PODRĘCZNIK

Podręcznik europejskiego prawa o ochronie danych

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

Pracę nad tekstem podręcznika zakończono w kwietniu 2014 r.
Przyszłe aktualizacje będą dostępne na stronie internetowej FRA pod adresem fra.europa.eu, na stronie internetowej Rady Europy pod adresem coe.int/dataprotection oraz na stronie internetowej Europejskiego Trybunału Praw Człowieka w menu Case-Law [„Orzecznictwo"] pod adresem echr.coe.int.

Europe Direct to serwis, który pomoże Państwu uzyskać odpowiedzi na pytania dotyczące Unii Europejskiej.

Bezpłatny numer infolinii (*):
00 800 6 7 8 9 10 11

(*) Informacje udzielane są nieodpłatnie, większość połączeń również jest bezpłatna (jednak niektórzy operatorzy, hotele lub aparaty w budkach telefonicznych mogą naliczać opłaty).

Zdjęcia (okładka i wnętrze): © iStockphoto

Szczegółowe informacje na temat Unii Europejskiej dostępne są w portalu Europa (http://europa.eu).

Informacje katalogowe znajdują się na końcu publikacji.

Luksemburg: Urząd Publikacji Unii Europejskiej, 2014

ISBN 978-92-871-9940-9 (RE)
ISBN 978-92-9239-338-0 (FRA)
doi:10.2811/5514

Printed in Belgium

Wydrukowano na (PCF)

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

Podręcznik europejskiego prawa o ochronie danych

Przedmowa

Niniejszy podręcznik europejskiego prawa o ochronie danych został opracowany wspólnie przez Agencję Praw Podstawowych (APP) Unii Europejskiej i Radę Europy z udziałem sekretariatu Europejskiego Trybunału Praw Człowieka. Jest to trzeci z serii podręczników prawnych opracowanych wspólnie przez APP i Radę Europy. W marcu 2011 r. opublikowano pierwszy podręcznik na temat europejskiego prawa o niedyskryminacji, a w czerwcu 2013 r. drugi o europejskim prawie odnoszącym się do azylu, granic i imigracji.

Zdecydowaliśmy się kontynuować współpracę w związku z bardzo aktualnym tematem, który dotyczy nas wszystkich w życiu codziennym, a mianowicie ochroną danych osobowych. Europa posiada w tym zakresie jeden z systemów zapewniających najlepszą ochronę, który oparto na Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencji nr 108) i aktach prawnych Unii Europejskiej (UE), a także na orzecznictwie Europejskiego Trybunału Praw Człowieka (ETPC) oraz Trybunału Sprawiedliwości Unii Europejskiej (TSUE).

Niniejszy podręcznik ma stanowić główny punkt odniesienia dla czytelników, podnosząc ich świadomość i poszerzając wiedzę na temat przepisów dotyczących ochrony danych w państwach członkowskich Unii Europejskiej oraz Rady Europy. Jest on przeznaczony dla prawników niespecjalizujących się w tej dziedzinie, sędziów, krajowych urzędów ochrony danych i innych osób zajmujących się tematyką ochrony danych.

W grudniu 2009 r., wraz z wejściem w życie Traktatu z Lizbony, prawnie wiążąca stała się Karta praw podstawowych UE, a tym samym prawo do ochrony danych osobowych zyskało status samodzielnego prawa podstawowego. Aby chronić to prawo podstawowe, niezbędne jest lepsze zrozumienie konwencji nr 108 Rady Europy, jak też aktów prawnych UE, które utorowały drogę do ochrony danych w Europie, a także orzecznictwa TSUE i ETPC.

Pragniemy podziękować Instytutowi Praw Człowieka Ludwiga Boltzmanna za pomoc w opracowaniu podręcznika. Chcielibyśmy też wyrazić wdzięczność dla biura Europejskiego Inspektora Ochrony Danych za jego wkład na etapie przygotowywania tekstu. Szczególnie dziękujemy jednostce ds. ochrony danych Komisji Europejskiej za pomoc w przygotowaniu podręcznika. Pragniemy również wyrazić naszą

wdzięczność dla Biura Generalnego Inspektora Ochrony Danych Osobowych, które dokonało weryfikacji polskiej wersji językowej podręcznika.

Philippe Boillat

Dyrektor generalny
ds. Praw Człowieka i Spraw Prawnych
Rady Europy

Morten Kjaerum

Dyrektor
Agencji Praw Podstawowych
Unii Europejskiej

Spis treści

Skróty i akronimy

BCR	Wiążące reguły korporacyjne
CCTV	Telewizja przemysłowa
CETS	Seria Traktatów Rady Europy
CIS	System informacji celnej
CRM	Zarządzanie kontaktami z klientami
C-SIS	System centralny systemu informacyjnego Schengen
EAW	Europejski nakaz aresztowania
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
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
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
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
SEPA	Jednolity obszar płatności w euro
SIS	System informacyjny Schengen
SWIFT	Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych
TFUE	Traktat o funkcjonowaniu Unii Europejskiej
TSUE	Trybunał Sprawiedliwości Unii Europejskiej (do grudnia 2009 r. nosił on nazwę Trybunału Sprawiedliwości Wspólnot Europejskich)
TUE	Traktat o Unii Europejskiej
UE	Unia Europejska
VIS	Wizowy system informacyjny
WE	Wspólnota Europejska

Jak korzystać z podręcznika

Niniejszy podręcznik zawiera ogólne informacje o przepisach Unii Europejskiej (UE) i Rady Europy (RE) dotyczących ochrony danych.

Ma on stanowić pomoc dla prawników praktyków, którzy nie specjalizują się w dziedzinie ochrony danych; jest przeznaczony dla adwokatów, sędziów i innych praktyków, jak też dla osób pracujących dla innych podmiotów, w tym organizacji pozarządowych (NGO), które mogą w swojej działalności zetknąć się z zagadnieniami prawnymi związanymi z ochroną danych.

Podręcznik stanowi podstawowe kompendium wiedzy zarówno o prawie unijnym, jak i o zapisach europejskiej konwencji praw człowieka (EKPC) dotyczących ochrony danych, a także o sposobie uregulowania tej dziedziny na mocy przepisów UE i postanowień EKPC oraz 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, w tym wybrane istotne orzecznictwo związane z dwoma odrębnymi europejskimi systemami prawnymi. Następnie w ramach tych dwóch europejskich porządków przedstawiane są stosowne przepisy odnoszące się do kolejnych poruszanych tematów. Pozwala to czytelnikowi ustalić, w jakich aspektach te systemy prawne są zbieżne, a w jakich się różnią.

W tabelach na początku każdego rozdziału wyliczono poruszone w nim tematy, podano też stosowne przepisy prawa i pozostałe istotne materiały, takie jak orzecznictwo. Kolejność tematów może nieznacznie różnić się od tej w tekście rozdziału, jeżeli uznano to za wskazane w celu zwięzłego przedstawienia jego treści. W tabelach omówiono zarówno prawo RE, jak i UE. Powinno to pomóc użytkownikom w odnalezieniu najważniejszych informacji dotyczących ich sytuacji, zwłaszcza jeżeli podlegają wyłącznie prawu RE.

Prawnicy praktycy z krajów nienależących do UE, które są państwami członkowskimi Rady Europy oraz 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 członkowskich UE powinni korzystać z obydwu sekcji, gdyż państwa te należą do obydwu porządków prawnych. Osoby potrzebujące więcej informacji na konkretny temat znajdą wykaz odnośników do bardziej specjalistycznych materiałów w sekcji podręcznika zatytułowanej „Dodatkowe lektury” .

Prawo RE przedstawiono, posługując się krótkimi odniesieniami do wybranych spraw Europejskiego Trybunału Praw Człowieka (ETPC). Wybrano je spośród licznych wyroków i decyzji ETPC dotyczących ochrony danych.

Prawo UE jest zawarte w przyjętych aktach prawnych, odpowiednich postanowieniach traktatów oraz w Karcie praw podstawowych Unii Europejskiej zgodnie z wykładnią zawartą w orzecznictwie Trybunału Sprawiedliwości Unii Europejskiej (TSUE; przed 2009 r. określanego jako Trybunał Sprawiedliwości Wspólnot Europejskich).

Orzecznictwo opisane lub cytowane w podręczniku obejmuje przykłady ważnych wyroków zarówno ETPC, jak i TSUE. Wskazówki zamieszczone na końcu podręcznika mają pomóc czytelnikowi w wyszukiwaniu orzecznictwa w internecie.

Ponadto w ramkach podano praktyczne przykłady z hipotetycznymi scenariuszami, których celem jest dokładniejsze zilustrowanie zastosowania europejskich przepisów dotyczących ochrony danych w praktyce, zwłaszcza w przypadkach, gdy nie istnieje konkretne orzecznictwo ETPC lub TSUE na dany temat.

Na początku podręcznika zamieszczono krótki opis roli dwóch systemów prawnych, których podstawę stanowią EKPC i prawo UE (rozdział 1). W rozdziałach 2–8 omówiono następujące zagadnienia:

- terminologię związaną z ochroną danych;
- najważniejsze zasady europejskiego prawa o ochronie danych;
- przepisy europejskiego prawa o ochronie danych;
- prawa osób, których dane dotyczą, oraz ich egzekwowanie;
- transgraniczny przepływ danych;
- ochronę danych w kontekście działań policji i wymiaru sprawiedliwości w sprawach karnych;
- inne europejskie przepisy w zakresie ochrony danych.

1

Kontekst i ogólne informacje o europejskim prawie o ochronie danych

UE	Omówione zagadnienia	RE
Prawo do ochrony danych		
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.		Artykuł 8 EKPC (prawo do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji) Konwencja o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108)
Wyważenie praw		
TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 2010	**Ogólne**	
TSUE, C-73/07, *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy*, 2008	**Wolność wypowiedzi**	ETPC, *Axel Springer AG przeciwko Niemcom*, 2012 ETPC, *Mosley przeciwko Zjednoczonemu Królestwu*, 2011
	Wolność sztuki i nauki	ETPC, *Vereinigung bildender Künstler przeciwko Austrii*, 2007
TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU*, 2008	**Ochrona własności**	
TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*, 2010	**Dostęp do dokumentów**	ETPC, *Társaság a Szabadságjogokért przeciwko Węgrom*, 2009

1.1. Prawo do ochrony danych

Najważniejsze kwestie

- Na mocy art. 8 EKPC prawo do ochrony przed gromadzeniem i wykorzystywaniem danych osobowych stanowi część prawa do poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji.
- Konwencja nr 108 RE jest pierwszym prawnie wiążącym aktem międzynarodowym odnoszącym się wprost do ochrony danych.
- W prawie UE zagadnienie ochrony danych uregulowano po raz pierwszy w dyrektywie o ochronie danych.
- Na mocy prawa UE ochronę danych uznano za prawo podstawowe.

Prawo do ochrony sfery prywatnej jednostki przed ingerencją ze strony innych, a zwłaszcza ze strony państwa, po raz pierwszy zapisano w międzynarodowym akcie prawnym w art. 12 Powszechnej deklaracji praw człowieka Organizacji Narodów Zjednoczonych (ONZ) z 1948 r., który dotyczy poszanowania życia prywatnego i rodzinnego[1]. PDPC wpłynęła na rozwój innych instrumentów ochrony praw człowieka w Europie.

1.1.1. 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. europejską konwencję praw człowieka (EKPC), która weszła w życie w 1953 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.

Aby zapewnić przestrzeganie przez umawiające się strony zobowiązań wynikających z EKPC, w Strasburgu (Francja) ustanowiono w 1959 r. Europejski Trybunał Praw Człowieka (ETPC). ETPC zapewnia przestrzeganie przez państwa zobowiązań

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

na mocy konwencji, rozpatrując skargi wnoszone przez osoby, grupy osób, organizacje pozarządowe lub osoby prawne zarzucające naruszenia konwencji. W 2013 r. Rada Europy składała się z 47 państw członkowskich, z których 28 było zarazem państwami członkowskimi UE. Skarżący nie musi być obywatelem jednego z państw członkowskich. ETPC może także rozpatrywać sprawy międzypaństwowe wnoszone przez jedno lub więcej państw członkowskich RE przeciwko innemu państwu członkowskiemu.

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[2].

W swoim orzecznictwie ETPC zbadał wiele przypadków, w których pojawiało się zagadnienie ochrony danych, w szczególności dotyczących przechwytywania łączności[3], różnych form nadzoru[4] oraz ochrony przed przechowywaniem danych osobowych przez władze publiczne[5]. 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[6]. Wiele spośród tych przypadków zostanie szczegółowo omówionych w stosownych rozdziałach.

1.1.2. Konwencja Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych

Pojawienie się technologii informacyjnych w latach 60. XX w. poskutkowało rosnącą potrzebą opracowania bardziej szczegółowych zasad zabezpieczenia osób

2 RE, Europejska konwencja praw człowieka, CETS nr 005, 1950.

3 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.

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

5 Zob. na przykład ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.; ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu*, nr 30562/04, 4 grudnia 2008 r.

6 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.

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[7]. W 1981 r. otwarto do podpisu Konwencję o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (konwencja nr 108)[8]. 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 sektro prywatny, jak i publiczny, np. do przetwarzania danych przez organy sądowe i organy ds. egzekwowania prawa. Zapewnia ona osobom fizycznym ochronę przed nadużyciami, które mogą towarzyszyć gromadzeniu i przetwarzaniu danych osobowych, a jej drugim celem jest uregulowanie transgranicznego przepływu danych osobowych. Zasady ustanowione w konwencji w odniesieniu do gromadzenia i przetwarzania danych osobowych dotyczą w szczególności rzetelnego i zgodnego z prawem gromadzenia oraz automatycznego przetwarzania danych, które powinny być gromadzone dla określonych i usprawiedliwionych celów oraz 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 (proporcjonalność), a także prawidłowe.

Oprócz gwarancji w zakresie gromadzenia i przetwarzania danych osobowych konwencja zawiera także zakaz, 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. Ograniczenia praw zapisanych w konwencji dopuszcza się jedynie w przypadku, gdy zagrożone są nadrzędne interesy, takie jak bezpieczeństwo lub obronność państwa.

7 RE, Komitet Ministrów (1973), Resolution (73) 22 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the private sector [„Rezolucja (73) 22 o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze prywatnym"], 26 września 1973 r.; RE, Komitet Ministrów (1974), Resolution (74) 29 on the protection of the privacy of individuals *vis-à-vis* electronic data banks in the public sector [„Rezolucja (74) 29 o ochronie życia prywatnego osób fizycznych w kontekście elektronicznych banków danych w sektorze publicznym"], 20 września 1974 r.

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

Mimo że w konwencji przewidziano swobodny przepływ danych osobowych między państwami-stronami, nałożono także pewne ograniczenia na przepływ tych danych do krajów, których regulacje prawne nie zapewniają równoważnej ochrony.

W celu dalszego rozwoju ogólnych zasad i przepisów ustanowionych w konwencji nr 108 Komitet Ministrów RE przyjął pewne zalecenia, które nie mają charakteru prawnie wiążącego (zob. rozdziały 7 i 8).

Konwencję nr 108 ratyfikowały wszystkie państwa członkowskie UE. W 1999 r. konwencję nr 108 zmieniono, aby umożliwić UE stanie się jej stroną[9]. 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 nadzorujących ochronę danych[10].

Perspektywy

Konsultacje społeczne przeprowadzone w 2011 r. po podjęciu decyzji o modernizacji konwencji nr 108 zaowocowały potwierdzeniem dwóch głównych celów prac: wzmocnienia ochrony prywatności w środowisku cyfrowym i usprawnienia mechanizmu związanego z działaniami następczymi w ramach konwencji.

Do konwencji nr 108 mogą przystępować państwa niebędące członkami RE, w tym kraje spoza Europy. Możliwość stosowania konwencji jako powszechnego standardu i jej otwarty charakter mogą uczynić ją podstawą promowania ochrony danych na poziomie globalnym.

