować wydarzenia poświęcone nurtującym ich problemom.

Oczekuje się, że Internet rzeczy, który stanowi część unijnej strategii rozwoju jednolitego rynku treści cyfrowych, przyniesie również wiele korzyści gospodarce. W UE szacowana liczba połączeń w ramach Internetu rzeczy ma do 2020 r. wynieść sześć miliardów. Z ekspansji łączności mają wyniknąć istotne korzyści gospodarcze płynące z rozwoju innowacyjnych usług i aplikacji, udoskonalenia opieki zdrowotnej, lepszego zrozumienia potrzeb konsumentów oraz większej wydajności.

Jednocześnie, z uwagi na ogromną ilość danych osobowych generowanych przez użytkowników mediów społecznościowych, a następnie przetwarzanych przez operatorów usług, rozprzestrzenianie się sieci społecznościowych pociąga za sobą **rosnące obawy** o to, jak można chronić prywatność i dane osobowe. Portale społecznościowe mogą zagrozić prawu do życia prywatnego i wolności wypowiedzi. Wśród potencjalnych zagrożeń można wymienić: „brak prawnych i proceduralnych zabezpieczeń dotyczących procesów mogących prowadzić do wykluczenia użytkowników; niewystarczająca ochrona dzieci i młodzieży przed szkodliwymi treściami i zachowaniami; brak poszanowania praw innych osób; brak domyślnych ustawień sprzyjających ochronie prywatności; brak przejrzystości co do celów zbierania i przetwarzania danych osobowych”[1019]. W ramach europejskiego prawa o ochronie danych podejmowane są próby sprostania stawianym przez media społecznościowe wyzwaniom związanym z ochroną prywatności/danych. Takie zasady

1019 Rada Europy, Recommendation Rec(2012)4 to member states on the protection of human rights with regard to social networking services, 4 kwietnia 2012 r.

jak zgoda, uwzględnienie ochrony prywatności/danych już w fazie projektowania oraz domyślna ochrona danych, jak również prawa osób fizycznych, są szczególnie ważne w kontekście mediów i serwisów społecznościowych.

W kontekście Internetu rzeczy ogrom danych osobowych generowanych przez rozmaite wzajemnie połączone urządzenia również pociąga za sobą ryzyko związane z ochroną prywatności i danych. Choć przejrzystość to ważna zasada europejskiego prawa o ochronie danych, z uwagi na mnogość połączonych urządzeń nie zawsze jest jasne, kto ma możliwość gromadzenia danych zebranych dzięki urządzeniom Internetu rzeczy, dostępu do nich i ich wykorzystania[1020]. Zgodnie z prawem UE i RE zasada przejrzystości nakłada jednak na administratorów obowiązek informowania osób, których dane dotyczą – na bieżąco i jasnym i prostym językiem – o sposobie wykorzystywania ich danych. Należy w przejrzysty sposób informować osoby, których dane dotyczą, o ryzyku, zasadach, zabezpieczeniach i prawach odnoszących się do przetwarzania ich danych osobowych. Połączone urządzenia Internetu rzeczy oraz liczne operacje przetwarzania i przetwarzane dane mogą ponadto stanowić wyzwanie w kontekście obowiązku uzyskiwania jednoznacznej, świadomej zgody na przetwarzanie danych – gdy opiera się ono na takiej zgodzie. Osoby fizyczne często nie rozumieją technicznych aspektów takiego przetwarzania, a co za tym idzie – konsekwencji, jakie pociąga za sobą wyrażenie zgody.

Kolejnym istotnym problemem jest bezpieczeństwo, gdyż połączone urządzenia są szczególnie podatne na ryzyko związane z bezpieczeństwem. W przypadku poszczególnych połączonych urządzeń poziom bezpieczeństwa może się różnić. Funkcjonują one poza standardową infrastrukturą IT, dlatego mogą nie mieć mocy obliczeniowej i pojemności wystarczającej do zainstalowania oprogramowania zabezpieczającego bądź wdrożenia technik takich jak szyfrowanie, pseudonimizacja bądź anonimizacja, mających na celu ochronę danych osobowych użytkowników.

Przykład: Niemieckie organy regulacyjne postanowiły wycofać z obrotu zabawkę połączoną z Internetem po tym, jak zaistniały silne obawy o wpływ zabawki na poszanowanie życia prywatnego dzieci. Organy te uznały, że podłączona do sieci lalka imieniem Cayla w rzeczywistości stanowiła ukryte urządzenie szpiegujące. Lalka przesyłała pytania w formie nagrań głosowych bawiącego się nią dziecka do aplikacji w usłudze cyfrowej, która z kolei przekształcała je w tekst i na tej podstawie wyszukiwała w Internecie

1020 Europejski Inspektor Ochrony Danych (2017), *Understanding the Internet of Things.*

odpowiedzi. Wówczas aplikacja przesyłała do lalki odpowiedź, którą zabawka przedstawiała dziecku. Za pośrednictwem tej lalki możliwe było rejestrowanie i przesyłanie do aplikacji komunikacji dziecka i towarzyszących mu dorosłych. Gdyby producenci lalki nie zastosowali odpowiednich środków zabezpieczających, lalka mogłaby posłużyć niepożądanym osobom do podsłuchiwania takich rozmów.

10.2.3. Zagadnienia związane z ochroną danych

Zgoda

W Europie przetwarzanie danych osobowych jest zgodne z prawem wyłącznie wówczas, gdy jest dopuszczone na mocy europejskiego prawa o ochronie danych. W przypadku dostawców sieci społecznościowych zgoda osób, których dane dotyczą, co do zasady stanowi zgodną z prawem podstawę przetwarzania danych. Zgoda musi zostać wyrażona dobrowolnie, konkretnie, świadomie i jednoznacznie (zob. sekcja 4.1.1)[1021]. „Wyrażona dobrowolnie" oznacza, że osoba, której dane dotyczą, musi być w stanie dokonać rzeczywistego wyboru. Zgoda jest „konkretna" i „świadoma", jeżeli jest zrozumiała i w czytelny i precyzyjny sposób odnosi się do pełnego zakresu, celów i konsekwencji przetwarzania danych. W kontekście mediów społecznościowych można zakwestionować to, czy zgoda jest dobrowolna, konkretna i świadoma w odniesieniu do wszystkich rodzajów przetwarzania danych przez operatora sieci społecznościowej i osoby trzeciej.

Przykład: Aby dołączyć do sieci społecznościowej i z niej korzystać, osoby fizyczne często muszą wyrazić zgodę na różne rodzaje przetwarzania swoich danych osobowych, niejednokrotnie bez wiedzy o niezbędnych specyfikacjach bądź alternatywnych rozwiązaniach. Jako przykład można podać konieczność wyrażenia zgody na otrzymywanie reklam behawioralnych w celu rejestracji w sieci społecznościowej. Jak zauważa Grupa Robocza Art. 29 w opinii w sprawie definicji zgody, „ze względu na znaczenie, jakie zyskały niektóre serwisy społecznościowe, niektóre kategorie użytkowników (na przykład młodzież) zgadzają się otrzymywać reklamę behawioralną, aby uniknąć ryzyka częściowego wykluczenia

1021 Ogólne rozporządzenie o ochronie danych, art. 4 i art. 7; zaktualizowana konwencja nr 108, art. 5.

z interakcji społecznych. Użytkownik powinien mieć możliwość wyrażenia dobrowolnej i konkretnej zgody na otrzymywanie reklamy behawioralnej niezależnie od dostępu do serwisu społecznościowego"[1022].