Jak dotąd 45 spośród 46 umawiających się stron konwencji nr 108 stanowią państwa członkowskie RE. Pierwszym krajem spoza Europy jest Urugwaj, który przystąpił w sierpniu 2013 r.; Maroko, które otrzymało od Komitetu Ministrów zaproszenie do przystąpienia do konwencji nr 108, jest w trakcie formalności związanych z przystąpieniem.

9 RE, Zmiany Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (ETS nr 108) pozwalające na przystąpienie Wspólnot Europejskich, przyjęte przez Komitet Ministrów w Strasburgu w dniu 15 czerwca 1999 r.; art. 23 ust. 2 konwencji nr 108 w nowym brzmieniu.

10 RE, Protokół dodatkowy do Konwencji o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych dotyczący organów nadzoru i transgranicznych przepływów danych, CETS nr 181, 2001.

1.1.3. Prawo Unii Europejskiej dotyczące ochrony danych

Prawo UE składa się z traktatów i prawa wtórnego UE. Traktaty, czyli Traktat o Unii Europejskiej (TUE) i Traktat o funkcjonowaniu Unii Europejskiej (TFUE), zostały zaaprobowane 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".

Głównym aktem prawnym UE dotyczącym ochrony danych jest 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*)[11]. Przyjęto ją w 1995 r., gdy niektóre państwa członkowskie posiadały już krajowe przepisy dotyczące ochrony danych. Swobodny przepływ towarów, kapitału, usług i osób w obrębie rynku wewnętrznego wymagał swobodnego przepływu danych, który nie byłby możliwy, gdyby państwa członkowskie nie mogłyby powołać się na jednolity, wysoki poziom ochrony danych.

Jako że celem przyjęcia dyrektywy o ochronie danych była harmonizacja[12] prawa o ochronie danych na szczeblu krajowym, jej przepisy cechują się stopniem szczegółowości porównywalnym do (wówczas) obowiązujących krajowych przepisów dotyczących ochrony danych. Według TSUE „Dyrektywa 95/46 ma na celu [...] zapewnienie, że poziom ochrony praw i wolności osób w odniesieniu do przetwarzania danych osobowych, będzie równoważny we wszystkich państwach członkowskich. [...] Przybliżenie przepisów krajowych właściwych w tym obszarze nie musi się przyczyniać do zmniejszenia ochrony przez nie przewidzianej, ale, wręcz przeciwnie, musi dążyć do zapewnienia wysokiego poziomu ochrony w UE. W związku z tym, [...] harmonizacja tych przepisów krajowych nie jest ograniczona do minimalnej harmonizacji, ale oznacza harmonizację, która jest generalnie całkowita"[13]. Ponadto państwa członkowskie dysponują ograniczonym marginesem swobody przy wdrażaniu dyrektywy.

11 Dyrektywa o ochronie danych, Dz.U. L 281 z 23.11.1995, s. 31.

12 Zob. na przykład dyrektywę o ochronie danych, motywy 1, 4, 7 i 8.

13 TSUE, sprawy połączone C-468/10 oraz C-469/10, *Asociación Nacional de Establecimientos Financieros de Crédito (ASNEF) and Federación de Comercio Electrónico y Marketing Directo (FECEMD) przeciwko Administración del Estado*, 24 listopada 2011, ust. 28-29."

Celem dyrektywy o ochronie danych jest skonkretyzowanie zawartych już w konwencji nr 108 zasad dotyczących prawa do prywatności oraz ich rozszerzenie. W związku z faktem, że wszystkie 15 państw członkowskich UE w 1995 r. było również umawiającymi się stronami konwencji nr 108, wykluczone jest przyjęcie sprzecznych ze sobą przepisów w tych dwóch aktach prawnych. 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).

Zakres terytorialny stosowania dyrektywy o ochronie danych wykracza poza 28 państw członkowskich UE, obejmując także inne państwa należące do Europejskiego Obszaru Gospodarczego (EOG)[14], tj. Islandię, Liechtenstein i Norwegię.

TSUE w Luksemburgu jest właściwy do ustalenia, czy państwo członkowskie wypełnia swoje zobowiązania na mocy dyrektywy o ochronie danych, oraz do orzekania w trybie prejudycjalnym o ważności i wykładni dyrektywy w celu zapewnienia jej skutecznego i jednolitego stosowania w państwach członkowskich. Ważnym wyłączeniem od stosowania dyrektywy o ochronie danych jest tzw. zwolnienie dotyczące danych o charakterze domowym, które dotyczy przetwarzania danych osobowych przez osoby prywatne wyłącznie w celach osobistych lub domowych[15]. Przetwarzanie takie jest generalnie uznawane za element wolności osoby prywatnej.

Zgodnie z prawem pierwotnym UE obowiązującym w chwili przyjęcia dyrektywy o ochronie danych zakres przedmiotowy tej dyrektywy ogranicza się do zagadnień rynku wewnętrznego. Poza jej zakresem stosowania znajdują się, co najważniejsze, zagadnienia współpracy policyjnej i sądowej w sprawach karnych. Ochrona danych w takich przypadkach opiera się na innych aktach prawnych, które omówiono szczegółowo w rozdziale 7.

W związku z tym, że dyrektywa o ochronie danych mogła objąć swoim zakresem tylko państwa członkowskie UE, niezbędny był dodatkowy akt prawny, aby

14 Porozumienie o Europejskim Obszarze Gospodarczym, Dz.U. L 1 z 3.1.1994, które weszło w życie dnia 1 stycznia 1994 r.

15 Dyrektywa o ochronie danych, art. 3 ust. 2 tiret drugie.

zapewnić ochronę danych w związku z przetwarzaniem danych osobowych przez instytucje i organy UE. Funkcję tę pełni 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*)[16].

Ponadto nawet w dziedzinach objętych zakresem dyrektywy o ochronie danych niezbędne bywają często bardziej szczegółowe przepisy dotyczące ochrony danych, aby wyważyć inne uzasadnione interesy w wystarczająco jasny sposób. Dwoma przykładami są tutaj dyrektywa 2002/58/WE dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (*dyrektywa o prywatności i łączności elektronicznej*)[17] oraz dyrektywa 2006/24/WE 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 (*dyrektywa o zatrzymywaniu danych,* unieważniona 8 kwietnia 2014 r.)[18]. Inne przykłady zostaną omówione w rozdziale 8. Przepisy takie muszą być zgodne z dyrektywą o ochronie danych.

Karta praw podstawowych Unii Europejskiej

Traktaty założycielskie Wspólnot Europejskich nie zawierały żadnych odniesień do praw człowieka lub ich ochrony. Kiedy jednak do ówczesnego Trybunału Sprawiedliwości Wspólnot Europejskich zaczęły trafiać skargi dotyczące naruszeń praw człowieka w obszarach wchodzących w zakres prawa UE, wypracowano nowe podejście. Aby przyznać ochronę osobom fizycznym, w poczet tzw. ogólnych zasad prawa europejskiego włączono prawa podstawowe. Według TSUE wspomniane ogólne zasady odzwierciedlają zakres ochrony praw człowieka na mocy konstytucji krajowych i traktatów dotyczących praw człowieka, w szczególności EKPC. W opinii TSUE takie włączenie zapewni zgodność prawa UE z tymi zasadami.

16 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.

17 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.

18 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 (*dyrektywa o zatrzymywaniu danych*), Dz.U. L 105, unieważniona 8 kwietnia 2014 r.

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[19] jako prawo pierwotne UE (zob. art. 6 ust. 1 TUE) wraz z wejściem w życie 1 grudnia 2009 r. Traktatu z Lizbony[20].

W prawie pierwotnym UE przyznano także UE ogólne kompetencje do stanowienia prawa w zakresie ochrony danych (art. 16 TFUE).

W karcie zagwarantowano nie tylko poszanowanie życia prywatnego i rodzinnego (art. 7), ale również ustanowiono prawo do ochrony danych osobowych (art. 8), wyraźnie podnosząc je 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 w kilka lat po 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, ale także zamieszczono odniesienie do podstawowych zasad ochrony danych w art. 8 ust. 2. Wreszcie, w art. 8 ust. 3 zagwarantowano kontrolę przestrzegania tych zasad przez niezależny organ.

Perspektywy

W styczniu 2012 r. Komisja Europejska zaproponowała pakiet dotyczący reformy w zakresie ochrony danych, stwierdzając, że obecne przepisy wymagają modernizacji w związku z szybkim rozwojem technicznym i globalizacją. Pakiet dotyczący reformy składa się z wniosku dotyczącego ogólnego rozporządzenia o ochronie

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

20 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.

danych[21], które ma zastąpić dyrektywę o ochronie danych, jak również nowej dyrektywy o ochronie danych[22], która zapewni ochronę danych w obszarze współpracy policyjnej i sądowej w sprawach karnych. W chwili publikacji niniejszego podręcznika trwały dyskusje na temat pakietu.

1.2. Wyważenie praw

Najważniejsza kwestia

- Prawo do ochrony danych osobowych nie jest prawem absolutnym i musi zostać wyważone względem innych praw.

Prawo podstawowe do ochrony danych osobowych na mocy art. 8 karty praw podstawowych „nie stanowi jednak prawa o charakterze absolutnym i powinno być oceniane w świetle jego funkcji społecznej”[23]. Tak więc w art. 52 ust. 1 karty uznano, że w korzystaniu z praw, takich jak te wskazane w jej art. 7 i 8, mogą zostać wprowadzone ograniczenia, o ile są one przewidziane ustawą, szanują istotę tych praw i wolności oraz, z zastrzeżeniem zasady proporcjonalności, są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię Europejską lub potrzebom ochrony praw i wolności innych osób[24].

W ramach EKPC ochronę danych gwarantuje art. 8 (prawo do poszanowania życia prywatnego i rodzinnego); podobnie jak w przypadku karty praw podstawowych, prawo to musi być stosowane przy poszanowaniu zakresu innych konkurencyjnych praw. Zgodnie z art. 8 ust. 2 EKPC „[n]iedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa z wyjątkiem przypadków przewidzianych przez

21 Komisja Europejska (2012), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólnego rozporządzenia o ochronie danych), COM(2012) 11 final, Bruksela, 25 stycznia 2012 r.

22 Komisja Europejska (2012), Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (ogólnej dyrektywy o ochronie danych), COM(2012) 10 final, Bruksela, 25 stycznia 2012 r.

23 Zob. na przykład TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r., pkt 48.

24 *Tamże*, pkt 50.

ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na [...] ochronę praw i wolności osób".

W konsekwencji zarówno ETPC, jak i TSUE wielokrotnie stwierdzały, że przy stosowaniu i interpretacji art. 8 EKPC oraz art. 8 karty praw podstawowych niezbędne jest wyważenie ich z innymi prawami[25]. Sposób takiego wyważenia zostanie zilustrowany na kilku ważnych przykładach.

1.2.1. Wolność wypowiedzi

Jednym z praw, które często wchodzą w konflikt 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". Artykuł 11 odpowiada art. 10 EKPC. Zgodnie z art. 52 ust. 3 karty praw podstawowych, w zakresie, w jakim zawiera ona prawa, które odpowiadają prawom zagwarantowanym w EKPC, „ich znaczenie i zakres są takie same jak praw przyznanych przez tę konwencję". Dlatego też ograniczenia, które mogą zostać zgodnie z prawem nałożone na prawo zagwarantowane w art. 11 karty, nie mogą wykraczać poza przewidziane w art. 10 ust. 2 EKPC, czyli muszą być przewidziane przez ustawę i niezbędne w społeczeństwie demokratycznym „z uwagi na [...] ochronę dobrego imienia i praw innych osób". Pojęcie to obejmuje prawo do ochrony danych.

Związek między ochroną danych osobowych a wolnością wypowiedzi uregulowano w art. 9 dyrektywy o ochronie danych zatytułowanym „Przetwarzanie danych osobowych i wolność wypowiedzi"[26]. Zgodnie z tym artykułem państwa członkowskie zostały zobowiązane do ustanowienia pewnych odstępstw lub ograniczeń ochrony

25 ETPC, Von Hannover przeciwko Niemcom (nr 2) [Wielka Izba], 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*, 29 stycznia 2008 r., pkt 68. Zob. też Rada Europy (2013), Case law of the European Court of Human Rights concerning the protection of personal data [„Orzecznictwo Europejskiego Trybunału Praw Człowieka w sprawie ochrony danych osobowych"], DP (2013) Case Law, dokument dostępny pod adresem: www.coe.int/t/dghl/standardsetting/dataprotection/Judgments/DP%202013%20Case%20Law_Eng%20%28final%2018%2007%202013%29.pdf.

26 Dyrektywa o ochronie danych, art. 9.

danych, odnoszących się w związku z tym do podstawowego prawa do prywatności, które zostały przewidziane w rozdziałach II, IV i VI tej dyrektywy. Odstępstwa te powinny zostać ustanowione jedynie w celach dziennikarskich lub w celu uzyskania wyrazu artystycznego lub literackiego, co jest objęte podstawowym prawem do wolności wypowiedzi, o ile jest to konieczne do pogodzenia prawa do prywatności z przepisami dotyczącymi wolności wypowiedzi".

Przykład: W sprawie *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy*[27] zwrócono się do TSUE o wykładnię art. 9 dyrektywy o ochronie danych oraz o określenie związku między ochroną danych a wolnością prasy. Trybunał badał sprawę rozpowszechniania przez Markkinapörssi i Satamedia danych podatkowych około 1,2 mln osób fizycznych uzyskanych zgodnie z prawem od fińskich organów podatkowych. W szczególności miał on za zadanie 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 Satakunnan stanowiły „przetwarzanie danych osobowych" w rozumieniu art. 3 ust. 1 dyrektywy o ochronie danych, Trybunał przystąpił do wykładni art. 9 dyrektywy. Najpierw 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 Trybunał uznał, że działania takie, jak prowadzone przez Markkinapörssi i Satamedia, 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. TSUE pozostawił jednak sądowi krajowemu ustalenie, czy tak było w tym konkretnym przypadku.

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

Jeżeli chodzi o godzenie prawa do ochrony danych z prawem do wolności wypowiedzi, kilka przełomowych wyroków wydał Europejski Trybunał Praw Człowieka.

Przykład: W sprawie *Axel Springer AG przeciwko Niemcom*[28] ETPC uznał, że zakaz nałożony przez sąd krajowy na właściciela gazety, który chciał opublikować artykuł na temat aresztowania i skazania znanego aktora, naruszał art. 10 EKPC. ETPC ponownie wymienił kryteria, które ustanowił w swoim orzecznictwie, wyważając prawo do wolności wypowiedzi z prawem do poszanowania życia prywatnego:

- po pierwsze, czy zdarzenie, którego dotyczył opublikowany artykuł, stanowiło przedmiot ogólnego zainteresowania; aresztowanie i skazanie osoby było publicznym faktem związanym z wymiarem sprawiedliwości, a zatem była to kwestia stanowiąca przedmiot publicznego zainteresowania;

- po drugie, czy dana osoba była osobą publiczną: chodziło o aktora na tyle znanego, aby można go było zakwalifikować jako osobę publiczną; oraz

- po trzecie, w jaki sposób uzyskano informacje i czy były one wiarygodne: informacje zostały dostarczone przez prokuraturę, a dokładność informacji zawartych w obydwu publikacjach nie była przedmiotem sporu między stronami.

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: W sprawie *Von Hannover przeciwko Niemcom (nr 2)*[29] ETPC nie stwierdził naruszenia prawa do poszanowania życia prywatnego na mocy art. 8 EKPC, gdy księżniczce Karolinie z Monako odmówiono nakazu sądowego zapobiegającego publikacji zdjęcia jej i jej męża podczas urlopu na nartach. Zdjęciu towarzyszył artykuł, w którym informowano między innymi o złym stanie zdrowia księcia Rainiera. ETPC stwierdził, że sądy krajowe starannie wyważyły prawo do wolności wypowiedzi wydawnictw z jednej strony oraz prawo skarżących do poszanowania ich życia prywatnego z drugiej strony. Określenie

28 ETPC, *Axel Springer AG przeciwko Niemcom* [Wielka Izba], nr 39954/08, 7 lutego 2012 r., pkt 90 i 91.

29 ETPC, *Von Hannover przeciwko Niemcom (nr 2)* [Wielka Izba], nr 40660/08 i 60641/08, 7 lutego 2012 r., pkt 118 i 124.

przez sądy krajowe choroby księcia Rainiera jako wydarzenia istotnego dla współczesnego społeczeństwa nie może zostać uznane za nieuzasadnione i ETPC przyjął, że zdjęcie, rozpatrywane w świetle tego artykułu, wnosiło przynajmniej w pewnym stopniu wkład w debatę stanowiącą przedmiot ogólnego zainteresowania. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

W orzecznictwie ETPC jednym z najważniejszych kryteriów związanych z wyważeniem tych praw jest to, czy dana wypowiedź wnosi wkład w debatę stanowiącą przedmiot ogólnego zainteresowania publicznego.

Przykład: W sprawie *Mosley przeciwko Zjednoczonemu Królestwu*[30] krajowy tygodnik opublikował intymne zdjęcia skarżącego. Skarżący zarzucił następnie naruszenie art. 8 EKPC, gdyż nie był w stanie wystąpić o nakaz sądowy przed publikacją tych zdjęć ze względu na brak wymogu uprzedniego zgłoszenia przez gazetę zamiaru publikacji materiałów mogących naruszyć prawo do prywatności. Chociaż rozpowszechnianie tych materiałów służyło ogólnie celom rozrywki, a nie edukacji, 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. Należy 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 zakres uznania w tej dziedzinie, ETPC stwierdził, że istnienie prawnie wiążącego wymogu uprzedniego zgłoszenia nie jest wymagane na mocy art. 8. W związku z tym Trybunał stwierdził, że nie doszło do naruszenia art. 8.

Przykład: W sprawie *Biriuk przeciwko Litwie*[31] skarżąca domagała się odszkodowania od dziennika, który opublikował artykuł informujący, że jest ona nosicielką wirusa HIV. Informacje te miały rzekomo zostać potwierdzone przez lekarzy z lokalnego szpitala. ETPC nie uznał, aby wspomniany artykuł wnosił wkład w jakąkolwiek debatę stanowiącą przedmiot ogólnego zainteresowania, i powtórzył, że ochrona danych osobowych, w szczególności danych medycznych, ma fundamentalne znaczenie w kontekście korzystania przez konkretną osobę z prawa do poszanowania życia prywatnego i rodzinnego, co gwarantuje art. 8 EKPC. Trybunał przywiązał szczególną wagę do faktu, że zgodnie z

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

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

informacjami podanymi w gazecie personel medyczny szpitala udzielił informacji o zakażeniu HIV skarżącej z ewidentnym naruszeniem obowiązku zachowania tajemnicy lekarskiej. W związku z tym państwo nie zagwarantowało skarżącej prawa do poszanowania jej życia prywatnego. Trybunał stwierdził, że doszło do naruszenia art. 8.

1.2.2. Dostęp do dokumentów

Zgodnie z art. 11 karty praw podstawowych oraz art. 10 EKPC wolność informacji obejmuje prawo nie tylko do przekazywania, ale także do *otrzymywania* informacji. Coraz bardziej rośnie świadomość znaczenia, jakie ma przejrzyste działanie rządu dla funkcjonowania demokratycznego społeczeństwa. W związku z tym w ostatnich dwóch dekadach prawo dostępu do dokumentów znajdujących się w posiadaniu organów władzy publicznej zostało uznane za istotne prawo każdego obywatela UE oraz każdej osoby fizycznej lub prawnej mającej miejsce zamieszkania bądź 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*)[32]. **W prawie UE** prawo dostępu do dokumentów jest zagwarantowane rozporządzeniem nr 1049/2001 w sprawie publicznego dostępu do dokumentów Parlamentu Europejskiego, Rady i Komisji (*rozporządzeniem o dostępie do dokumentów*)[33].W art. 42 karty praw podstawowych oraz art. 15 ust. 3 TFUE to prawo dostępu rozszerzono o „dokument[y] instytucji, organów i jednostek organizacyjnych Unii, niezależnie od ich formy". Zgodnie z art. 52 ust. 2 karty prawo dostępu do dokumentów jest również wykonywane na warunkach i w granicach określonych w art. 15 ust. 3 TFUE. Prawo to może wejść w kolizję z prawem do ochrony danych, jeżeli dostęp do dokumentu skutkowałby ujawnieniem danych osobowych innych osób. Może zatem być niezbędne wyważenie wniosków o dostęp do dokumentów lub informacji znajdujących się w posiadaniu organów władzy publicznej z prawem do ochrony danych osób, których dane są zawarte w żądanych dokumentach.

32 Rada Europy, Komitet Ministrów (2002), Recommendation Rec(2002)2 to member states on access to official documents [„Zalecenie Rec(2002)2 dla państw członkowskich w sprawie dostępu do dokumentów urzędowych"], 21 lutego 2002 r.; Rada Europy, Konwencja w sprawie dostępu do dokumentów urzędowych, CETS nr 205, 18 czerwca 2009 r. Konwencja nie weszła jeszcze w życie.

33 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 31.5.2001.

Przykład: W sprawie *Komisja przeciwko Bavarian Lager*[34] 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*). 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. Nie zgadzając się z tym stanowiskiem, Bavarian Lager wniosła skargę do Sądu Pierwszej Instancji, który 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. TSUE 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 znajdują w pełni

34 TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd.*, 29 czerwca 2010 r., pkt 60, 63, 76, 78 i 79.

zastosowanie. TSUE 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.

Zgodnie z tym wyrokiem ingerencja w prawo do ochrony danych w przypadku dostępu do dokumentów wymaga szczególnego i uzasadnionego powodu. Prawo dostępu do dokumentów nie może automatycznie uchylać prawa do ochrony danych[35].

W kolejnym wyroku ETPC zajęto się szczególnym aspektem wniosku o dostęp.

Przykład: W sprawie *Társaság a Szabadságjogokért przeciwko Węgrom*[36] skarżący, którym jest organizacja pozarządowa zajmująca się prawami człowieka, złożył do Trybunału Konstytucyjnego wniosek o dostęp do informacji o toczącym się postępowaniu. Nie konsultując się z posłem, który wniósł przedeń sprawę, Trybunał Konstytucyjny odrzucił wniosek o dostęp, uzasadniając, że rozpatrywane przezeń skargi mogą zostać udostępnione stronom trzecim wyłącznie za zgodą skarżącego. Sądy krajowe podtrzymały tę odmowę, stwierdzając, że inne uzasadnione interesy, w tym także dostęp do informacji publicznej, nie mogą przeważać nad ochroną takich danych osobowych. Skarżący działał jako „społeczna organizacja strażnicza", której działalność zasługiwała na ochronę podobną do przyznawanej prasie. Zgodnie z utrwalonym

35 Zob. jednak szczegółowe rozważania w: Europejski Inspektor Ochrony Danych (EIOD) (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* [„Dostęp publiczny do dokumentów zawierających dane osobowe po orzeczeniu *Bavarian Lager*"], Bruksela, 24 marca 2011 r., dokument dostępny pod adresem: www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

36 ETPC, *Társaság a Szabadságjogokért przeciwko Węgrom*, nr 37374/05, 14 kwietnia 2009 r.; zob. pkt 27, 36–38.

orzecznictwem ETPC odnoszącym się do wolności prasy społeczeństwo ma prawo do otrzymywania informacji stanowiących przedmiot ogólnego zainteresowania. Informacje, o które wnioskował skarżący, były „gotowe i dostępne", nie wymagając żadnego gromadzenia danych. W takich okolicznościach państwo miało obowiązek nieutrudniania przepływu informacji, o które wnioskował skarżący. Podsumowując, ETPC uznał, że przeszkody mające na celu utrudnienie dostępu do informacji będących przedmiotem zainteresowania publicznego mogą zniechęcać osoby pracujące w mediach lub pokrewnych dziedzinach do wykonywania ważnej roli „strażnika publicznego". Trybunał stwierdził, że doszło do naruszenia art. 10.

Znaczenie przejrzystości **w prawie UE** nie ulega wątpliwości. Zasadę przejrzystości zapisano w art. 1 i 10 TUE oraz w art. 15 ust. 1 TFUE[37]. Zgodnie z motywem 2 rozporządzenia (WE) nr 1049/2001 pozwala ona obywatelom na bliższe uczestnictwo w procesie podejmowania decyzji i gwarantuje, że administracja cieszy się większą prawowitością, jest bardziej skuteczna i odpowiedzialna względem obywateli w systemie demokratycznym[38].

Zgodnie z tym rozumowaniem w rozporządzeniu Rady (WE) nr 1290/2005 w sprawie finansowania wspólnej polityki rolnej oraz w rozporządzeniu Komisji (WE) nr 259/2008 ustanawiającym szczegółowe zasady jego stosowania zawarto wymóg publikowania informacji na temat beneficjentów pewnych funduszy UE w sektorze rolnym oraz kwot otrzymanych przez poszczególnych beneficjentów[39]. Ich publikacja powinna przyczynić się do publicznej kontroli właściwego wykorzystania środków publicznych przez administrację. Kilku beneficjentów zakwestionowało proporcjonalność publikacji tych danych.

37 UE (2012), Skonsolidowane wersje Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, Dz.U. C 326 z 26.10.2012.

38 TSUE, C-41/00 P, *Interporc Im- und Export GmbH przeciwko Komisji Wspólnot Europejskich*, 6 marca 2003 r., pkt 39; oraz TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*., 29 czerwca 2010 r., pkt 54.

39 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; oraz 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.

Przykład: W sprawach *Volker und Markus Schecke oraz Hartmut Eifert przeciwko Land Hessen*[40] TSUE musiał ocenić proporcjonalność wymaganej na mocy ustawodawstwa UE publikacji nazwisk beneficjentów dopłat rolnych UE i otrzymanych przez nich kwot.

Trybunał, zauważając, że prawo do ochrony danych nie stanowi prawa o charakterze absolutnym, stwierdził, iż publikacja na stronie internetowej imiennych danych o beneficjentach dwóch funduszy rolnych UE oraz o dokładnych otrzymanych kwotach stanowi ogólnie ingerencję w ich życie prywatne, a w szczególności w ich prawo do ochrony danych osobowych.

Trybunał uznał, że możliwość ingerencji w prawa na mocy art. 7 i 8 karty praw podstawowych została przewidziana przepisami prawa i służyła celowi interesu ogólnego uznawanego przez UE, a mianowicie poprawie przejrzystości wykorzystania funduszy wspólnotowych. TSUE orzekł jednak, że publikacja nazwisk osób fizycznych będących beneficjentami dotacji rolnych UE z tych dwóch funduszy oraz dokładnych otrzymanych kwot stanowiła środek nieproporcjonalny i nie była uzasadniona w świetle art. 52 ust. 1 karty praw podstawowych. Trybunał stwierdził zatem częściową nieważność ustawodawstwa UE w sprawie publikacji informacji dotyczących beneficjentów europejskich funduszy rolnych.

1.2.3. 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. 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[41]. Prawo zagwarantowane w art. 13 karty praw podstawowych może także podlegać ograniczeniom dopuszczalnym zgodnie z art. 10 EKPC[42].

40 TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR (C-92/09) oraz Hartmut Eifert (C-93/09) przeciwko Land Hessen*, 9 listopada 2010 r., pkt 47–52, 58, 66–67, 75, 86 i 92.

41 ETPC, *Müller i inni przeciwko Szwajcarii*, nr 10737/84, 24 maja 1988 r.

42 Wyjaśnienia dotyczące karty praw podstawowych, Dz.U. C 303 z 14.12.2007.

Przykład: W sprawie *Vereinigung bildender Künstler przeciwko Austrii*[43] sądy austriackie zakazały skarżącemu stowarzyszeniu dalszego wystawiania obrazu, który przedstawiał zdjęcia głów różnych osób publicznych 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. ETPC 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 stwierdził, że doszło do naruszenia art. 10 EKPC.

Jeżeli chodzi o naukę, w europejskim prawie ochrony danych da się dostrzec świadomość jej szczególnej wartości dla społeczeństwa. W związku z tym ogólne ograniczenia dotyczące wykorzystywania danych osobowych zostały złagodzone. Zarówno w dyrektywie o ochronie danych, jak i w konwencji nr 108 dopuszcza się zatrzymywanie danych do celów badań naukowych, gdy nie są one już potrzebne w pierwotnym celu, w którym zostały zgromadzone. Ponadto późniejsze wykorzystanie danych osobowych do badań naukowych nie jest uważane za niezgodne z celem. Bardziej szczegółowe przepisy, w tym niezbędne zabezpieczenia mające na celu pogodzenie interesu związanego z badaniami naukowymi z prawem do ochrony danych, należy zawrzeć w prawie krajowym (zob. także sekcje 3.3.3 i 8.4).

43 ETPC, *Vereinigung bildender Künstler przeciwko Austrii*, nr 68345/01, 25 stycznia 2007 r.; zob. zwłaszcza pkt 26 i 34.

1.2.4. Ochrona własności

Prawo do ochrony własności zapisano w art. 1 pierwszego protokołu do europejskiej konwencji praw człowieka, a także w artykule 17 ust. 1 karty praw podstawowych. 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, ale także prawa dotyczące patentów i znaków towarowych oraz prawa pokrewne.

Jak jasno wynika z orzecznictwa TSUE, ochronę podstawowego prawa własności trzeba wyważyć z ochroną innych praw podstawowych, w szczególności prawa do ochrony danych[44]. W niektórych przypadkach instytucje ochrony praw autorskich domagają się od usługodawców internetowych 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: W sprawie *Promusicae przeciwko Telefónica de España*[45] hiszpański usługodawca internetowy Telefónica odmówił ujawnienia Promusicae, niekomercyjnej organizacji producentów muzycznych oraz wydawców nagrań muzycznych i audiowizualnych, danych osobowych niektórych osób, którym świadczył usługi dostępu do internetu. Promusicae wnioskowała o ujawnienie tych informacji, aby móc wszcząć postępowanie cywilne przeciwko tym 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. 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 praw podstawowych. Trybunał stwierdził, że trzy wymienione dyrektywy, jak również dyrektywa o

44 ETPC, *Ashby Donald i inni przeciwko Francji*, nr 36769/08, 10 stycznia 2013 r.

45 TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU*, 29 stycznia 2008 r., pkt 54 i 60.

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.

TSUE 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”[46].

46 *Tamże*, pkt 65 i 68; zob. też TSUE, C-360/10, *SABAM przeciwko NetlogNV*, 16 lutego 2012 r.