Zgodnie z ogólnym rozporządzeniem o ochronie danych dane osobowe dzieci, które nie ukończyły 16 lat, co do zasady nie mogą być przetwarzane na podstawie ich zgody[1023]. Jeżeli jest wymagana zgoda na przetwarzanie, musi ją wyrazić rodzic lub opiekun prawny. Dzieci zasługują na szczególną ochronę, bowiem mogą one być mniej świadome ryzyka i konsekwencji wynikających z przetwarzania danych. Kwestia ta ma szczególne znaczenie w kontekście mediów społecznościowych, gdyż dzieci są bardziej podatne na pewne negatywne skutki korzystania z takich serwisów, na przykład cyberprzemoc, cyberstalking czy kradzież tożsamości.

Bezpieczeństwo i uwzględnienie ochrony prywatności/danych już w fazie projektowania i domyślna ochrona prywatności/danych

Przetwarzanie danych osobowych zawsze pociąga za sobą ryzyko związane z bezpieczeństwem, ponieważ stale zachodzi prawdopodobieństwo naruszenia bezpieczeństwa oraz wynikającego z niego przypadkowego lub niezgodnego z prawem zniszczenia, utraty, zmiany, nieuprawnionego dostępu lub ujawnienia przetwarzanych danych osobowych. Zgodnie z europejskim prawem o ochronie danych administratorzy i podmioty przetwarzające mają obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne, aby zapobiec wszelkiej nieuprawnionej ingerencji w operacje przetwarzania danych. Dostawcy sieci społecznościowych objęci zakresem przepisów europejskiego prawa o ochronie danych również muszą wypełnić ten obowiązek.

Zasady uwzględnienia ochrony prywatności/danych już w fazie projektowania i domyślnej ochrony prywatności/danych wymagają od administratorów zapewnienia bezpieczeństwa w projektach swoich produktów oraz automatycznego stosowania odpowiednich ustawień prywatności i ochrony danych. Oznacza to, że gdy ktoś postanowi dołączyć do sieci społecznościowej, dostawca usługi nie może automatycznie udostępniać wszystkich informacji o nowym użytkowniku serwisu pozostałym użytkownikom. Gdy nowy użytkownik dołącza do serwisu, domyślne ustawienia prywatności i ochrony danych powinny zakładać udostępnienie takich

1022 Grupa Robocza Art. 29 (2011), *Opinion 15/2011 Consent*, WP 187, 13 lipca 2011 r., s. 18.

1023 Zob. ogólne rozporządzenie o ochronie danych, art. 8. Państwa członkowskie UE mogą przewidzieć w swoim prawie niższą granicę wiekową, która musi wynosić co najmniej 13 lat.

informacji wyłącznie wskazanym przez niego użytkownikom. Umożliwienie dostępu do danych osobom spoza tego grona powinno być możliwe wyłącznie po podjęciu przez użytkownika działań w celu ręcznej zmiany domyślnych ustawień prywatności i ochrony danych. Może to mieć znaczenie również w przypadkach, gdy do naruszenia ochrony danych dochodzi pomimo zastosowania środków bezpieczeństwa. Wówczas usługodawcy muszą powiadomić użytkowników, których naruszenie dotyczy, że może ono powodować wysokie ryzyko naruszenia praw lub wolności osoby, której dane dotyczą[1024].

Zasady uwzględnienia ochrony prywatności/danych już w fazie projektowania i domyślnej ochrony prywatności/danych mają szczególne znaczenie w kontekście sieci społecznościowych, ponieważ oprócz nieuprawnionego dostępu, który ma miejsce w przypadku większości rodzajów przetwarzania, udostępnianie danych osobowych w mediach społecznościowych powoduje dodatkowe ryzyko związane z bezpieczeństwem. Ryzyko to często wynika z tego, że osoby nie rozumieją, *kto* może uzyskiwać dostęp do ich informacji i w jaki sposób można je wykorzystywać. Wraz z upowszechnieniem korzystania z mediów społecznościowych dochodzi do zwiększenia liczby przypadków kradzieży tożsamości.

Przykład: Kradzież tożsamości to zjawisko polegające na zdobyciu przez jedną osobę informacji, danych lub dokumentów należących do innej osoby (ofiary), a następnie posłużenie się nimi w celu podania się za ofiarę i pozyskania towarów lub usług w jej imieniu. Przykładowo Paul ma konto w serwisie społecznościowym. Jest nauczycielem i czynnie uczestniczy w życiu swojej społeczności, a do tego jest bardzo towarzyski i nie przejmuje się zbytnio ustawieniami prywatności i ochrony danych w swoim koncie w serwisie. Ma liczne grono znajomych w portalu, a wśród nich są też osoby, których nie zna osobiście. Uczy w dużej szkole, a ponieważ cieszy się sporą popularnością jako trener szkolnej drużyny piłkarskiej, sądzi, że osoby te to najprawdopodobniej rodzice uczniów lub osoby zaprzyjaźnione ze szkołą. Adres e-mail i data urodzin Paula są widoczne w jego profilu w serwisie. Ponadto Paul regularnie publikuje zdjęcia swojego psa, Toby'ego, opisując je na przykład: „z Tobym na porannej przebieżce". Paul nie zdawał sobie sprawy, że jednym z najczęstszych pytań zabezpieczających jego

1024 Tamże, art. 34.

adres e-mail lub konto telefonu komórkowego jest „podaj imię swojego zwierzęcia". Za pomocą informacji dostępnych w profilu Paula w serwisie społecznościowym Nick z łatwością zhakował jego konta.

Prawa osób fizycznych

Dostawcy sieci społecznościowych muszą szanować prawa osób fizycznych (zob. sekcja 6.1), w tym prawo do informacji o celu przetwarzania oraz możliwym sposobie wykorzystania danych osobowych do celów marketingu bezpośredniego. Osobom należy ponadto zapewnić prawo dostępu do danych osobowych wygenerowanych na platformie społecznościowej oraz ich usunięcia. Nawet w sytuacji, gdy osoba fizyczna wyraziła zgodę na przetwarzanie danych osobowych i przesłała informacje za pośrednictwem Internetu, powinna mieć możliwość „bycia zapomnianym", jeżeli chce zrezygnować z usług sieci społecznościowej. Dodatkowo prawo do przenoszenia danych umożliwia użytkownikom otrzymanie kopii danych osobowych przekazanych dostawcy usług sieci społecznościowej w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego formacie oraz przesyłania ich innemu usługodawcy[1025].