2

Terminologia związana z ochroną danych

UE	Omówione zagadnienia	RE
Dane osobowe		
Artykuł 2 lit. a) dyrektywy o ochronie danych TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r. TSUE, C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU*, 29 stycznia 2008 r.	**Definicja prawna**	Artykuł 2 lit. a) konwencji nr 108 ETPC, *Bernh Larsen Holding AS i inni przeciwko Norwegii*, nr 24117/08, 14 marca 2013 r.
Artykuł 8 ust. 1 dyrektywy o ochronie danych TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.	**Szczególne kategorie danych osobowych (dane szczególnie chronione)**	Artykuł 6 konwencji nr 108
Artykuł 6 ust. 1 lit. e) dyrektywy o ochronie danych	**Dane zanonimizowane i spseudonimizowane**	Artykuł 5 lit. e) konwencji nr 108 Artykuł 42 sprawozdania wyjaśniającego do konwencji nr 108
Przetwarzanie danych		
Artykuł 2 lit. b) dyrektywy o ochronie danych TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.	**Definicje**	Artykuł 2 lit. c) konwencji nr 108

UE	Omówione zagadnienia	RE
Użytkownicy danych		
Artykuł 2 lit. d) dyrektywy o ochronie danych	**Administrator**	Artykuł 2 lit. d) konwencji nr 108 Artykuł 1 lit. g) zalecenia w sprawie profilowania*
Artykuł 2 lit. e) dyrektywy o ochronie danych TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.	**Podmiot przetwarzający**	Artykuł 1 lit. h) zalecenia w sprawie profilowania
Artykuł 2 lit. g) dyrektywy o ochronie danych	**Odbiorca**	Artykuł 2 ust. 1 protokołu dodatkowego do konwencji nr 108
Artykuł 2 lit. f) dyrektywy o ochronie danych	**Strona trzecia**	
Zgoda		
Artykuł 2 lit. h) dyrektywy o ochronie danych TSUE, C-543/09, *Deutsche Telekom AG przeciwko Bundesrepublik Deutschland*, 5 maja 2011 r.	**Definicja ważnej zgody i wymagania z nią związane**	Artykuł 6 zalecenia dotyczącego danych medycznych i pewne późniejsze zalecenia

*Uwaga: *Rada Europy, Komitet Ministrów (2010), Recommendation Rec(2010)13 to member states on the protection of individuals with regard to automatic processing of personal data in the context of profiling [„Zalecenie Rec(2010)13 dla państw członkowskich w sprawie ochrony osób fizycznych w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania"] (Zalecenie w sprawie profilowania), 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.
- Osoba jest możliwa do zidentyfikowania, jeżeli bez nadmiernego wysiłku można uzyskać dodatkowe informacje umożliwiające identyfikację osoby, której dane dotyczą.
- Uwierzytelnienie oznacza udowodnienie, że dana osoba posiada pewną tożsamość i/lub jest uprawniona do wykonania pewnych czynności.

- Istnieją szczególne kategorie danych, tak zwane dane szczególnie chronione, wymienione w konwencji nr 108 i dyrektywie o ochronie danych, które wymagają zwiększonej ochrony i podlegają z tego powodu specjalnemu reżimowi prawnemu.
- Dane są zanonimizowane, jeżeli nie zawierają żadnych identyfikatorów; w przypadku danych spseudonimizowanych identyfikatory są zaszyfrowane.
- W przeciwieństwie do danych zanonimizowanych dane spseudonimizowane są danymi osobowymi.

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[47], czyli informacje o osobie, której tożsamość jest oczywista bądź przynajmniej może zostać ustalona przez uzyskanie dodatkowych informacji.

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

Osoba

Prawo do ochrony danych wywodzi się z prawa do poszanowania życia prywatnego. Pojęcie życia prywatnego odnosi się do istot ludzkich. Dlatego też głównymi beneficjentami ochrony danych są osoby fizyczne. Ponadto zgodnie z opinią Grupy Roboczej Art. 29 na mocy europejskiego prawa o ochronie danych ochrona przysługuje jedynie *osobom żyjącym*[48].

Orzecznictwo ETPC odnoszące się do art. 8 EKPC wskazuje, że całkowite rozdzielenie zagadnień związanych z życiem prywatnym i zawodowym bywa trudne[49].

47 Dyrektywa o ochronie danych, art. 2 lit. a); konwencja nr 108, art. 2 lit. a).

48 Grupa Robocza Art. 29 (2007), *Opinia 4/2007 w sprawie pojęcia danych osobowych*, WP 136, 20 czerwca 2007 r., s. 22.

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

Przykład: W sprawie *Amann przeciwko Szwajcarii*[50] władze przechwyciły połączenie przychodzące do skarżącego, podczas którego omawiano sprawy biznesowe. W oparciu o tę rozmowę władze wszczęły dochodzenie w sprawie skarżącego i założyły mu rekord w bazie danych dotyczących bezpieczeństwa narodowego. Chociaż przechwycono biznesową rozmowę telefoniczną, ETPC uznał przechowywanie danych na temat tej rozmowy za odnoszące się do życia prywatnego skarżącego. Wskazał przy tym, że terminu „życie prywatne" nie można interpretować w sposób zawężający, w szczególności dlatego, że poszanowanie życia prywatnego obejmuje prawo do nawiązywania i rozwijania relacji z innymi ludźmi. Ponadto nie było uzasadnienia dla wyłączenia działalności zawodowej lub biznesowej z zakresu „życia prywatnego". Tak szeroka interpretacja odpowiada przyjętej w konwencji nr 108. Ponadto ETPC ustalił, że ingerencja w przypadku skarżącego nie była zgodna z prawem, gdyż prawo krajowe nie zawierało konkretnych i szczegółowych przepisów dotyczących gromadzenia, rejestrowania oraz przechowywania informacji. W związku z tym stwierdził, że doszło do naruszenia art. 8 EKPC.

Ponadto jeżeli sprawy zawodowe również mogą być przedmiotem ochrony danych, wydaje się wątpliwe, aby należało ją przyznawać tylko osobom fizycznym. Prawa na mocy EKPC przysługują nie tylko osobom fizycznym, lecz wszystkim.

Istnieje orzecznictwo ETPC w sprawie skarg osób prawnych zarzucających naruszenie ich prawa do ochrony przed wykorzystaniem ich danych na mocy art. 8 EKPC. Trybunał zbadał jednak odnośną sprawę z punktu widzenia prawa do poszanowania mieszkania i korespondencji, a nie życia prywatnego.

Przykład: Sprawa *Bernh Larsen Holding AS i inni przeciwko Norwegii*[51] 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 firmy.

ETPC stwierdził, że taki obowiązek nałożony na skarżące przedsiębiorstwa stanowił ingerencję w ich prawa do poszanowania „mieszkania" oraz „korespondencji" w rozumieniu artykułu 8 EKPC. Trybunał stwierdził wszakże też, że

50 ETPC, *Amann przeciwko Szwajcarii* [Wielka Izba], nr 27798/95, 16 lutego 2000 r., pkt 65.

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

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 w związku z tym do naruszenia art. 8.

Zgodnie z **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. **Prawo o ochronie danych UE** nie obejmuje generalnie ochrony osób prawnych w odniesieniu do przetwarzania ich danych. Krajowe organy regulacyjne mają swobodę ustanawiania regulacji w tym zakresie[52].

Przykład: W sprawach *Volker und Markus Schecke oraz Hartmut Eifert przeciwko Land Hessen*[53] 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. [...P]oszanowanie 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 [...]"[54].

Możliwość identyfikacji osoby

Zarówno **w prawie UE**, jak i **w prawie RE** informacje zawierają dane o osobie, jeżeli:

- w informacjach tych zidentyfikowano osobę; lub

52 Dyrektywa o ochronie danych, motyw 24.

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

54 *Tamże*, pkt 52.

- osoba, choć nie zidentyfikowano jej, została opisana w tych informacjach w sposób, który umożliwia ustalenie, kim jest osoba, której dane dotyczą, po przeprowadzeniu dalszych badań.

Obydwa rodzaje informacji są chronione w taki sam sposób na mocy europejskiego prawa o ochronie danych. ETPC wielokrotnie stwierdzał, że pojęcie „danych osobowych" na mocy EKPC jest identyczne, jak w konwencji nr 108, w szczególności w odniesieniu do warunku, aby informacje odnosiły się do zidentyfikowanych lub możliwych do zidentyfikowania osób[55].

W definicjach prawnych danych osobowych nie zawarto dodatkowych wyjaśnień, kiedy daną osobę uważa się za zidentyfikowaną[56]. Identyfikacja najwyraźniej wymaga elementów opisujących osobę w taki sposób, że jest ona możliwa do odróżnienia od wszystkich innych osób i możliwa do rozpoznania jako jednostka. Doskonałym przykładem takiego elementu opisu jest nazwisko danej osoby. W wyjątkowych przypadkach podobny do nazwiska skutek mogą nieść inne identyfikatory. W przypadku osób publicznych wystarczające może być odniesienie do stanowiska danej osoby, np. przewodniczącego Komisji Europejskiej.

Przykład: W sprawie *Promusicae*[57] TSUE stwierdził, że „bezsporne jest, że żądane przez Promusicae przekazanie nazwisk i adresów określonych użytkowników [pewnej internetowej platformy wymiany plików] wiąże się z udostępnieniem danych osobowych, to znaczy – zgodnie z definicją zawartą w art. 2 lit. a) dyrektywy 95/46 – informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób fizycznych [...]. Tego rodzaju przekazanie informacji, które zdaniem Promusicae są przechowywane przez Telefónicę – czemu ta ostatnia nie zaprzecza – stanowi przetwarzanie danych osobowych w rozumieniu art. 2 akapit pierwszy dyrektywy 2002/58 w związku z art. 2 lit. b) dyrektywy 95/46".

Jako że wiele nazwisk się powtarza, w celu ustalenia tożsamości osoby konieczne mogą być dodatkowe identyfikatory gwarantujące, że osoby tej nie mylimy z inną. Często wykorzystywane są data i miejsce urodzenia. Ponadto w niektórych krajach

55 Zob. ETPC, *Amann przeciwko Szwajcarii* [Wielka Izba], nr 27798/95, 16 lutego 2000 r., pkt 65 i in.

56 Zob. też ETPC, *Odièvre przeciwko Francji* [Wielka Izba], nr 42326/98, 13 lutego 2003 r.; oraz ETPC, *Godelli przeciwko Włochom*, nr 33783/09, 25 września 2012 r.

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

wprowadzono indywidualne numery w celu lepszego rozróżnienia między obywatelami. W erze technologii coraz ważniejszym środkiem identyfikacji osób stają się dane biometryczne, takie jak odciski palców, zdjęcia cyfrowe czy skany tęczówki.

Aby jednak zastosowanie znalazło europejskie prawo o ochronie danych, nie jest niezbędna wysokiej jakości 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[58]. Zgodnie z motywem 26 dyrektywy o ochronie danych 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 stronami trzecimi (zob. sekcję 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, gdyż 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 dyrektywy o ochronie danych. 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

58 Dyrektywa o ochronie danych, art. 2 lit. a).

gromadzeniem danych na temat możliwych do zidentyfikowania osób, a zatem wymagają podstawy prawnej na mocy prawa o ochronie danych.

W prawie RE możliwość identyfikacji jest rozumiana w podobny sposób. Na przykład w art. 1 ust. 2 zalecenia w sprawie danych wykorzystywanych do płatności[59] stwierdza się, że danej osoby nie uznaje się za „możliwą do identyfikacji", jeżeli taka identyfikacja wymaga nadmiernego nakładu czasu, kosztów lub pracy ludzkiej.

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; lub prosząc o informacje, które powinny być znane tylko osobie o pewnej tożsamości lub uprawnieniach, takie jak osobisty numer identyfikacyjny (kod PIN) bądź hasło; lub żądając przedstawienia pewnego przedmiotu, który powinna posiadać wyłącznie osoba o pewnej tożsamości lub uprawnieniach, takiego jak specjalna karta chipowa bądź klucz do skrytki bankowej. Oprócz haseł lub kart chipowych, czasem wykorzystywanych w połączeniu z kodem PIN, narzędziem szczególnie przydatnym przy identyfikacji i uwierzytelnianiu osób w komunikacji elektronicznej są podpisy elektroniczne.

Charakter danych

Danymi osobowymi mogą być wszelkiego rodzaju informacje, które odnoszą się do osoby.

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

59 RE, Komitet Ministrów (1990), Recommendation No. R Rec(90) 19 on the protection of personal data used for payment and other related operations [„Zalecenie Rec(90)19 w sprawie ochrony danych osobowych wykorzystywanych do płatności i innych powiązanych czynności"], 13 września 1990 r.

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

W sprawie *Amann*[60] ETPC zinterpretował termin „dane osobowe" jako nieograniczający się do sfery prywatnej danej osoby (zob. sekcję 2.1.1). Znaczenie terminu „dane osobowe" jest także istotne dla dyrektywy o ochronie danych:

> Przykład: W sprawie *Volker und Markus Schecke oraz Hartmut Eifert przeciwko Land Hessen*[61] 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 EKPC, że termin »życie prywatne« nie może być interpretowany w sposób zawężający oraz że »nic nie uzasadnia wyłączenia działalności zawodowej [...] z zakresu życia prywatnego«".

Dane odnoszą się do osób także jeżeli treść informacji pośrednio ujawnia dane o osobie. W niektórych przypadkach, gdy istnieje ścisły związek między przedmiotem lub zdarzeniem, np. telefonem komórkowym, samochodem, wypadkiem z jednej strony, a osobą, np. jako jego właścicielem, użytkownikiem, ofiarą z drugiej strony, wówczas informacje o przedmiocie bądź zdarzeniu należy także uznać za dane osobowe.

> Przykład: W sprawie *Uzun przeciwko Niemcom*[62] skarżący wraz z innym mężczyzną znaleźli się pod nadzorem sprawowanym za pośrednictwem urządzenia globalnego systemu pozycjonowania (GPS) zamontowanego w samochodzie wspomnianego innego mężczyzny z powodu ich podejrzewanego udziału w zamachach bombowych. W tym przypadku ETPC uznał, że obserwacja skarżącego przy użyciu GPS stanowiła ingerencję w jego życie prywatne objęte ochroną na mocy art. 8 EKPC. Nadzór GPS był jednak zgodny z prawem, a także proporcjonalny do uzasadnionego celu przeprowadzenia dochodzenia w związku z kilkoma próbami zabójstwa, dlatego też był konieczny w demokratycznym społeczeństwie. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

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

61 TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r., pkt 59.

62 ETPC, *Uzun przeciwko Niemcom*, nr 35623/05, 2 września 2010 r.

Postać występowania danych

Postać, w której przechowywane lub wykorzystywane są dane osobowe, nie ma znaczenia dla zastosowania prawa o ochronie danych. Dane osobowe może zawierać pisemna lub ustna komunikacja, jak też obrazy[63], w tym nagrania telewizji przemysłowej[64], lub dźwięki[65]. Danymi osobowymi mogą być informacje zapisane w postaci elektronicznej, jak też informacje na papierze; danymi osobowymi mogą być nawet próbki tkanki ludzkiej, gdyż zawierają one DNA osoby.

2.1.2. Szczególne kategorie danych osobowych

Zarówno **w prawie UE**, jak i **w prawie RE** istnieją szczególne kategorie danych osobowych, które ze swojej natury mogą stanowić podczas przetwarzania zagrożenie dla osób, których dane dotyczą, i wymagają zwiększonej ochrony. Przetwarzanie tych szczególnych kategorii danych („danych szczególnie chronionych") musi zatem być dozwolone tylko z zastosowaniem specjalnych zabezpieczeń.

Jeżeli chodzi o definicję danych szczególnie chronionych, zarówno w konwencji nr 108 (art. 6), jak i w dyrektywie o ochronie danych (art. 8) wymienia się następujące kategorie:

- dane osobowe ujawniające pochodzenie rasowe lub etniczne;
- dane osobowe ujawniające opinie polityczne, przekonania religijne lub inne; oraz
- dane osobowe dotyczące zdrowia lub życia seksualnego.

Przykład: W sprawie *Bodil Lindqvist*[66] TSUE stwierdził, że „informacja, iż dana osoba doznała urazu stopy i przebywa na zwolnieniu lekarskim w niepełnym wymiarze, stanowi dane osobowe dotyczące zdrowia w rozumieniu art. 8 ust. 1 dyrektywy 95/46".

63 ETPC, *Von Hannover przeciwko Niemcom*, nr 59320/00, 24 czerwca 2004 r.; ETPC, *Sciacca przeciwko Włochom*, nr 50774/99, 11 stycznia 2005 r.

64 ETPC, *Peck przeciwko Zjednoczonemu Królestwu*, nr 44647/98, 28 stycznia 2003 r.; ETPC, *Köpke przeciwko Niemcom*, nr 420/07, 5 października 2010 r.

65 Dyrektywa o ochronie danych, motywy 16 i 17; ETPC, *P.G. i J.H. przeciwko Zjednoczonemu Królestwu*, nr 44787/98, 25 września 2001 r., pkt 59 i 60; ETPC, *Wisse przeciwko Francji*, nr 71611/01, 20 grudnia 2005 r.

66 TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r., pkt 51.

W dyrektywie o ochronie danych jako dane szczególnie chronione wymieniono dodatkowo „przynależność do związków zawodowych", gdyż informacje na ten temat bywają wyraźnym wskazaniem przekonań lub przynależności politycznej.

W konwencji nr 108 za szczególnie chronione uznano także dane osobowe dotyczące skazujących wyroków karnych.

W art. 8 ust. 7 dyrektywy o ochronie danych nakazuje się państwom członkowskim UE określenie warunków, „w których może następować przetwarzanie krajowego numeru identyfikacyjnego lub innego identyfikatora ogólnego stosowania".

2.1.3. Dane zanonimizowane i spseudonimizowane

Zgodnie z zasadą przechowywania danych przez określony czas zapisaną w dyrektywie o ochronie danych, jak również w konwencji nr 108 (i omówioną bardziej szczegółowo w rozdziale 3), dane muszą być „przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane"[67]. Skutkuje to wymogiem anonimizacji danych, jeżeli administrator pragnie je przechowywać po tym, jak utraciły swoją aktualność i nie służą już pierwotnemu celowi.

Dane zanonimizowane

Dane zostały zanonimizowane, jeżeli ze zbioru danych osobowych usunięto wszystkie elementy identyfikujące. Informacje nie mogą zawierać żadnego elementu, przy użyciu którego można byłoby, dokładając rozsądnych starań, ponownie zidentyfikować daną osobę lub osoby[68]. Po udanej anonimizacji dane przestają być danymi osobowymi.

Jeżeli dane osobowe nie służą już swojemu pierwotnemu celowi, lecz mają być przechowywane w spersonalizowanej formie do celów historycznych, statystycznych lub naukowych, w dyrektywie o ochronie danych i konwencji nr 108 dopuszcza się taką możliwość pod warunkiem zastosowania odpowiednich zabezpieczeń przed nadużyciami[69].

67 Dyrektywa o ochronie danych, art. 6 ust. 1 lit. e); oraz konwencja nr 108, art. 5 lit. e).

68 *Tamże*, motyw 26.

69 *Tamże,* art. 6 ust. 1 lit. e); oraz konwencja nr 108, art. 5 lit. e).

Dane spseudonimizowane

Dane osobowe zawierają identyfikatory, takie jak nazwisko, data urodzenia, płeć i adres. Podczas pseudonimizacji danych osobowych identyfikatory te zostają zastąpione jednym pseudonimem. Pseudonimizacja następuje na przykład przez zaszyfrowanie identyfikatorów zawartych w danych osobowych.

Dane spseudonimizowane nie zostały wymienione wprost w definicjach prawnych zawartych w konwencji nr 108 bądź w dyrektywie o ochronie danych. Jednakże w art. 42 sprawozdania wyjaśniającego do konwencji nr 108 stwierdza się, że „wymóg [...] co do terminów zatrzymywania danych w postaci powiązanej z nazwiskami nie oznacza, że dane te powinny zostać po pewnym czasie zostać nieodwracalnie oddzielone od nazwiska osoby, do której się odnoszą, lecz jedynie to, że nie powinna istnieć możliwość łatwego powiązania danych z identyfikatorami". Efekt ten można uzyskać, pseudonimizując dane. Dla osób nieposiadających klucza do odszyfrowania spseudonimizowane dane mogą być możliwe do zidentyfikowania, ale z trudnością. Zachowują one jednak związek z tożsamością w postaci pseudonimu wraz z kluczem do odszyfrowania. Osoby uprawnione do użycia klucza do odszyfrowania mogą łatwo dokonać ponownej identyfikacji. Należy w szczególności zapobiec użyciu kluczy do szyfrowania przez osoby nieuprawnione.

Ponieważ pseudonimizacja danych jest jednym z najważniejszych sposobów zapewnienia ochrony danych na dużą skalę w sytuacjach, gdzie nie jest możliwa całkowita rezygnacja z wykorzystywania danych osobowych, należy bardziej szczegółowo wyjaśnić logikę i skutki takiego działania.

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".

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. W niewielkiej wsi, w której mieszka Charles Spencer, zdanie „C. S. 1967 jest ojcem czwórki dzieci: dwóch chłopców i dwóch dziewczynek" może umożliwiać łatwe rozpoznanie jego osoby. Metoda pseudonimizacji wpływa na skuteczność ochrony danych.

Dane osobowe z zaszyfrowanymi identyfikatorami są wykorzystywane w wielu sytuacjach, aby zachować tożsamość osób w tajemnicy. Jest to szczególnie przydatne, 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 przypadek, gdy naukowiec bada przebieg choroby u pacjentów, których tożsamość jest znana tylko szpitalowi, gdzie są leczeni, i skąd badacz uzyskuje spseudonimizowane historie choroby. Pseudonimizacja stanowi zatem istotny składnik technologii zwiększających prywatność. 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.

2.2. Przetwarzanie danych

Najważniejsze kwestie

- Termin „przetwarzanie" odnosi się przede wszystkim do przetwarzania automatycznego.
- 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.

Ochrona danych na podstawie konwencji nr 108 i dyrektywy o ochronie danych koncentruje się głównie na automatycznym przetwarzaniu danych.

W definicji automatycznego przetwarzania zawartej **w prawie RE** uznaje się jednak, że między operacjami automatycznymi niezbędne mogą być etapy związane z ręcznym wykorzystywaniem danych osobowych. Podobnie **w prawie UE** automatyczne przetwarzanie danych definiuje się jako operacje dokonywane na danych osobowych w całości lub częściowo za pomocą procedur zautomatyzowanych[70].

Przykład: W sprawie *Bodil Lindqvist*[71] TSUE uznał, 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".

Ręczne przetwarzanie danych również wymaga ochrony danych,.

Ochrona danych **w prawie UE** nie jest w żaden sposób ograniczona do automatycznego 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[72]. Powód tego rozszerzenia ochrony danych jest następujący:

- zbiory w postaci papierowej można zorganizować w sposób, który czyni znajdowanie informacji szybkim i łatwym; oraz
- przechowywanie danych osobowych w zorganizowanych zbiorach w postaci papierowej ułatwia obejście określonych w przepisach ograniczeń dotyczących automatycznego przetwarzania danych[73].

W prawie Rady Europy konwencja nr 108 reguluje przede wszystkim przetwarzanie danych w zautomatyzowanych zbiorach danych[74]. Umożliwia ona jednak rozszerzenie ochrony w prawie krajowym tak, aby objęła też przetwarzanie ręczne. Wiele

70 Konwencja nr 108, art. 2 lit. c); oraz dyrektywa o ochronie danych, art. 2 lit. b) i art. 3 ust. 1.

71 TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r., pkt 27.

72 Dyrektywa o ochronie danych, art. 3 ust. 1.

73 *Tamże*, motyw 27.

74 Konwencja nr 108, art. 2 lit. b).

stron konwencji nr 108 skorzystało z tej możliwości i złożyło stosowne deklaracje na ręce Sekretarza Generalnego RE[75]. Rozszerzenie ochrony danych na mocy takiej deklaracji musi dotyczyć wszystkich rodzajów ręcznego przetwarzania danych i nie może się ograniczać do przetwarzania w ręcznych zbiorach[76].

Jeżeli chodzi o charakter czynności klasyfikowanych jako przetwarzanie, definicja przetwarzania **zarówno w prawie UE, jak i RE** jest szeroka: „»przetwarzanie danych osobowych« oznacza każdą operację [...] jak gromadzenie, rejestracja, porządkowanie, przechowywanie, adaptacja lub modyfikacja, odzyskiwanie, konsultowanie, wykorzystywanie, ujawnianie poprzez przekazanie, rozpowszechnianie lub udostępnianie w inny sposób, układanie lub kompilowanie, blokowanie, usuwanie lub niszczenie"[77] dokonywaną na danych osobowych. Termin „przetwarzanie" obejmuje także działania, w ramach których administrator przestaje być odpowiedzialny za dane, przekazując je innemu, który staje się za nie odpowiedzialny.

Przykład: Pracodawcy gromadzą i przetwarzają dane o swoich pracownikach, w tym informacje dotyczące ich wynagrodzeń. Podstawą prawną prowadzenia takich działań zgodnie z prawem jest umowa o pracę.

Pracodawcy muszą przekazywać dane o wynagrodzeniach pracowników organom podatkowym. Takie przekazywanie danych również stanowi „przetwarzanie" w rozumieniu tego pojęcia w konwencji nr 108 i w dyrektywie. W przypadku tego ujawnienia podstawą prawną nie jest jednak umowa o pracę. Musi istnieć dodatkowa podstawa prawna dla czynności przetwarzania, które skutkują przekazaniem danych o wynagrodzeniach przez pracodawcę organom podatkowym. Ta podstawa prawna jest zazwyczaj zawarta w krajowych przepisach podatkowych. Bez tych przepisów przekazywanie danych stanowiłoby ich przetwarzanie niezgodnie z prawem.

75 Zob. deklaracje złożone na podstawie art. 3 ust. 2 lit. c) konwencji nr 108.

76 Zob. sformułowanie art. 3 ust. 2 konwencji nr 108.

77 Dyrektywa o ochronie danych, art. 2 lit. b). Zob. też konwencja nr 108, art. 2 lit. c).

2.3. Użytkownicy danych osobowych

Najważniejsze kwestie

- Dowolna osoba decydująca się przetwarzać dane osobowe innych osób staje się „administratorem" na mocy prawa o ochronie danych; jeżeli taką decyzję podejmuje większa liczba osób wspólnie, mogą one być „współadministratorami".
- „Podmiot przetwarzający" jest odrębnym prawnie podmiotem, który przetwarza dane osobowe w imieniu administratora.
- Podmiot przetwarzający staje się administratorem, jeżeli wykorzystuje dane do własnych celów, nie zaś wykonując polecenia administratora.
- Każdy, kto otrzymuje dane od administratora, jest „odbiorcą".
- „Strona trzecia" oznacza osobę fizyczną lub prawną, która nie wykonuje poleceń administratora (i nie jest osobą, której dane dotyczą).
- „Strona trzecia będąca odbiorcą" oznacza osobę lub podmiot, który jest odrębny prawnie od administratora, ale otrzymuje od niego dane osobowe.

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. Role te mogą zatem odgrywać wyłącznie podmioty, które można pociągnąć do odpowiedzialności zgodnie z obowiązującym prawem. W sektorze prywatnym są to zazwyczaj osoby fizyczne lub prawne; w sektorze publicznym są to zazwyczaj organy. Inne podmioty, takie jak ciała lub instytucje nieposiadające osobowości prawnej, mogą być administratorami lub podmiotami przetwarzającymi tylko wówczas, gdy przewidują to specjalne przepisy.

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

W grupach kapitałowych odrębnymi administratorami lub podmiotami przetwarzającymi są spółka dominująca i poszczególne spółki stowarzyszone, gdyż są one odrębnymi podmiotami prawnymi. W związku z tym odrębnym statusem prawnym

dla przekazywania danych między członkami grupy kapitałowej niezbędna jest specjalna podstawa prawna. Nie istnieje zasada umożliwiająca wymianę danych osobowych jako takich między odrębnymi podmiotami prawnymi w obrębie grupy kapitałowej.

W tym kontekście należy wspomnieć o roli osób fizycznych. **W prawie UE** osoby prywatne, gdy przetwarzają dane o innych osobach w trakcie czynności o czysto osobistym lub domowym charakterze, nie podlegają przepisom dyrektywy o ochronie danych i nie są uważane za podmioty przetwarzające[78].

W orzecznictwie ustalił się jednak pogląd, że prawo o ochronie danych znajduje niemniej zastosowanie, gdy osoba prywatna publikuje dane na temat innych osób, korzystając z internetu.

Przykład: W sprawie *Bodil Lindqvist*[79] TSUE uznał, 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"[80].

Takie przetwarzanie danych osobowych nie wchodzi w zakres czynności o czysto osobistym lub domowym charakterze, których nie dotyczą przepisy dyrektywy 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"[81].

78 Dyrektywa o ochronie danych, motyw 12 i art. 3 ust. 2 ostatnie tiret.

79 TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.

80 *Tamże*, pkt 27.

81 *Tamże*, pkt 47.

Administrator

W prawie UE administrator oznacza podmiot, który „samodzielnie lub wspólnie z innymi podmiotami określa cele i sposoby przetwarzania danych”[82]. Administrator decyduje o tym, dlaczego i w jaki sposób będą przetwarzane dane. W definicji administratora **w prawie RE** wspomniano dodatkowo, że administrator decyduje o tym, jakie kategorie danych osobowych będą gromadzone[83].

W definicji administratora zawartej w konwencji nr 108 mowa jest o dodatkowym aspekcie tej roli, który wymaga rozważenia. Definicja ta odnosi się do zagadnienia, kto może zgodnie z prawem przetwarzać pewne dane w określonym celu. Gdy jednak pojawi się zarzut, że czynności przetwarzania odbywają się niezgodnie z prawem, i konieczne będzie ustalenie odpowiedzialnego za to administratora, za administratora uznana zostanie osoba lub podmiot, taki jak przedsiębiorstwo lub organ, który zadecydował o przetwarzaniu danych, niezależnie od tego, czy był uprawniony do tego, czy też nie[84]. W związku z tym wniosek o usunięcie danych należy zawsze kierować do „faktycznego” administratora.

Współadministracja

W definicji „administratora” zawartej w dyrektywie o ochronie danych przewidziano, że może występować kilka odrębnych prawnie podmiotów, które działają razem lub wspólnie z innymi jako administratorzy. Oznacza to, że podejmują one wspólną decyzję o przetwarzaniu danych we wspólnym celu[85]. Jest to jednak możliwe zgodnie z prawem tylko w przypadkach, gdy istnieje specjalna podstawa prawna wspólnego przetwarzania danych we wspólnym celu.

Przykład: Częstym przykładem współadministracji 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.

82 Dyrektywa o ochronie danych, art. 2 lit. d).

83 Konwencja nr 108, art. 2 lit. d).

84 Zob. też Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych” i „przetwarzający”*, WP 169, Bruksela, 16 lutego 2010 r., s. 15.

85 Dyrektywa o ochronie danych, art. 2 lit. d).

W przepisach nie stwierdza się wyraźnie, czy w celu współadministracji 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 oraz nie ma jasności co do konsekwencji dotyczących odpowiedzialności. Grupa Robocza Art. 29 opowiada się za szerszą interpretacją pojęcia współadministracji, co ma zapewnić pewną elastyczność ze względu na rosnącą złożoność obecnych realiów w zakresie przetwarzania danych[86]. Ilustracją dla stanowiska Grupy Roboczej jest sprawa związana ze Stowarzyszeniem Międzynarodowej Teletransmisji Danych Finansowych (SWIFT).

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[87]. Decydując o ujawnieniu danych, SWIFT przyjął – niezgodnie z prawem – rolę administratora; instytucje bankowe w oczywisty sposób nie dopełniły obowiązku sprawowania nadzoru nad podmiotem przetwarzającym, w związku z czym nie można ich całkowicie zwolnić z odpowiedzialności jako administratorów. Taka sytuacja skutkuje współadministracją.

Podmiot przetwarzający

Podmiot przetwarzający jest zdefiniowany **w prawie UE** jako podmiot, który przetwarza dane osobowe w imieniu administratora[88]. Czynności powierzone podmiotowi przetwarzającemu mogą ograniczać się do ściśle określonego zadania lub kontekstu bądź mogą być określone w sposób dość ogólny i szeroki.