Administratorzy danych

W kontekście mediów społecznościowym często pada trudne pytanie o to, kto jest administratorem danych, tj.: na kim spoczywa obowiązek zapewnienia zgodności z przepisami dotyczącymi ochrony danych. Zgodnie z europejskim prawem o ochronie danych dostawcy sieci społecznościowych są administratorami danych. Jednoznacznie wynika to z szerokiej definicji pojęcia „administrator" oraz faktu, że ci usługodawcy ustalają cel i środki przetwarzania danych osobowych udostępnianych przez osoby fizyczne. Zgodnie z prawem UE administratorzy świadczący usługi na rzecz osób, których dane dotyczą, w UE, muszą przestrzegać zapisów ogólnego rozporządzenia o ochronie danych nawet wówczas, gdy sami nie mają jednostki organizacyjnej na terytorium Unii.

Czy użytkowników sieci społecznościowych również można uznawać za administratorów danych? Gdy osoby fizyczne przetwarzają dane osobowe „w ramach czynności o czysto osobistym lub domowym charakterze", przepisy o ochronie danych nie mają zastosowania. W europejskim prawie o ochronie danych zasadę tę określa się

1025 Ogólne rozporządzenie o ochronie danych, art. 21.

mianem „wyjątku do użytku domowego". W niektórych przypadkach użytkownik sieci społecznościowej może jednak nie być objęty zakresem tego wyjątku.

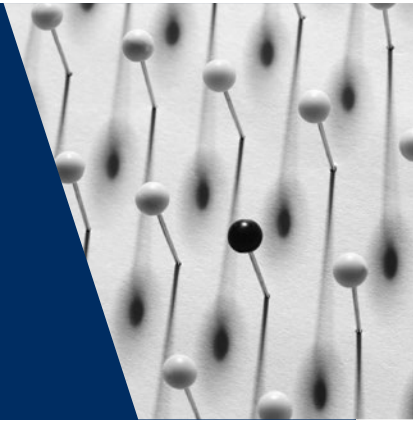
Użytkownicy dobrowolnie udostępniają swoje dane osobowe w Internecie. Często jednak udostępniane informacje zawierają dane osobowe innych osób.

Przykład: Paul ma konto na bardzo popularnej platformie społecznościowej. Jest aspirującym aktorem, a jego konto służy mu do publikacji zdjęć, filmów i wpisów opisujących jego zamiłowanie do sztuki. Jego przyszłość w dużej mierze zależy od popularności, dlatego uznał, że jego profil nie powinien ograniczać się tylko do grona najbliższych znajomych, i postanowił udostępnić go wszystkim użytkownikom Internetu – niezależnie od tego, czy są użytkownikami serwisu, czy też nie. Czy Paul może publikować zdjęcia i filmy, na których towarzyszy mu jego przyjaciółka Sarah bez jej zgody? Sarah, nauczycielka w szkole podstawowej, dba o to, by jej pracodawca oraz uczniowie i ich rodzice nie mieli wglądu w jej prywatne życie. Wyobraźmy sobie, że Sarah, która nie korzysta z sieci społecznościowych, dowiaduje się od wspólnego znajomego, Nicka, że w sieci opublikowano zdjęcie z przyjęcia, w którym uczestniczyła z Paulem. W takim przypadku przetwarzanie danych przez Paula nie jest objęte prawem UE, ponieważ ma zastosowanie „wyjątek do użytku domowego".

Ważne jednak, by użytkownicy byli świadomi i mieli na uwadze, że publikowanie informacji o innych osobach bez ich zgody może naruszać ich prawa do prywatności i ochrony danych. Nawet w przypadku gdy wspomniany wyjątek ma zastosowanie – przykładowo gdy użytkownik udostępnia dane treści wyłącznie wybranym znajomym – publikacja danych osobowych innych osób i tak może rodzić odpowiedzialność po jego stronie. Choć przepisy o ochronie danych nie mają zastosowania, gdy stosuje się „wyjątek do użytku domowego", odpowiedzialność może wynikać z innych przepisów krajowych, na przykład dotyczących zniesławienia bądź naruszenia osobowości. Ponadto wyłącznie użytkownicy sieci społecznościowych są chronieni „wyjątkiem do użytku domowego": administratorzy i podmioty przetwarzające, którzy zapewniają środki umożliwiające przetwarzanie danych do celów prywatnych, są objęci prawem UE o ochronie danych[1026].

1026 Tamże, motyw 18.

W następstwie reformy dyrektywy o prywatności i łączności elektronicznej zasady dotyczące ochrony danych, prywatności i bezpieczeństwa, które mają zastosowanie do dostawców usług telekomunikacyjnych na mocy aktualnych ram prawnych, będą miały również zastosowanie do łączności maszyna-maszyna i usług łączności elektronicznej, w tym na przykład usług OTT.



Dodatkowe lektury

Rozdział 1

Araceli Mangas, M. (red.) (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*, Wiedeń, Manzsche Verlags- und Universitätsbuchhandlung.

Docksey, C. „Four fundamental rights: finding the balance", *International Data Privacy Law*, t. 6, nr 3, s. 195–209.

EDRi, *An introduction to data protection*, Bruksela.

Frowein, J. i Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

González Fuster, G. i 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*, t. 26 (1), s. 73–82.

Grabenwarter, C. i Pabel, K. (2012), *Europäische Menschenrechtskonvention*, Monachium, C. H. Beck.

Gutwirth, S., Poullet, Y., de Hert, P., de Terwange, C. i Nouwt, S. (red.) (2009), *Reinventing Data Protection*, Springer.

Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009), *Law of the European Convention on Human Rights*, Oksford, 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*, Monachium, C. H. Beck.

Kokott, J. i Sobotta, C. (2013), „The distinction between privacy and data protection in the case law of the CJEU and the ECtHR", *International Data Privacy Law*, t. 3, nr 4, s. 222–228.

Kranenborg, H. (2015), „Google and the Right to be Forgotten", *European Data Protection Law Review*, t. 1, nr 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*, t. 63, nr 3, s. 569–597.

Lynskey, O. (2015), *The Foundations of EU Data Protection Law*, Oksford, 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*, Oksford, Oxford University Press.

Nowak, M., Januszewski, K. i Hofstätter, T. (2012), *All human rights for all – Vienna manual on human rights*, Antwerpia, intersentia N. V., Neuer Wissenschaftlicher Verlag.

Picharel, C. i Coutron, L. (2010), *Charte des droits fondamentaux de l'Union européenne et convention européenne des droits de l'homme*, Bruksela, Emile Bruylant.

Simitis, S. (1997), „Die EU-Datenschutz-Richtlinie – Stillstand oder Anreiz?", *Neue Juristische Wochenschrift*, nr 5, s. 281–288.

Warren, S. i Brandeis, L. (1890), „The right to privacy", *Harvard Law Review,* t. 4, nr 5, s. 193–220.

White, R. i Ovey, C. (2010), *The European Convention on Human Rights*, Oksford, Oxford University Press.

Rozdział 2

Acquisty, A. i Gross R. (2009), „Predicting Social Security numbers from public data", *Proceedings of the National Academy of Science*, 7 lipca 2009 r.

Carey, P. (2009), *Data protection: A practical guide to UK and EU law*, Oksford, Oxford University Press.

de Montjoye, Y.-A., Hidalgo, C. A., Verleysen, M. i Blondel, V. D. (2013), „Unique in the Crowd: the Privacy Bounds of Human Mobility", *Nature Scientific Reports*, t. 3, 2013.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madryt, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paryż, 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. i Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance*, Londyn, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization", *UCLA Law Review*, t. 57, nr 6, s. 1701–1777.

Samarati, P. i 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*, t. 10, nr 5, s. 557–570.

Tinnefeld, M., Buchner, B. i Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, Monachium, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), Anonymisation: managing data protection risk. Code of practice.

Rozdziały 3–6

Brühann, U. (2012), „Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr" w: Grabitz, E., Hilf, M. i Nettesheim, M. (red.), *Das Recht der Europäischen Union*, Band IV, A. 30, Monachium, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Kadyks, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Curren, L. i Kaye, J. (2010), „Revoking consent: a 'blind spot' in data protection law?", *Computer Law & Security Review*, t. 26, nr 3 s. 273–283.

Dammann, U. i Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

De Hert, P. i Papakonstantinou, V. (2012), „The Police and Criminal Justice Data Protection Directive: Comment and Analysis", *Computers & Law Magazine of SCL*, t. 22, nr 6, s. 1–5.

De Hert, P. i 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*, t. 28, nr 2, s. 130–142.

European data protection's looking glass after the Lisbon treaty: Taking rights seriously", *European Review of Private Law*, t. 20, nr 2, s. 473–506.

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".

FRA (Agencja Praw Podstawowych Unii Europejskiej) (2010), *Data Protection in the European Union: the role of National Supervisory authorities (Strengthening the fundamental rights architecture in the EU II)*, Luksemburg, Urząd Publikacji Unii Europejskiej (Urząd Publikacji).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* (Conference edition), Wiedeń, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities*, Luksemburg, Urząd Publikacji.

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. i Saxby, S. (2011), „30 years on – The review of the Council of Europe Data Protection Convention 108", *Computer Law & Security Review*, t. 27, nr 3, s. 223–231.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, Privacy Impact Assessment.

Rozdział 7

Europejski Inspektor Ochrony Danych (2014), Position paper on transfer of personal data to third countries and international organisations by EU institutions and bodies.

Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. i Nouwt, S. (2009), *Reinventing data protection?*, Berlin, Springer.

Kuner, C. (2007), *European data protection law*, Oksford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law*, Oksford, Oxford University Press.

Rozdział 8

Blasi Casagran, C. (2016) *Global Data Protection in the Field of Law Enforcement, an EU Perspective*, Londyn, Routledge.

Boehm, F. (2012), *Information Sharing and Data Protection in the Area of Freedom, Security and Justice. Towards Harmonised Data Protection Principles for Information Exchange at EU-level,* Berlin, Springer.

De Hert, P. i Papakonstantinou, V. (2012), 'The Police and Criminal Justice Data Protection Directive: Comment and Analysis', *Computers & Law Magazine of SCL*, t. 22, nr 6, s. 1–5.

Drewer, D. i Ellermann, J. (2012), „Europol's data protection framework as an asset in the fight against cybercrime", *ERA Forum*, t. 13, nr 3, s. 381–395.

Eurojust (2014), *Data protection at Eurojust: A robust, effective and tailor-made regime*, Haga, Eurojust.

Europol (2012), *Data Protection at Europol*, Luksemburg, Urząd Publikacji.

Gutiérrez Zarza, A. (2015), *Exchange of Information and Data Protection in Cross-border Criminal Proceedings in Europe*, Berlin, Springer.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i 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*, t. 36, nr 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.

Rozdział 9

Büllesbach, A., Gijrath, S., Poullet, Y. i Hacon, R. (2010), *Concise European IT law*, Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. i Poullet, Y. (2012), *European data protection: In good health?*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world*, Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i 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*, t. 36, nr 5, s. 722–776.

Rosemary, J. i Hamilton, A. (2012), *Data protection law and practice*, Londyn, Sweet & Maxwell.

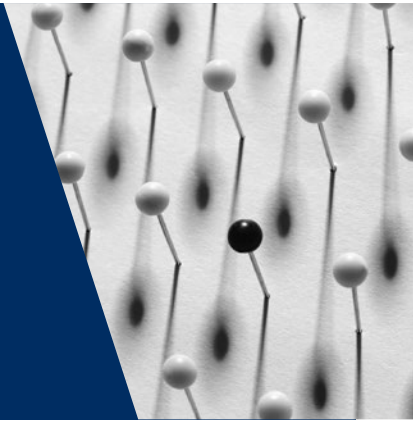
Rozdział 10

El Emam, K. i Álvarez, C. (2015), „A critical appraisal of the Article 29 Working Party Opinion 05/2014 on data anonymization techniques", *International Data Privacy Law*, t. 5, nr 1, s. 73–87.

Mayer-Schönberger, V. i Cate, F. (2013), „Notice and consent in a world of Big Data", *International Data Privacy Law*, t. 3, nr 2, s. 67–73.

Rubinstein, I. (2013), „Big Data: The End of Privacy or a New Beginning?", *International Data Privacy Law*, t. 3, nr 2, s. 74–87.

Orzecznictwo



Wybrane orzecznictwo Europejskiego Trybunału Praw Człowieka

Dostęp do danych osobowych
Gaskin przeciwko Zjednoczonemu Królestwu, nr 10454/83, 7 lipca 1989 r.
Godelli przeciwko Włochom, nr 33783/09, 25 września 2012 r.
K.H. i in. przeciwko Słowacji, nr 32881/04, 28 kwietnia 2009 r.
Leander przeciwko Szwecji, nr 9248/81, 26 marca 1987 r.
M.K. przeciwko Francji, nr 19522/09, 18 kwietnia 2013 r.
Odièvre przeciwko Francji [WI], nr 42326/98, 13 lutego 2003 r.

Osiągnięcie równowagi między ochroną danych a wolnością wypowiedzi i prawem do informacji
Axel Springer AG przeciwko Niemcom [WI], nr 39954/08, 7 lutego 2012 r.
Bohlen przeciwko Niemcom, nr 53495/09, 19 lutego 2015 r.
Couderc i Hachette Filipacchi Associés przeciwko Francji [WI], nr 40454/07, 10 listopada 2015 r.
Magyar Helsinki Bizottság przeciwko Węgrom [WI], nr 18030/11, 8 listopada 2016 r.
Müller i in. przeciwko Szwajcarii, nr 10737/84, 24 maja 1988 r.
Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii [WI], nr 931/13, 27 czerwca 2017 r.
Vereinigung bildender Künstler przeciwo Austrii, nr 68354/01, 25 stycznia 2007 r.
Von Hannover przeciwko Niemcom (nr 2) [WI], nr 40660/08 i 60641/08, 7 lutego 2012 r.

Osiągnięcie równowagi między ochroną danych a wolnością religii
Sinan Işık przeciwko Turcji, nr 21924/05, 2 lutego 2010 r.