86 Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, WP 169, Bruksela, 16 lutego 2010 r., s. 19.

87 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.

88 Dyrektywa o ochronie danych, art. 2 lit. e).

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

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.

Przykłady: 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 czynności przetwarzania danych w związku z wypełnianiem swoich obowiązków jako pracodawcy.

Relacja między administratorem a podmiotem przetwarzającym

Jak widać, administratora definiuje się jako podmiot, który określa cele i środki przetwarzania.

Przykład: Dyrektor spółki Sunshine decyduje, że analizę rynkową danych o jej klientach powinna przeprowadzić spółka Moonlight, która specjalizuje się w analizie rynku. Chociaż zadanie określenia środków przetwarzania zostanie tym samym przekazane spółce Moonlight, spółka Sunshine pozostaje administratorem, a spółka Moonlight zaledwie podmiotem przetwarzającym, gdyż zgodnie z umową Moonlight może wykorzystywać dane spółki Sunshine o klientach wyłącznie do celów określonych przez Sunshine.

W przypadku gdy uprawnienie do określenia środków przetwarzania zostaje przekazane podmiotowi przetwarzającemu, administrator musi niemniej mieć możliwość ingerencji w decyzje podmiotu przetwarzającego dotyczące środków przetwarzania. Ogólna odpowiedzialność nadal spoczywa na administratorze, który musi nadzorować podmioty przetwarzające w celu zapewnienia zgodności ich decyzji z prawem o ochronie danych. Umowa zakazująca administratorowi ingerencji w decyzje podmiotu przetwarzającego byłaby zatem prawdopodobnie interpretowana jako skutkująca współadministracją, w którym to przypadku odpowiedzialność prawna administratora spoczywa na obydwu stronach.

Ponadto jeżeli podmiot przetwarzający nie stosuje się do nałożonych przez administratora ograniczeń dotyczących wykorzystania danych, podmiot przetwarzający stanie się administratorem co najmniej w zakresie, w jakim postępuje niezgodnie z poleceniami 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. W istocie Grupa Robocza Art. 29 zazwyczaj zakłada w takich przypadkach, że doszło do współadministracji, gdyż zapewnia to najlepszą ochronę interesów osób, których dane dotyczą[89]. Ważną konsekwencją współadministracji powinna być solidarna odpowiedzialność za szkody, co udostępnia osobom, których dane dotyczą, większy zakres środków prawnych.

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[90].

Dla zapewnienia jasności i przejrzystości szczegóły relacji łączącej administratora z podmiotem przetwarzającym powinny zostać określone w pisemnej umowie[91]. Brak takiej umowy stanowi naruszenie obowiązku administratora w zakresie dostarczenia pisemnej dokumentacji dotyczącej wzajemnych obowiązków i może skutkować sankcjami[92].

Podmioty przetwarzające mogą chcieć przekazać niektóre zadania 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.

89 Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, WP 169, Bruksela, 16 lutego 2010 r., s. 25; oraz 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.

90 Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, WP 169, Bruksela, 16 lutego 2010 r., s. 26.

91 Dyrektywa o ochronie danych, art. 17 ust. 3 i 4.

92 Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, WP 169, Bruksela, 16 lutego 2010 r., s. 27.

W prawie RE powyższa interpretacja pojęć administratora i podmiotu przetwarzającego ma pełne zastosowanie, czego dowodzą zalecenia opracowane na podstawie konwencji nr 108[93].

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 prawnie od administratora. Dlatego też ujawnienie danych stronie trzeciej zawsze wymaga konkretnej podstawy prawnej. Zgodnie z art. 2 lit. f) dyrektywy o ochronie danych strona trzecia oznacza „osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ niebędący osobą, której dane dotyczą, ani administratorem danych, ani przetwarzającym lub jedną z osób, które pod bezpośrednim zwierzchnictwem administratora danych lub przetwarzającego upoważnione są do przetwarzania danych". Oznacza to, że osoby pracujące w organizacji, która jest podmiotem odrębnym prawnie 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[94].

„Odbiorca" jest pojęciem szerszym od „strony trzeciej". W rozumieniu art. 2 lit. g) dyrektywy o ochronie danych odbiorca oznacza „osobę fizyczną lub prawną, władzę publiczną, agencję lub inny organ, któremu ujawniane są dane, będący lub niebędący osobą 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

93 Zob. na przykład zalecenie w sprawie profilowania, art. 1.

94 Grupa Robocza Art. 29 (2010), *Opinia 1/2010 w sprawie pojęć „administrator danych" i „przetwarzający"*, WP 169, Bruksela, 16 lutego 2010 r., s. 31.

podmiotu przetwarzającego mogą bez żadnych dalszych wymogów prawnych być odbiorcami danych osobowych, jeżeli uczestniczą w czynnościach przetwarzania danych prowadzonych przez administratora lub podmiot przetwarzający. Z kolei strona trzecia, jako odrębna prawnie od administratora lub podmiotu przetwarzającego, nie jest upoważniona do wykorzystywania danych osobowych przetwarzanych przez administratora, chyba że w konkretnym przypadku istnieje stosowna podstawa prawna. Tak więc „strony trzecie będące odbiorcami" danych zawsze potrzebują podstawy prawnej, aby otrzymać dane osobowe zgodnie z prawem.

Przykład: Pracownik podmiotu przetwarzającego, który wykorzystuje dane osobowe przy wykonywaniu zadań powierzonych mu przez pracodawcę, jest odbiorcą danych, ale nie stroną trzecią, gdyż wykorzystuje dane w imieniu podmiotu przetwarzającego i na mocy jego poleceń.

Jeżeli jednak ten sam pracownik zdecyduje się wykorzystać dane, do których może uzyskać dostęp jako pracownik podmiotu przetwarzającego, do własnych celów i sprzeda je innemu przedsiębiorstwu, pracownik ten działa jako strona trzecia. Nie postępuje on już zgodnie z poleceniami podmiotu przetwarzającego (pracodawcy). Jako strona trzecia, pracownik potrzebuje podstawy prawnej, aby uzyskać i sprzedać dane. W tym przykładzie pracownik z pewnością nie posiada takiej podstawy prawnej, więc jego działania są niezgodne z prawem.

2.4. Zgoda

Najważniejsze kwestie

- Zgoda jako podstawa prawna przetwarzania danych osobowych musi być dobrowolna, świadoma i konkretna.
- Zgoda musi zostać udzielona w jednoznaczny sposób. Zgoda może zostać udzielona w sposób wyraźny lub dorozumiany – czyli wyrażona przez działanie w sposób niepozostawiający wątpliwości co do tego, że osoba, której dane dotyczą, wyraża zgodę na ich przetwarzanie.
- Przetwarzanie danych szczególnie chronionych na podstawie zgody wymaga wyraźnej zgody.
- Zgoda może zostać odwołana w każdej chwili.

Zgoda oznacza „konkretne i świadome, dobrowolne wskazanie przez osobę, której dane dotyczą”[95]. W wielu przypadkach stanowi ona podstawę prawną legalnego przetwarzania danych (zob. sekcję 4.1).

2.4.1. Elementy ważnej zgody

W prawie UE wskazano trzy elementy ważnej zgody, które mają zagwarantować, że osoby, których dane dotyczą, rzeczywiście chciały wyrazić zgodę na wykorzystanie ich danych:

- osoba, której dane dotyczą, nie może być poddawana żadnej presji w chwili wyrażania zgody;
- osoba, której dane dotyczą, musi zostać należycie poinformowana o tym, czego dotyczy zgoda, i o konsekwencjach jej udzielenia; oraz
- zakres zgody musi zostać w wystarczającym stopniu skonkretyzowany.

Jedynie spełnienie wszystkich tych wymogów skutkuje ważną zgodą w rozumieniu prawa o ochronie danych.

Konwencja nr 108 nie zawiera definicji zgody, którą pozostawiono do uznania prawa krajowego. **W prawie RE** elementy ważnej zgody odpowiadają jednak wymienionym powyżej, na co wskazują zalecenia opracowane na podstawie konwencji nr 108[96]. Wymogi dotyczące zgody są takie same, jak w przypadku ważnego oświadczenia woli w europejskim prawie cywilnym.

Dodatkowe wymagania na mocy prawa cywilnego warunkujące ważność zgody, takie jak zdolność do czynności prawnych, obowiązują oczywiście także w kontekście ochrony danych, gdyż są to podstawowe wstępne wymagania prawne. Nieważna zgoda wyrażona przez osoby, które nie mają zdolności do czynności prawnych, skutkuje brakiem podstawy prawnej przetwarzania danych na temat takich osób.

95 Dyrektywa o ochronie danych, art. 2 lit. h).

96 Zob. na przykład konwencję nr 108, zalecenie dotyczące danych statystycznych, pkt 6.

Zgoda może zostać udzielona w sposób wyraźny[97] lub dorozumiany. Ta pierwsza nie pozostawia wątpliwości co do zamiarów osoby, której dane dotyczą, i może zostać udzielona w formie ustnej lub pisemnej; o udzieleniu tej drugiej wnioskuje się natomiast na podstawie okoliczności. Zgoda musi w każdym przypadku zostać udzielona w sposób jednoznaczny[98]. Oznacza to, że musi zostać ustalone ponad wszelką wątpliwość, iż osoba, której dane dotyczą, chciała zakomunikować zgodę, aby umożliwić przetwarzanie swoich danych. Nie jest na przykład możliwe wywnioskowanie jednoznacznej zgody z zaniechania działania. W przypadku gdy mają być przetwarzane dane szczególnie chronione, wymagana jest wyraźna i jednoznaczna zgoda.

Dobrowolna zgoda

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”[99].

Przykład: W wielu portach lotniczych pasażerowie muszą poddać się prześwietleniu w specjalnych urządzeniach, aby przejść do strefy, w której oczekuje się na wejście na pokład[100]. Ze względu na fakt, że w chwili prześwietlania dane pasażerów są przetwarzane, przetwarzanie to musi następować zgodnie z jedną z podstaw prawnych określonych w art. 7 dyrektywy o ochronie danych (zob. sekcję 4.1.1). Poddanie się prześwietleniu jest czasem przedstawiane pasażerom jako opcjonalne, co sugeruje, że przetwarzanie może być uzasadnione przez ich zgodę. Pasażerowie mogą jednak się obawiać, że odmowa poddania się prześwietleniu może wzbudzić podejrzenia lub poskutkować dodatkową kontrolą, na przykład kontrolą osobistą. Wielu pasażerów zgadza się na prześwietlenie, gdyż w ten sposób unikają potencjalnych problemów lub opóźnień. Taka zgoda nie jest prawdopodobnie w wystarczającym stopniu dobrowolna.

Dlatego też mocną i uzasadnioną podstawę można znaleźć wyłącznie w akcie prawnym opartym na art. 7 lit. e) dyrektywy o ochronie danych, w którym na pasażerów nakłada się obowiązek współpracy ze względu na nadrzędny interes

97 Dyrektywa o ochronie danych, art. 8 ust. 2.

98 *Tamże, art.* 7 lit. a) i art. 26 ust. 1.

99 Zob. też Grupa Robocza Art. 29 (2011), *Opinia 15/2011 w sprawie definicji zgody*, WP 187, Bruksela, 13 lipca 2011 r., s. 12.

100 Przykład pochodzi z *Tamże*, s. 15.

publiczny. Taki akt prawny może nadal umożliwiać wybór między prześwietleniem a przeszukaniem ręcznym, ale tylko w ramach dodatkowych środków kontroli granicznej niezbędnych w określonych okolicznościach. Takie właśnie zapisy znalazły się w dwóch rozporządzeniach Komisji Europejskiej dotyczących urządzeń do prześwietlania osób z 2011 r.[101].

Zagrożenia dla dobrowolnej zgody mogą również występować w sytuacji podporządkowania, gdy istnieje znaczna nierównowaga ekonomiczna lub inna między starającym się o zgodę administratorem a udzielającą jej osobą, której dane dotyczą[102].

Przykład: Duże przedsiębiorstwo planuje stworzyć spis zawierający nazwiska wszystkich pracowników, ich stanowiska i służbowe dane kontaktowe – wyłącznie w celu usprawnienia komunikacji wewnętrznej firmy. Dyrektor działu kadr proponuje zamieścić w spisie zdjęcia wszystkich pracowników, na przykład po to, 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 oczywiste, że publikacja zdjęcia w spisie nie ma negatywnych konsekwencji sama w sobie, a ponadto należy sądzić, że pracownik nie będzie musiał liczyć się z negatywną reakcją ze strony pracodawcy, jeżeli nie zgodzi się na zamieszczenie zdjęcia w spisie.

Nie oznacza to jednak, że zgoda nigdy nie może być ważna w sytuacji, gdy brak zgody miałby negatywne konsekwencje. Jeżeli na przykład brak zgody na wydanie karty stałego klienta supermarketu skutkuje jedynie nieuzyskaniem rabatów na pewne towary, zgoda pozostaje ważną podstawą prawną przetwarzania danych osobowych tych klientów, którzy wyrazili zgodę na wydanie im takiej karty. Nie

101 Rozporządzenie Komisji (UE) nr 1141/2011 z dnia 10 listopada 2011 r. zmieniające rozporządzenie (WE) nr 272/2009 uzupełniające wspólne podstawowe normy ochrony lotnictwa cywilnego odnośnie do używania urządzeń do prześwietlania osób w portach lotniczych UE, Dz.U. L 293 z 11.11.2011; oraz rozporządzenie wykonawcze Komisji (UE) nr 1147/2011 z dnia 11 listopada 2011 r. zmieniające rozporządzenie (UE) nr 185/2010 ustanawiające szczegółowe środki w celu wprowadzenia w życie wspólnych podstawowych norm ochrony lotnictwa cywilnego odnośnie do używania urządzeń do prześwietlania osób w portach lotniczych UE, Dz.U. L 294 z 12.11.2011.

102 Grupa Robocza Art. 29 (2001), *Opinion 8/2001 on the processing of personal data in the employment context* [„Opinia 8/2001 w sprawie przetwarzania danych osobowych w kontekście zatrudnienia"], WP 48, Bruksela, 13 września 2001 r.; oraz Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*, WP 114, Bruksela, 25 listopada 2005 r.

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.

Z drugiej strony w każdym przypadku, gdy wystarczająco ważne towary lub usługi można uzyskać tylko i wyłącznie pod warunkiem ujawnienia pewnych danych osobowych stronom trzecim, zgody osoby, której dane dotyczą, na ujawnienie jej danych nie można zwykle uznać za decyzję dobrowolną, zatem zgoda taka nie jest ważna na mocy prawa o ochronie danych.

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. To, czy podane informacje są wystarczające, można stwierdzić jedynie w zależności od konkretnego przypadku. Zazwyczaj świadoma zgoda wymaga przedstawienia dokładnego i łatwo zrozumiałego opisu tego, czego dotyczy wymagana zgoda, a dodatkowo wskazania konsekwencji udzielenia lub nieudzielenia zgody. Język, w jakim podawane są informacje, należy dostosować do możliwych do przewidzenia adresatów.

Informacje muszą też być łatwo dostępne dla osób, których dane dotyczą. Ważnymi elementami są dostępność i widoczność informacji. W internecie dobrym rozwiązaniem mogą być warstwowe noty informacyjne, gdyż oprócz skrótowej wersji informacji osoba, której dane dotyczą, może też uzyskać dostęp do wersji bardziej rozbudowanej.

Konkretna zgoda

Aby zgoda była ważna, musi też być konkretna. Ma to ścisły związek z jakością informacji na temat tego, czego dotyczy 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 przetwarzania ma zostać poszerzony lub mają one ulec zmianie w sposób, którego nie można było racjonalnie przewidzieć w chwili udzielania pierwotnej zgody.

Przykład: W sprawie *Deutsche Telekom AG*[103] TSUE zajął się zagadnieniem, czy usługodawca telekomunikacyjny, który musiał przekazać dane osobowe abonentów na mocy art. 12 *dyrektywy o prywatności i łączności elektronicznej*[104], potrzebował ponownej zgody osób, których dane dotyczą, gdyż w chwili udzielania pierwotnej zgody nie podano odbiorców danych.

TSUE orzekł, że na mocy tego artykułu ponowna zgoda przed przekazaniem danych nie była niezbędna, gdyż osoby, których dane dotyczą, miały na mocy tego przepisu jedynie możliwość wyrażenia zgody na cel przetwarzania, którym była publikacja ich danych, nie mogły natomiast wybrać spisów, w których te dane mogą być publikowane.

Jak podkreślił Trybunał: „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”[105]. Ponadto „samo opublikowanie danych osobowych w spisie mającym szczególne przeznaczenie może okazać się dla abonenta niekorzystne”[106], nie zaś to, kto jest autorem danej publikacji.

103 TSUE, C-543/09, *Deutsche Telekom AG przeciwko Niemcom*, 5 maja 2011 r.; zob. w szczególności pkt 53 i 54.

104 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.

105 TSUE, C-543/09, *Deutsche Telekom AG przeciwko Niemcom*, 5 maja 2011 r.; zob. w szczególności pkt 61.

106 *Tamże*, zob. w szczególności pkt 62.

2.4.2. Prawo wycofania zgody w każdej chwili

W dyrektywie o ochronie danych nie zapisano ogólnego prawa do wycofania zgody w każdej chwili. Powszechnie uznaje się jednak, że takie prawo istnieje i że osoba, której dane dotyczą, musi mieć możliwość skorzystania z niego według własnego uznania. Nie powinno być wymagane uzasadnienie wycofania zgody i nie powinno się z nim wiązać ryzyko negatywnych konsekwencji wychodzących poza utratę wszelkich korzyści wynikających z wyrażonej wcześniej zgody na wykorzystanie danych.

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.

Jeżeli klient otrzymywał 5% rabat od ceny noclegu hotelowego w zamian za zgodę na wykorzystanie jego danych do celów wysyłania wiadomości promocyjnych, późniejsze wycofanie zgody na otrzymywanie wiadomości promocyjnych nie powinno skutkować koniecznością zwrotu udzielonych rabatów.

3

Najważniejsze zasady europejskiego prawa o ochronie danych

UE	Omówione zagadnienia	RE
Artykuł 6 ust. 1 lit. a) i b) dyrektywy o ochronie danych TSUE, C-524/06, *Huber przeciwkoBundesrepublik Deutschland*, 16 grudnia 2008 r. TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r.	**Zasada przetwarzania danych zgodnie z prawem**	Artykuł 5 lit. a) i b) konwencji nr 108 ETPC, *Rotaru przeciwko Rumunii* [Wielka Izba], nr 28341/95, 4 maja 2000 r. ETPC, *Taylor-Sabori przeciwko Zjednoczonemu Królestwu*, nr 47114/99, 22 października 2002 r. ETPC, *Peck przeciwko Zjednoczonemu Królestwu*, nr 44647/98, 28 stycznia 2003 r. ETPC, *Khelili przeciwko Szwajcarii*, nr 16188/07, 18 października 2011 r. ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.
Artykuł 6 ust. 1 lit. b) dyrektywy o ochronie danych	**Zasada określenia i organiczenia celu**	Artykuł 5 lit. b) konwencji nr 108
	Zasady jakości danych:	
Artykuł 6 ust. 1 lit. c) dyrektywy o ochronie danych	**Stosowność danych**	Artykuł 5 lit. c) konwencji nr 108
Artykuł 6 ust. 1 lit. d) dyrektywy o ochronie danych	**Prawidłowość danych**	Artykuł 5 lit. d) konwencji nr 108

UE	Omówione zagadnienia	RE
Artykuł 6 ust. 1 lit. e) dyrektywy o ochronie danych	Przechowywanie danych przez określony czas	Artykuł 5 lit. e) konwencji nr 108
Artykuł 6 ust. 1 lit. e) dyrektywy o ochronie danych	Wyłączenie do celów badań naukowych i statystyki	Artykuł 9 ust. 3 konwencji nr 108
Artykuł 6 ust. 1 lit. a) dyrektywy o ochronie danych	Zasada rzetelnego przetwarzania	Artykuł 5 lit. a) konwencji nr 108 ETPC, *Haralambie przeciwko Rumunii*, nr 21737/03, 27 października 2009 r. ETPC, *K.H. i inni przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.
Artykuł 6 ust. 2 dyrektywy o ochronie danych	Zasada rozliczalności	

Zasady określone w art. 5 konwencji nr 108 stanowią istotę europejskiego prawa o ochronie danych. Zamieszczono je także w art. 6 dyrektywy o ochronie danych jako punkt wyjścia dla bardziej szczegółowych przepisów w następnych artykułach dyrektywy. Wszelkie późniejsze ustawodawstwo w zakresie ochrony danych na szczeblu RE lub UE musi być zgodne z tymi zasadami, które trzeba też uwzględniać podczas interpretacji przepisów. Na szczeblu krajowym możliwe są wyłączenia od tych podstawowych zasad i ograniczenia w ich stosowaniu[107]; muszą one zostać zapisane w ustawie, służyć uzasadnionemu celowi i być konieczne w demokratycznym społeczeństwie. Wszystkie trzy warunki muszą zostać spełnione.

3.1. Zasada przetwarzania danych zgodnie z prawem

Najważniejsze kwestie

- Aby zrozumieć zasadę przetwarzania danych zgodnie z prawem, należy odnieść się do warunków, pod jakimi prawo do ochrony danych może zostać zgodnie z prawem

107 Konwencja nr 108, art. 9 ust. 2; dyrektywa o ochronie danych, art. 13.

ograniczone w świetle art. 52 ust. 1 karty praw podstawowych, oraz wymogów związanych z usprawiedliwioną ingerencją na mocy art. 8 ust. 2 EKPC.

- Przetwarzanie danych osobowych jest zatem zgodne z prawem tylko wtedy, gdy:
  - następuje zgodnie z prawem; oraz
  - służy uzasadnionemu celowi, oraz
  - jest niezbędne w demokratycznym społeczeństwie dla realizacji uzasadnionego celu.

W prawie o ochronie danych UE i RE przetwarzanie danych zgodnie z prawem jest pierwszą wskazaną zasadą; wyrażono ją w niemal identyczny sposób w art. 5 konwencji nr 108 oraz w art. 6 dyrektywy o ochronie danych.

W żadnym z tych przepisów nie zdefiniowano pojęcia „przetwarzania danych zgodnie z prawem". Aby zrozumieć ten termin prawny, trzeba odnieść się do zasady uzasadnionej ingerencji na mocy EKPC zgodnie z jej wykładnią w orzecznictwie ETPC oraz do warunków nałożenia ograniczeń zgodnie z prawem na mocy art. 52 karty praw podstawowych.

3.1.1. Wymagania dotyczące usprawiedliwionej ingerencji na mocy EKPC

Przetwarzanie danych osobowych może stanowić ingerencję w prawo do poszanowania życia prywatnego osoby, której dane dotyczą. Prawo do poszanowania życia prywatnego nie jest jednak prawem absolutnym, lecz musi zostać wyważone względem innych uzasadnionych interesów i pogodzone z nimi, przy czym mogą to być interesy innych osób (interesy prywatne) bądź społeczeństwa jako całości (interesy publiczne).

Ingerencja państwa jest usprawiedliwiona pod następującymi warunkami:

Zgodność z prawem

Zgodnie z orzecznictwem ETPC ingerencja jest zgodna z prawem, jeżeli jej podstawą jest przepis prawa krajowego, który ma pewne cechy. Prawo musi być „dostępne

dla zainteresowanych osób, a jego skutki muszą być przewidywalne"[108]. Przepis jest przewidywalny „jeżeli został sformułowany wystarczająco precyzyjnie, aby umożliwić każdej osobie – w razie potrzeby po zasięgnięciu odpowiedniej porady – dostosowanie swojego postępowania"[109]. „Stopień precyzji wymagany od »prawa« w tym kontekście jest zależny od konkretnego zagadnienia"[110].

Przykład: W sprawie *Rotaru przeciwko Rumunii*[111] ETPC stwierdził naruszenie art. 8 EKPC, gdyż prawo rumuńskie zezwalało na gromadzenie, rejestrację i archiwizację w tajnych aktach informacji mających wpływ na bezpieczeństwo narodowe bez ustanowienia 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. Ze względu na te braki Trybunał stwierdził, że prawo krajowe nie jest zgodne z wymogiem przewidywalności na mocy art. 8 EKPC i doszło do naruszenia tego artykułu.

Przykład: W sprawie *Taylor-Sabori przeciwko Zjednoczonemu Królestwu*[112] skarżący był przedmiotem nadzoru ze strony policji. „Sklonowawszy" pager skarżącego, policja była w stanie przechwytywać wysyłane do niego wiadomości. Skarżącego następnie aresztowano i oskarżono o zmowę przestępczą w celu rozpowszechniania narkotyków. 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 wiadomości przekazywanych za pośrednictwem prywatnego systemu telekomunikacyj-

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

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

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

111 ETPC, *Rotaru przeciwko Rumunii* [Wielka Izba], nr 28341/95, 4 kwietnia 2000 r., pkt 57; zob. też ETPC, *Association for European Integration and Human Rightsoraz 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.

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

nego. Ingerencja w prawa skarżącego nie nastąpiła więc „zgodnie z prawem". ETPC stwierdził, że doszło do naruszenia art. 8 EKPC.

Służenie uzasadnionemu celowi

Uzasadnionym celem może być jeden z wymienionych rodzajów interesu publicznego bądź praw i wolności innych osób.

Przykład: W sprawie *Peck przeciwko Zjednoczonemu Królestwu*[113] 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. ETPC 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 stwierdził, że doszło do naruszenia art. 8 EKPC.

Niezbędne w demokratycznym społeczeństwie

ETPC stwierdził, że „pojęcie konieczności implikuje, że ingerencja odpowiada pilnej potrzebie społecznej, a w szczególności, że jest ona proporcjonalna do uzasadnionego celu"[114].

Przykład: W sprawie *Khelili przeciwko Szwajcarii*[115] 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. ETPC 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

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

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

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

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 prwidłowości danych przechowywanych na temat skarżącej, oraz ze względu na powagę ingerencji w prawa skarżącej, Trybunał orzekł, iż wieloletnia obecność wzmianki „prostytutka" w aktach policyjnych nie była konieczna w demokratycznym społeczeństwie. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Leander przeciwko Szwecji*[116] ETPC orzekł, że tajne postępowania sprawdzające 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 zawarte 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 spełnia wymagania art. 8 ust. 2 EKPC. Uwzględniając szeroki zakres uznania, którym dysponowało, pozwane państwo miało prawo uznać, że w przypadku skarżącego interes bezpieczeństwa narodowego przeważa nad interesem indywidualnym. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

3.1.2. 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 korzystania 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 :

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

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

Przykłady: W sprawie *Volker i Markus Schecke*[117] TSUE orzekł, że nakazując publikację danych osobowych wszystkich osób fizycznych będących beneficjentami pomocy z [pewnych funduszy rolnych] bez wprowadzenia rozróżnienia według odpowiednich kryteriów, takich jak okresy, w których otrzymały one tę pomoc, jej częstość czy też rodzaj i wysokość, Rada i Komisja przekroczyły granice, które wyznacza poszanowanie zasady proporcjonalności.

Dlatego też TSUE uznał za konieczne stwierdzenie nieważności niektórych przepisów rozporządzenia Rady (WE) nr 1290/2005 oraz stwierdzenie nieważności rozporządzenia nr 259/2008 w całości[118].

Mimo odmiennych sformułowań warunki przetwarzania danych zgodnie z prawem określone w art. 52 ust. 1 karty praw podstawowych są podobne do wskazanych w art. 8 ust. 2 EKPC. W istocie warunki wymienione w art. 52 ust. 1 karty muszą być zgodne z wskazanymi w art. 8 ust. 2 EKPC, gdyż w pierwszym zdaniu art. 52 ust. 3 karty stwierdza się: „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".

Jednak zgodnie z ostatnim zdaniem art. 52 ust. 3: „[n]iniejsze postanowienie nie stanowi przeszkody, aby prawo Unii przyznawało szerszą ochronę". W kontekście

117 TSUE, Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r., pkt 89 i 86.

118 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.

porównania art. 8 ust. 2 EKPC oraz pierwszego zdania art. 52 ust. 3 karty może to oznaczać jedynie, że warunki usprawiedliwionej ingerencji zgodnie z art. 8 ust. 2 EKPC stanowią minimalne wymagania dla zgodnych z prawem ograniczeń prawa do ochrony danych zgodnie z kartą. W związku z tym przetwarzanie danych osobowych zgodnie z prawem wymaga na mocy prawa UE co najmniej spełnienia warunków określonych w art. 8 ust. 2 EKPC; prawo UE może jednak ustanawiać w konkretnych przypadkach dodatkowe wymogi.

Związek między zasadą przetwarzania danych zgodnie z prawem na mocy prawa UE a stosownymi zapisami EKPC dodatkowo podkreślono w art. 6 ust. 3 TUE, w którym stwierdza się, że „[p]rawa podstawowe, zagwarantowane w europejskiej Konwencji o ochronie praw człowieka i podstawowych wolności [...] stanowią część prawa Unii jako zasady ogólne prawa".

3.2. Zasada określenia i ograniczenia celu

Najważniejsze kwestie

- Cel przetwarzania danych musi zostać jasno określony przed rozpoczęciem przetwarzania.
- Na mocy prawa UE cel przetwarzania musi zostać wyraźnie określony; w prawie RE kwestię tę pozostawiono do rozstrzygnięcia w prawie krajowym.
- Przetwarzanie w nieokreślonych celach nie jest zgodne z prawem o ochronie danych.
- Dalsze wykorzystanie danych w innym celu wymaga dodatkowej podstawy prawnej, jeżeli nowy cel przetwarzania jest niezgodny z pierwotnym.
- Przekazywanie danych stronom trzecim stanowi nowy cel i wymaga dodatkowej podstawy prawnej.

W gruncie rzeczy zasada określenia i usprawiedliwienia celu oznacza, że zgodność przetwarzania danych osobowych z prawem zależy od celu ich przetwarzania[119]. Cel musi zostać określony i ujawniony przez administratora przed rozpoczęciem przetwarzania danych[120]. **Na mocy prawa UE** należy to uczynić, składając deklarację, a więc innymi słowy dokonując zawiadomienia właściwego organu nadzorczego lub

119 Konwencja nr 108, art. 5 lit. b); dyrektywa o ochronie danych, art. 6 ust. 1 lit. b).

120 Zob. też Grupa Robocza Art. 29 (2013), *Opinion 03/2013 on purpose limitation* [„Opinia 3/2013 w sprawie ograniczenia celów"], WP 203, Bruksela, 2 kwietnia 2013 r.

co najmniej sporządzając wewnętrzną dokumentację, która musi zostać udostępniona przez administratora do kontroli przez organy nadzorcze oraz musi być udostępniana osobom, których dane dotyczą.

Przetwarzanie danych osobowych do nieokreślonych i/lub nieograniczonych celów jest niezgodne z prawem.