Wyzwania związane z ochroną danych w Internecie
K.U. przeciwko Finlandii, nr 2872/02, 2 grudnia 2008 r.

Zgoda osoby, której dane dotyczą
Elberte przeciwko Łotwie, nr 61243/08, 13 stycznia 2015 r.
Sinan Işık przeciwko Turcji, nr 21924/05, 2 lutego 2010 r.
Y przeciwko Turcji, nr 648/10, 17 lutego 2015 r.

Korespondencja
Amann przeciwko Szwajcarii [WI], nr 27798/95, 16 lutego 2000 r.
Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii, nr 62540/00, 28 czerwca 2007 r.
Bernh Larsen Holding AS i in. przeciwko Norwegii, nr 24117/08, 14 marca 2013 r.
Cemalettin Canli przeciwko Turcji, nr 22427/04, 18 listopada 2008 r.
Dalea przeciwko Francji, nr 964/07, 2 lutego 2010 r.
D.L. przeciwko Bułgarii, nr 7472/14, 19 maja 2016 r.
Gaskin przeciwko Zjednoczonemu Królestwu, nr 10454/83, 7 lipca 1989 r.
Haralambie przeciwko Rumunii, nr 21737/03, 27 października 2009 r.
Khelili przeciwko Szwajcarii, nr 16188/07, 18 października 2011 r.
Leander przeciwko Szwecji, nr 9248/81, 26 marca 1987 r.
Malone przeciwko Zjednoczonemu Królestwu, nr 8691/79, 2 sierpnia 1984 r.
Rotaru przeciwko Rumunii [WI], nr 28341/95, 4 maja 2000 r.
S. i Marper przeciwko Zjednoczonemu Królestwu [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.
Shimovolos przeciwko Rosji, nr 30194/09, 21 czerwca 2011 r.
Silver i in. przeciwko Zjednoczonemu Królestwu, nr 5947/72, 6205/73, 7052/75, 7061/75, 7107/75, 7113/75 i 9405/81, 25 marca 1983 r.
The Sunday Times przeciwko Zjednoczonemu Królestwu, nr 6538/74, 26 kwietnia 1979 r.

Bazy danych rejestrów karnych
Aycaguer przeciwko Francji, nr 8806/12, 22 czerwca 2017 r.
B.B. przeciwko Francji, nr 5335/06, 17 grudnia 2009 r.
Brunet przeciwko Francji, nr 21010/10, 18 września 2014 r.
M.K. przeciwko Francji, nr 19522/09, 18 kwietnia 2013 r.
M.M. przeciwko Zjednoczonemu Królestwu, nr 24029/07, 13 listopada 2012 r.

Bezpieczeństwo danych
Haralambie przeciwko Rumunii, nr 21737/03, 27 października 2009 r.
K.H. i in. przeciwko Słowacji, nr 32881/04, 28 kwietnia 2009 r.

Bazy danych DNA
S. i Marper przeciwko Zjednoczonemu Królestwu [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.

Dane GPS
Uzun przeciwko Niemcom, nr 35623/05, 2 września 2010 r.

Dane dotyczące stanu zdrowia
Avilkina i in. przeciwko Rosji, nr 1585/09, 6 czerwca 2013 r.
Biriuk przeciwko Litwie, nr 23373/03, 25 listopada 2008 r.
I przeciwko Finlandii, nr 20511/03, 17 lipca 2008 r.
L.H. przeciwko Łotwie, nr 52019/07, 29 kwietnia 2014 r.
L.L. przeciwko Francji, nr 7508/02, 10 października 2006 r.
M.S. przeciwko Szwecji, nr 20837/92, 27 sierpnia 1997 r.
Szuluk przeciwko Zjednoczonemu Królestwu, nr 36936/05, 2 czerwca 2009 r.
Y przeciwko Turcji, nr 648/10, 17 lutego 2015 r.
Z przeciwko Finlandii, nr 22009/93, 25 lutego 1997 r.

Tożsamość
Godelli przeciwko Włochom, nr 33783/09, 25 września 2012 r.
Gurgurov przeciwko Mołdawii, nr 27138/04, 27 kwietnia 2010 r.
Odièvre przeciwko Francji [WI], nr 42326/98, 13 lutego 2003 r.

Informacje o działalności zawodowej
G.S.B. przeciwko Szwajcarii, nr 28601/11, 22 grudnia 2015 r.
M.N. i in. przeciwko San Marino, nr 28005/12, 7 lipca 2015 r.
Michaud przeciwko Francji, nr 12323/11, 6 grudnia 2012 r.
Niemietz przeciwko Niemcom, nr 13710/88, 16 grudnia 1992 r.

Przechwytywanie komunikacji
Amann przeciwko Szwajcarii [WI], nr 27798/95, 16 lutego 2000 r.
Brito Ferrinho Bexiga Villa-Nova przeciwko Portugalii, nr 69436/10, 1 grudnia 2015 r.
Copland przeciwko Zjednoczonemu Królestwu, nr 62617/00, 3 kwietnia 2007 r.
Halford przeciwko Zjednoczonemu Królestwu, nr 20605/92, 25 czerwca 1997 r.
Iordachi i in. przeciwko Bułgarii, nr 25198/02, 10 lutego 2009 r.

Kopp przeciwko Szwajcarii, nr 23224/94, 25 marca 1998 r.
Liberty i in. przeciwko Zjednoczonemu Królestwu, nr 58243/00, 1 lipca 2008 r.
Malone przeciwko Zjednoczonemu Królestwu, nr 8691/79, 2 sierpnia 1984 r.
Mustafa Sezgin Tanrıkulu przeciwko Turcji, nr 27473/06, 18 lipca 2017 r.
Pruteanu przeciwko Rumunii, nr 30181/05, 3 lutego 2015 r.
Szuluk przeciwko Zjednoczonemu Królestwu, nr 36936/05, 2 czerwca 2009 r.

Obowiązki spoczywające na podmiotach odpowiedzialnych
B.B. przeciwko Francji, nr 5335/06, 17 grudnia 2009 r.
I przeciwko Finlandii, nr 20511/03, 17 lipca 2008 r.
Mosley przeciwko Zjednoczonemu Królestwu, nr 48009/08, 10 maja 2011 r.

Dane osobowe
Amann przeciwko Szwajcarii [WI], nr 27798/95, 16 lutego 2000 r.
Bernh Larsen Holding AS i in. przeciwko Norwegii, nr 24117/08, 14 marca 2013 r.
Uzun przeciwko Niemcom, nr 35623/05, 2 września 2010 r.

Zdjęcia
Sciacca przeciwko Włochom, nr 50774/99, 11 stycznia 2005 r.
Von Hannover przeciwko Niemcom, nr 59320/00, 24 czerwca 2004 r.

Prawo do bycia zapomnianym
Satakunnan Markkinapörssi Oy i Satamedia Oy przeciwko Finlandii [WI], nr 931/13, 27 czerwca 2017 r.
Segerstedt-Wiberg i in. przeciwko Szwecji, nr 62332/00, 6 czerwca 2006 r.

Prawo do sprzeciwu
Leander przeciwko Szwecji, nr 9248/81, 26 marca 1987 r.
M.S. przeciwko Szwecji, nr 20837/92, 27 sierpnia 1997 r.
Mosley przeciwko Zjednoczonemu Królestwu, nr 48009/08, 10 maja 2011 r.
Rotaru przeciwko Rumunii [WI], nr 28341/95, 4 maja 2000 r.
Sinan Işık przeciwko Turcji, nr 21924/05, 2 lutego 2010 r.

Kategorie danych szczególnie chronionych
Brunet przeciwko Francji, nr 21010/10, 18 września 2014 r.
I przeciwko Finlandii, nr 20511/03, 17 lipca 2008 r.
Michaud przeciwko Francji, nr 12323/11, 6 grudnia 2012 r.
S. i Marper przeciwko Zjednoczonemu Królestwu [WI], nr 30562/04 i 30566/04, 4 grudnia 2008 r.

Nadzór i egzekwowanie
(role poszczególnych podmiotów, w tym organów nadzorczych)
I przeciwko Finlandii, nr 20511/03, 17 lipca 2008 r.
K.U. przeciwko Finlandii, nr 2872/02, 2 grudnia 2008 r.
Von Hannover przeciwko Niemcom, nr 59320/00, 24 czerwca 2004 r.
Von Hannover przeciwko Niemcom (nr 2) [WI], nr 40660/08 i 60641/08, 7 lutego 2012 r.

Metody nadzoru
Allan przeciwko Zjednoczonemu Królestwu, nr 48539/99, 5 listopada 2002 r.
Association for European Integration and Human Rights i Ekimdzhiev przeciwko Bułgarii, nr 62540/00, 28 czerwca 2007 r.
Bărbulescu przeciwko Rumunii [WI], nr 61496/08, 5 września 2017 r.
D.L. przeciwko Bułgarii, nr 7472/14, 19 maja 2016 r.
Dragojević przeciwko Chorwacji, nr 68955/11, 15 stycznia 2015 r.
Karabeyoğlu przeciwko Turcji, nr 30083/10, 7 czerwca 2016 r.
Klass i in. przeciwko Niemcom, nr 5029/71, 6 września 1978 r.
Roman Zakharov przeciwko Rosji [WI], nr 47143/06, 4 grudnia 2015 r.
Rotaru przeciwko Rumunii [WI], nr 28341/95, 4 maja 2000 r.
Szabó i Vissy przeciwko Węgrom, nr 37138/14, 12 stycznia 2016 r.
Taylor-Sabori przeciwko Zjednoczonemu Królestwu, nr 47114/99, 22 października 2002 r.
Uzun przeciwko Niemcom, nr 35623/05, 2 września 2010 r.
Versini-Campinchi i Crasnianski przeciwko Francji, nr 49176/11, 16 czerwca 2016 r.
Vetter przeciwko Francji, nr 59842/00, 31 maja 2005 r.
Vukota-Bojić przeciwko Szwajcarii, nr 61838/10, 18 października 2016 r.

Nadzór wideo
Köpke przeciwko Niemcom, nr 420/07, 5 października 2010 r.
Peck przeciwko Zjednoczonemu Królestwu, nr 44647/98, 28 stycznia 2003 r.

Próbki głosu
P.G. i J.H. przeciwko Zjednoczonemu Królestwu, nr 44787/98, 25 września 2001 r.
Wisse przeciwko Francji, nr 71611/01, 20 grudnia 2005 r.

Wybrane orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej

Orzecznictwo związane z dyrektywą o ochronie danych

Sprawy połączone C-468/10 i C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) i Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011 r.
[Prawidłowe wdrożenie art. 7 lit. f) dyrektywy o ochronie danych – „uzasadnione interesy osób trzecich" – w prawie krajowym]

C-360/10, *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) przeciwko Netlog NV*, 16 lutego 2012 r.
[Obowiązek zapobiegania przez dostawców sieci społecznościowych niezgodnemu z prawem korzystaniu z utworów muzycznych i audiowizualnych przez użytkowników sieci]

C-398/15, *Camera di Commercio, Industria, Artigianato e Agricoltura di Lecce przeciwko Salvatoremu Manniemu*, 9 marca 2017 r.
[Prawo usunięcia danych osobowych; Prawo do wniesienia sprzeciwu wobec przetwarzania]

C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M. E. E. Rijkeboerowi*, 7 maja 2009 r.
[Prawo dostępu przysługujące osobie, której dane dotyczą]

C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 5 maja 2011 r.
[Konieczność ponownej zgody]

Sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in.* oraz *Kärntner Landesregierung i in.* [WI], 8 kwietnia 2014 r.
[Naruszenie prawa pierwotnego UE przez dyrektywę o zatrzymywaniu danych; Zgodne z prawem przetwarzanie; Ograniczenie celu i przechowywania]

C-212/13, *František Ryneš przeciwko Úřad pro ochranu osobních údajů*, 11 grudnia 2014 r.
[Pojęcie „przetwarzania danych" i „administratora"]

C-131/12, *Google Spain SL, Google Inc. przeciwko Agencia Española de Protección de Datos (AEPD), Mariowi Costesze Gonzálezowi* [WI], 13 maja 2014 r.
[Obowiązki dostawców wyszukiwarek do niewyświetlania – na życzenie osoby, której dane dotyczą – danych osobowych w wynikach wyszukiwania; Zastosowanie dyrektywy o ochronie danych; Pojęcie „przetwarzania danych"; Znaczenie „administratorów"; Osiągnięcie równowagi między ochroną danych a wolnością wypowiedzi; Prawo do bycia zapomnianym]

C-524/06, *Heinz Huber przeciwko Bundesrepublik Deutschland* [WI], 16 grudnia 2008 r.
[Zasadność przechowywania danych na temat cudzoziemców w rejestrze statystycznym]

C-473/12, *Institut professionnel des agents immobiliers (IPI) przeciwko Geoffreyowi Englebertowi i in.*, 7 listopada 2013 r.
[Prawo do informacji o przetwarzaniu danych osobowych]

C-614/10, *Komisja Europejska przeciwko Republice Austrii* [WI], 16 października 2012 r.
[Niezależność krajowego organu nadzorczego]

C-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec* [WI], 9 marca 2010 r.
[Niezależność krajowego organu nadzorczego]

C-288/12, *Komisja Europejska przeciwko Węgrom* [WI], 8 kwietnia 2014 r.
[Zgodność z prawem likwidacji urzędu krajowego inspektora ochrony danych]

C-362/14, *Maximillian Schrems przeciwko Data Protection Commissioner* [WI], 6 października 2015 r.
[Zasada zgodnego z prawem przetwarzania; Prawa podstawowe; Nieważność decyzji dotyczącej „bezpiecznej przystani"; Uprawnienia niezależnych organów nadzorczych]

C-291/12, *Michael Schwarz przeciwko Stadt B ochum*, 17 października 2013 r.
[Wniosek o wydanie orzeczenia w trybie prejudycjalnym; Obszar wolności, bezpieczeństwa i sprawiedliwości; Paszport biometryczny; Odciski palców, podstawa prawna, proporcjonalność]

C-582/14, *Patrick Breyer przeciwko Bundesrepublik Deutschland*, 19 października 2016 r.
[Definicja „danych osobowych"; Adresy IP; Przechowywanie danych przez dostawcę usług mediów internetowych; Ustawodawstwo krajowe niedopuszczające uwzględnienia prawnie uzasadnionego interesu realizowanego przez administratora]

C-434/16, *Peter Nowak przeciwko Data Protection Commissioner*, Opinia rzecznika generalnego Juliane Kokott, 20 lipca 2017 r.
[Pojęcie „danych osobowych"; Dostęp do własnego egzemplarza arkusza egzaminacyjnego]

T-462/12 R, *Pilkington Group Ltd przeciwko Komisji Europejskiej*, Postanowienie Prezesa Sądu, 11 marca 2013 r.

C-101/01, *Postępowanie karne przeciwko Bodil Lindqvist*, 6 listopada 2003 r.
[Szczególne kategorie danych osobowych]

C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU* [WI], 29 stycznia 2008 r.
[Pojęcie „danych osobowych"; Obowiązek ujawnienia przez dostawców usług internetowych tożsamości użytkowników programów wymiany plików KaZaA stowarzyszeniu na rzecz ochrony własności intelektualnej]

Sprawy połączone C-465/00, C-138/01 i C-139/01, *Rechnungshof przeciwko Österreichischer Rundfunk i in.* oraz *Neukomm i Lauermann przeciwko Österreichischer Rundfunk*, 20 maja 2003 r.
[Proporcjonalność prawnego obowiązku publikowania danych osobowych dotyczących wynagrodzeń pracowników niektórych kategorii instytucji związanych z sektorem publicznym]

C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 listopada 2011 r.
[Społeczeństwo informacyjne; Prawa autorskie; Internet; Oprogramowanie „peer-to-peer"; Dostawcy usług internetowych; Instalacja systemu do filtrowania łączności elektronicznej w celu uniemożliwienia udostępniania plików naruszających prawa autorskie; Brak ogólnego obowiązku monitorowania przesyłanych informacji]

C-201/14, *Smaranda Bara i in. przeciwko Casa Națională de Asigurări de Sănătate i in.*, 1 października 2015 r.
[Prawo do informacji o przetwarzaniu danych osobowych]

Sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.* [WI], 21 grudnia 2016 r.
[Poufność łączności elektronicznej; Dostawcy usług łączności elektronicznej; Zobowiązania dotyczące uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji; Brak uprzedniego przeglądu przez sąd bądź niezależny organ administracyjny; Karta praw podstawowych Unii Europejskiej; Zgodność z prawem UE]

C-73/07, *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy* [WI], 16 grudnia 2008 r.
[Pojęcie „działalności dziennikarskiej" w rozumieniu art. 9 dyrektywy o ochronie danych]

C-13/16, *Valsts policijas Rīgas reģiona pārvaldes Kārtības policijas pārvalde przeciwko Rīgas pašvaldības SIA „Rīgas satiksme"*, 4 maja 2017 r.
[Zasada zgodnego z prawem przetwarzania danych: prawnie uzasadniony interes realizowany przez osoby trzecie]

Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR i Hartmut Eifert przeciwko Land Hessen* [WI], 9 listopada 2010 r.
[Pojęcie „danych osobowych"; Proporcjonalność obowiązku prawnego do publikacji danych osobowych o beneficjentach określonych funduszy rolnych]

C-230/14, *Weltimmo s.r.o. przeciwko Nemzeti Adatvédelmi és Információszabadság Hatóság*, 1 października 2015 r.
[Uprawnienia krajowych organów nadzorczych]

C-342/12, *Worten – Equipamentos para o Lar SA przeciwko Autoridade para as Condições de Trabalho (ACT)*, 30 maja 2013 r.
[Pojęcie „danych osobowych"; Ewidencja czasu pracy; Zasady dotyczące jakości danych i kryteriów zgodności przetwarzania danych z prawem; Dostęp organu krajowego odpowiedzialnego za monitorowanie warunków pracy; Zobowiązanie pracodawcy do udostępnienia ewidencji czasu pracy w celu zapewnienia natychmiastowego wglądu]

Sprawy połączone C-141/12 i C-372/12, *YS przeciwko Minister voor Immigratie, Integratie en Asiel* oraz *Minister voor Immigratie, Integratie en Asiel przeciwko M i S*, 17 lipca 2014 r.

[Zakres prawa dostępu przysługującego osobie, której dane dotyczą; Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych; Pojęcie „danych osobowych"; Dane dotyczące osoby wnioskującej o zezwolenie na pobyt i analiza prawna zawarta w dokumencie administracyjnym przygotowującym do wydania decyzji; Karta praw podstawowych Unii Europejskiej]

Orzecznictwo związane z dyrektywą 2016/681

Opinia 1/15 Trybunału [WI], 26 lipca 2017 r.

[Podstawa prawna; Projekt umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych PNR; Zgodność projektu umowy z art. 16 TFUE i art. 7 i 8 oraz art. 52 ust. 1 Karty praw podstawowych Unii Europejskiej]

Orzecznictwo związane z rozporządzeniem o ochronie danych przez instytucje UE

C-615/13 P, *ClientEarth, Pesticide Action Network Europe (PAN Europe) przeciwko Europejskiemu Urzędowi do spraw Bezpieczeństwa Żywności (EFSA), Komisji Europejskiej*, 16 lipca 2015 r.

[Dostęp do dokumentów]

C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.* [WI], 29 czerwca 2010 r.

[Dostęp do dokumentów]

Orzecznictwo związane z dyrektywą 2002/58/WE

C-461/10, *Bonnier Audio AB, Earbooks AB, Norstedts Förlagsgrupp AB, Piratförlaget AB, Storyside AB przeciwko Perfect Communication Sweden AB*, 19 kwietnia 2012 r.

[Prawo autorskie i prawa pokrewne; Przetwarzanie danych przez Internet; Naruszenie wyłącznego prawa; Książki audio udostępnione za pośrednictwem serwera FTP za pomocą Internetu przez adres IP dostarczony przez operatora Internetu; Skierowany do operatora Internetu sądowy nakaz dostarczenia nazwy i adresu użytkownika adresu IP]

C-70/10, *Scarlet Extended SA przeciwko Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM)*, 24 listopada 2011 r.

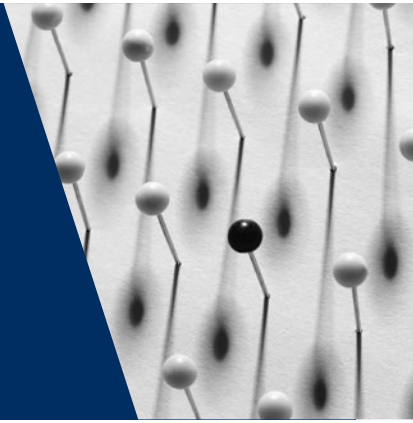
[Społeczeństwo informacyjne; Prawo autorskie; Internet; Oprogramowanie „peer-to-peer"; Dostawcy usług internetowych; Wprowadzenie systemu filtrowania połączeń elektronicznych celem uniemożliwienia wymiany plików naruszającej prawa autorskie; Brak ogólnego obowiązku nadzorowania przekazywanych informacji]

C-536/15, *Tele2 (Netherlands) BV i in. przeciwko Autoriteit Consument en Markt (AMC)*, 15 marca 2017 r.

[Zasada niedyskryminacji; Udostępnienie danych osobowych dotyczących abonentów dla celów świadczenia publicznie dostępnych usług biura numerów i spisu abonentów; Zgoda abonenta; Rozróżnienie według państwa członkowskiego, w którym świadczone są publicznie dostępne usługi biura numerów i spisu abonentów]

Sprawy połączone C-203/15 i C-698/15, *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.* [WI], 21 grudnia 2016 r.

[Poufność łączności elektronicznej; Dostawcy usług łączności elektronicznej; Zobowiązania dotyczące uogólnionego i niezróżnicowanego zatrzymywania danych o ruchu i danych dotyczących lokalizacji; Brak uprzedniego przeglądu przez sąd bądź niezależny organ administracyjny; Karta praw podstawowych Unii Europejskiej; Zgodność z prawem UE]



Indeks

Orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej

Orzecznictwo Europejskiego Trybunału Praw Człowieka

Orzecznictwo sądów krajowych

Wiele innych informacji na temat Agencji Praw Podstawowych Unii Europejskiej jest dostępnych w Internecie. Można do nich dotrzeć poprzez stronę internetową FRA fra.europa.eu.

Więcej informacji na temat orzecznictwa Europejskiego Trybunału Praw Człowieka można znaleźć na stronie internetowej Trybunału: echr.coe.int. Strona internetowa HUDOC zapewnia dostęp do wyroków i decyzji wydanych w języku angielskim i/lub francuskim, tłumaczeń na inne języki, biuletynów informacyjnych dotyczących orzecznictwa, komunikatów prasowych oraz innych informacji na temat pracy Trybunału (https://hudoc.echr.coe.int).

Jak uzyskać dostęp do publikacji Rady Europy

Wydawnictwo Rady Europy publikuje materiały dotyczące wszystkich zagadnień, jakimi zajmuje się ta organizacja, w tym: praw człowieka, nauk prawnych, ochrony zdrowia, etyki, polityki społecznej, ochrony środowiska, edukacji, kultury, sportu, młodzieży oraz ochrony zabytków. Książki i publikacje elektroniczne można znaleźć i zamówić spośród szerokiego katalogu dostępnego na stronie internetowej (http://book.coe.int/).

Wirtualna czytelnia umożliwia użytkownikom bezpłatne zapoznanie się zarówno z fragmentami najświeższych publikacji jak również z pełnym tekstem niektórych oficjalnych dokumentów.

Informacje o Radzie Europy, jak również pełne teksty Konwencji są dostępne na stronie internetowej Biura Traktatów: http://conventions.coe.int/.

Jak skontaktować się z UE

Osobiście

W całej Unii Europejskiej istnieje kilkaset centrów informacyjnych Europe Direct. Adres najbliższego centrum można znaleźć na stronie: https://europa.eu/european-union/contact_pl.

Telefonicznie lub drogą mailową

Europe Direct to serwis informacyjny, który udziela odpowiedzi na pytania na temat Unii Europejskiej. Można się z nim skontaktować:
- dzwoniąc pod bezpłatny numer telefonu: 00 800 6 7 8 9 10 11 (niektórzy operatorzy mogą naliczać opłaty za te połączenia),
- dzwoniąc pod standardowy numer telefonu: +32 22999696,
- drogą mailową: https://europa.eu/european-union/contact_pl.

Wyszukiwanie informacji o UE

Online

Informacje o Unii Europejskiej są dostępne we wszystkich językach urzędowych UE w portalu Europa: https://europa.eu/european-union/index_pl.

Publikacje UE

Bezpłatne i odpłatne publikacje UE można pobrać lub zamówić na stronie: https://publications.europa.eu/pl/publications. Większą liczbę egzemplarzy bezpłatnych publikacji można otrzymać, kontaktując się z serwisem Europe Direct lub z lokalnym centrum informacyjnym (zob. https://europa.eu/european-union/contact_pl).

Prawo UE i powiązane dokumenty

Informacje prawne dotyczące UE, w tym wszystkie unijne akty prawne od 1952 r., są dostępne we wszystkich językach urzędowych UE w portalu EUR-Lex: http://eur-lex.europa.eu.

Portal Otwartych Danych UE

Unijny portal otwartych danych (http://data.europa.eu/euodp/pl) umożliwia dostęp do zbiorów danych pochodzących z instytucji i innych organów UE. Dane można pobierać i wykorzystywać bezpłatnie, zarówno do celów komercyjnych, jak i niekomercyjnych.

doi:10.2811/69584 TK-05-17-225-PL-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

Szybki rozwój technologii informacyjnych skutkuje rosnącą potrzebą skutecznej ochrony danych osobowych – prawa zagwarantowanego w aktach prawnych zarówno Unii Europejskiej (UE), jak i Rady Europy (RE). Postęp technologiczny przesuwa na przykład granice nadzoru, przechwytywania łączności i przechowywania danych, co stanowi poważne wyzwanie w kontekście zapewnienia możliwości egzekwowania tego ważnego prawa. Niniejszy podręcznik ma stanowić wprowadzenie do tej powstającej dziedziny prawa dla prawników praktyków, którzy nie specjalizują się w ochronie danych. Zawiera on ogólny przegląd obowiązujących ram prawnych UE i RE. Wyjaśniono w nim najważniejsze orzecznictwo, streszczając istotne orzeczenia Trybunału Sprawiedliwości Unii Europejskiej i Europejskiego Trybunału Praw Człowieka. Oprócz tego w podręczniku przedstawiono hipotetyczne scenariusze, które służą jako praktyczne przykłady rozmaitych wyzwań, z jakimi przychodzi się borykać w tej stale rozwijającej się dziedzinie.

FRA – AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ
Schwarzenbergplatz 11 – 1040 Wiedeń – Austria
Tel. +43 158030-0 – Faks +43 158030-699
fra.europa.eu
facebook.com/fundamentalrights
linkedin.com/company/eu-fundamental-rights-agency
twitter.com/EURightsAgency

EUROPEJSKI TRYBUNAŁ PRAW CZŁOWIEKA
RADA EUROPY
67075 Strasburg – Francja
Tel. +33 (0) 3 88 41 20 18 – Faks +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

EUROPEJSKI INSPEKTOR OCHRONY DANYCH
Rue Wiertz 60 – 1047 Bruksela – Belgia
Tel. +32 2 283 19 00
edps.europa.eu – edps@edps.europa.eu – @EU_EDPS

Urząd Publikacji
Unii Europejskiej

ISBN 978-92-871-9842-6 (Rada Europy)
ISBN 978-92-9474-289-6 (FRA)