Każdy nowy cel przetwarzania danych musi posiadać własną konkretną podstawę prawną i nie można powoływać się na fakt, że dane zostały pierwotnie pozyskane bądź były przetwarzane w innym uzasadnionym celu. Przetwarzanie danych zgodnie z prawem ogranicza się do pierwotnie określonego celu, a każdy nowy cel przetwarzania wymaga nowej odrębnej podstawy prawnej. Szczególnie starannie należy rozważyć ujawnienie danych stronom trzecim, gdyż ujawnienie stanowi zazwyczaj nowy cel, a tym samym wymaga podstawy prawnej, odrębnej od wykorzystanej w celu zgromadzenia 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. zapotrzebowania na wózki inwalidzkie; 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, władzom imigracyjnym na lotnisku docelowym, dane te są w takim przypadku wykorzystywane do celów kontroli imigracji, który różni się od pierwotnego celu gromadzenia danych. Przekazanie tych danych organowi imigracyjnemu wymaga zatem nowej, odrębnej podstawy prawnej.

Jeżeli chodzi o zakres i granice danego celu, w konwencji nr 108 oraz dyrektywie o ochronie danych odwołano się do pojęcia zgodności: wykorzystanie danych do zgodnych celów może nastąpić w oparciu o pierwotną podstawę prawną. Nie zdefiniowano jednak, co oznacza termin „zgodny", co pozostawia pole do interpretacji w indywidualnych przypadkach.

Przykład: Sprzedaż danych klientów spółki Sunshine, które uzyskała ona w ramach zarządzania kontaktami z klientami, zajmującej się marketingiem bezpośrednim spółce Moonlight, która chce wykorzystać te dane w kampaniach marketingowych innych firm, jest nowym celem. Cel ten jest niezgodny z zarządzaniem kontaktami z klientami, czyli pierwotnym celem gromadzenia danych

klientów przez spółkę Sunshine. W związku z tym sprzedaż danych spółce Moonlight wymaga osobnej 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 dyrektywie o ochronie danych wyraźnie stwierdza się, że „dalsze przetwarzanie danych w celach historycznych, statystycznych lub naukowych nie jest uważane za niezgodne z przepisami pod warunkiem ustanowienia przez Państwa Członkowskie odpowiednich środków zabezpieczających”[121].

Przykłady: Spółka Sunshine gromadzi i przechowuje dane służące do zarządzania kontaktami z klientami. Dodatkowe wykorzystanie tych danych przez spółkę 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.

Gdyby te same dane miały zostać przekazane stronie trzeciej – spółce Starlight – wyłącznie w celach statystycznych, ich przekazanie byłoby dopuszczalne bez dodatkowej podstawy prawnej, ale jedynie pod warunkiem ustanowienia odpowiednich zabezpieczeń, takich jak zamaskowanie tożsamości osób, których dane dotyczą, gdyż informacje o tożsamości osób nie są zazwyczaj potrzebne do celów statystycznych.

3.3. Zasady jakości danych

Najważniejsze kwestie

- Administrator musi przestrzegać zasad jakości danych podczas wszystkich czynności przetwarzania.

121 Przykładem takich przepisów krajowych jest austriacka ustawa o ochronie danych (Datenschutzgesetz), Federalny Dziennik Ustaw I nr 165/1999, ust. 46, dostępna w języku angielskim na stronie: www.dsk.gv.at/DocView.axd?CobId=41936.

- Zgodnie z zasadą przechowywania danych przez określony czas niezbędne jest usuwanie danych, gdy tylko nie są one już potrzebne do celów, w których zostały zgromadzone.
- Wyjątki od zasady przechowywania danych przez określony czas muszą zostać ustanowione ustawą i niezbędne są wówczas specjalne środki bezpieczeństwa w celu ochrony osób, których dane dotyczą.

3.3.1. Zasada stosowności danych

Przetwarzane mogą być tylko dane „prawidłowe, stosowne oraz nienadmierne ilościowo w stosunku do celów, dla których zostały zgromadzone i/lub dalej przetworzone”[122]. Kategorie danych wybrane w celu przetwarzania muszą być niezbędne do osiągnięcia deklarowanego ogólnego celu czynności przetwarzania, a administrator powinien ściśle ograniczyć gromadzenie danych do tych informacji, które mają bezpośrednie zastosowanie do konkretnego celu przetwarzania.

We współczesnym społeczeństwie występuje dodatkowe zagadnienie związane z zasadą stosowności danych: dzięki wykorzystaniu specjalnych technologii zwiększających prywatność można czasem uniknąć wykorzystywania jakichkolwiek danych osobowych bądź wykorzystać dane spseudonimizowane, co skutkuje rozwiązaniem korzystnym z punktu widzenia prywatności. Jest to 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 układzie scalonym. 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 stosowności danych: sprawdzenia, czy dana osoba jest uprawniona, by korzystać ze środków transportu, można dokonać bez porównywania danych osobowych zapisanych w układzie scalonym karty z bazą danych. Wystarczyłoby na przykład zapisać w układzie scalonym karty specjalny elektroniczny obraz, taki jak np. kod kreskowy, który

122 Konwencja nr 108, art. 5 lit. c); oraz dyrektywa o ochronie danych, art. 6 ust. 1 lit. c).

po odczytaniu przez czytnik potwierdzałby, czy karta jest ważna, czy też nie. Taki system nie rejestrowałby, kto i kiedy używał jakiego środka transportu. Nie byłyby gromadzone żadne dane osobowe, co jest optymalnym rozwiązaniem z punktu widzenia zasady stosowności, gdyż zasada ta skutkuje obowiązkiem ograniczenia gromadzenia danych do minimum.

3.3.2. Zasada prawidłowości danych

Administrator przechowujący dane osobowe nie może korzystać z tych informacji bez podjęcia kroków w celu uzyskania odpowiedniej pewności, że dane są prawidłowe i aktualne.

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

Przykład: Firma sprzedająca meble zgromadziła dane identyfikacyjne i adresowe klienta, aby wystawić mu rachunek. Sześć miesięcy później ta sama firma chce wdrożyć kampanię marketingową i skontaktować się z byłymi klientami. Aby do nich dotrzeć, firma pragnie uzyskać dostęp do spisu meldunkowego, który prawdopodobnie zawiera aktualne adresy, gdyż mieszkańcy mają prawny obowiązek informowania urzędu meldunkowego o aktualnym adresie. Dostęp do danych w spisie mogą uzyskać tylko osoby i podmioty, które potrafią podać uzasadniony powód.

W tej sytuacji argument firmy, że posiadane przez nią dane muszą pozostać prawidłowe i aktualne, nie wystarczy, aby uprawnić ją do uzyskania nowych danych adresowych wszystkich byłych klientów ze spisu meldunkowego. Dane te zostały zgromadzone w celu wystawienia rachunków i do tego celu stosowny jest adres podany w chwili sprzedaży. Nie ma podstawy prawnej gromadzenia nowych danych adresowych, gdyż marketing nie jest interesem nadrzędnym w stosunku do prawa do ochrony danych, a zatem nie może uzasadniać dostępu do danych w spisie.

Mogą też występować przypadki, w których aktualizacja przechowywanych danych jest zabroniona prawem, gdyż głównym celem przechowywania danych jest udokumentowanie pewnych zdarzeń.

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 regularne sprawdzanie prawidłowości danych, w tym ich aktualizacja, jest bezwzględną koniecznością ze względu na potencjalne szkody wyrządzone osobie, której dane dotyczą, jeżeli dane pozostałyby niedokładne.

Przykład: Jeżeli potencjalny klient chce zawrzeć umowę 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 napotkać poważne problemy. W związku z tym administratorzy takich baz danych powinni dokładać szczególnych starań, aby przestrzegać zasady prawidłowości.

Ponadto dane, które nie odnoszą się do faktów, lecz do podejrzeń, np. dochodzeń w sprawach karnych, mogą być gromadzone i przechowywane, dopóki administrator dysponuje podstawą prawną gromadzenia takich informacji oraz posiada wystarczające powody do takich podejrzeń.

3.3.3. Zasada przechowywania danych przez określony czas

W art. 6 ust. 1 lit. e) dyrektywy o ochronie danych oraz w art. 5 lit. e) konwencji nr 108 od państw członkowskich wymaga się, aby dane osobowe były „przechowywane w formie umożliwiającej identyfikację osób, których dane dotyczą, przez czas nie dłuższy niż jest to konieczne do celów, dla których dane zostały zgromadzone lub dla których są dalej przetwarzane". Tak więc dane muszą zostać skasowane po osiągnięciu tych celów.

W sprawie *S. i Marper* ETPC stwierdził, że zgodnie z podstawowymi zasadami zapisanymi w stosownych aktach prawnych Rady Europy oraz z prawem i praktyką pozostałych umawiających się stron wymagany okres zatrzymywania danych

powinien być proporcjonalny w stosunku do celów ich gromadzenia oraz określony w czasie, w szczególności w odniesieniu do policji[123].

Ograniczenie okresu przechowywania danych osobowych ma jednak zastosowanie tylko do danych przechowywanych w postaci umożliwiającej identyfikację osób, których dane dotyczą. W związku z tym dane, które nie są już potrzebne, można zgodnie z prawem przechowywać dzięki anonimizacji lub pseudonimizacji.

W dyrektywie o ochronie danych przechowywanie danych do przyszłych celów naukowych, historycznych lub statystycznych wyraźnie wyłączono z zasady przechowywania danych przez określony czas[124]. Takiemu dalszemu przechowywaniu i wykorzystywaniu danych osobowych muszą jednak towarzyszyć specjalne zabezpieczenia na mocy prawa krajowego.

3.4. Zasada rzetelnego przetwarzania

Najważniejsze kwestie

- Rzetelne przetwarzanie oznacza przejrzystość przetwarzania, zwłaszcza w stosunku do osób, których dane dotyczą.
- Przed przetwarzaniem danych osób, których dane dotyczą, administratorzy muszą zawiadomić te osoby co najmniej o celu przetwarzania oraz o tożsamości i adresie administratora.
- O ile nie jest to wyraźnie dozwolone prawem, nie może dojść do tajnego i ukrytego przetwarzania danych osobowych.
- Osoby, których dane dotyczą, mają prawo dostępu do swoich danych wszędzie tam, gdzie są one przetwarzane.

Zasada rzetelnego przetwarzania dotyczy przede wszystkim relacji między administratorem a osobą, której dane dotyczą.

123 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu*, nr 30562/04 i 30566/04, 4 grudnia 2008 r.; zob. też na przykład ETPC, *M.M. przeciwko Zjednoczonemu Królestwu*, nr 24029/07, 13 listopada 2012 r.

124 Dyrektywa o ochronie danych, art. 6 ust. 1 lit. e).

3.4.1. Przejrzystość

Zasada ta nakłada na administratora obowiązek informowania osób, których dane dotyczą, o tym, jak są wykorzystywane ich dane.

> Przykład: W sprawie *Haralambie przeciwko Rumunii*[125] skarżący domagał się dostępu do akt przechowywanych na jego temat przez tajne służby, ale jego żądanie zostało spełnione dopiero pięć lat później. ETPC powtórzył, że osoby, których dotyczą akta osobowe będące w posiadaniu organów publicznych, mają istotny interes w uzyskaniu dostępu do nich. Władze miały obowiązek zapewnić skuteczną procedurę uzyskiwania dostępu do takich informacji. ETPC uznał, że ani ilość przekazywanych akt, ani uchybienia w systemie archiwalnym nie uzasadniały pięcioletniego opóźnienia w spełnieniu żądania skarżącego dotyczącego dostępu do jego akt. Władze nie udostępniły 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.

Czynności przetwarzania danych należy wyjaśnić osobom, których dane dotyczą, w przystępny sposób gwarantujący zrozumienie, co stanie się z ich danymi. Osoba, której dane dotyczą, ma również prawo uzyskać od administratora informację o tym, czy są przetwarzane jej dane, a jeżeli tak, jakie.

3.4.2. Budowanie zaufania

Administratorzy powinni wykazać osobom, których dane dotyczą, oraz ogółowi społeczeństwa, że będą przetwarzać dane zgodnie z prawem i w przejrzysty sposób. Czynności przetwarzania danych nie mogą być prowadzone w tajemnicy i nie powinny mieć nieprzewidzianych negatywnych skutków. Administratorzy powinni zapewnić informowanie klientów lub obywateli o sposobie wykorzystania ich danych. Ponadto administratorzy powinni w miarę możliwości niezwłocznie podejmować działania zgodne z życzeniami osoby, której dane dotyczą, w szczególności gdy zgoda tej osoby stanowi podstawę prawną przetwarzania danych.

> Przykład: W sprawie *K.H. i inni przeciwko Słowacji*[126] skarżącymi było osiem kobiet pochodzenia romskiego, które znajdowały się podczas ciąży i porodu

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

126 ETPC, *K.H. i inni przeciwko Słowacji*, nr 32881/04, 6 listopada 2009 r.

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. ETPC 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.

W przypadku usług internetowych systemy przetwarzające dane muszą funkcjonować w sposób umożliwiający osobom, których dane dotyczą, zrozumienie, co naprawdę dzieje się z ich danymi.

Rzetelne przetwarzanie oznacza też gotowość administratorów do wyjścia poza obowiązkowe minimalne wymogi prawne dotyczące usług świadczonych osobie, której dane dotyczą, jeżeli wymagają tego uzasadnione interesy tej osoby.

3.5. Zasada rozliczalności

Najważniejsze kwestie

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

- 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.

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 odpowiedzialności w następującym brzmieniu: „administrator danych powinien być odpowiedzialny za stosowanie środków wdrażających [istotne] zasady wskazane powyżej"[127].

Podczas gdy konwencja 108 nie zawiera odniesień do rozliczalności administratorów, pozostawiając w zasadzie tę kwestię do uregulowania w prawie krajowym, w art. 6 ust. 2 dyrektywy o ochronie danych stwierdza się, że administrator danych powinien zapewnić przestrzeganie zasad odnoszących się do jakości danych określonych w ust. 1.

Przykład: Przykładem położenia nacisku na zasadę rozliczalności w ustawodawstwie jest dokonana w 2009 r. zmiana[128] dyrektywy o prywatności i łączności elektronicznej 2002/58/WE. Zgodnie z art. 4 w zmienionym brzmieniu dyrektywa nakłada obowiązek wdrożenia polityki bezpieczeństwa: „zapewnić wdrożenie polityki bezpieczeństwa w odniesieniu do przetwarzania danych osobowych". Tak więc w odniesieniu do przepisów bezpieczeństwa zawartych w tej dyrektywie ustawodawca zdecydował, że konieczne jest wprowadzenie wyraźnego wymogu posiadania i wdrożenia polityki bezpieczeństwa.

Zgodnie z opinią Grupy Roboczej Art. 29[129] istotą rozliczalności jest obowiązek administratora:

127 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data* [„Wytyczne w zakresie ochrony prywatności i przepływu danych osobowych przez granice"], art. 14.

128 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, s. 11.

129 Grupa Robocza Art. 29, *Opinia 3/2010 w sprawie zasady rozliczalności*, WP 173, Bruksela, 13 lipca 2010 r.

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

- 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.

4

Przepisy europejskiego prawa o ochronie danych

UE	Omówione zagadnienia	RE
Przepisy dotyczące przetwarzania danych innych niż szczególnie chronione zgodnie z prawem		
Artykuł 7 lit. a) dyrektywy o ochronie danych	Zgoda	Artykuł 3 ust. 4 lit. b) i art. 3 ust. 6 zalecenia w sprawie profilowania
Artykuł 7 lit. b) dyrektywy o ochronie danych	Stosunek (przed) umowny	Artykuł 3 ust. 4 lit. b) zalecenia w sprawie profilowania
Artykuł 7 lit. c) dyrektywy o ochronie danych	Obowiązki prawne administratora	Artykuł 3 ust. 4 lit. a) zalecenia w sprawie profilowania
Artykuł 7 lit. d) dyrektywy o ochronie danych	Żywotne interesy osoby, której dane dotyczą	Artykuł 3 ust. 4 lit. b) zalecenia w sprawie profilowania
Artykuł 7 lit. e) i art. 8 ust. 4 dyrektywy o ochronie danych TSUE, C-524/06, *Huber przeciwkoBundesrepublik Deutschland*, 16 grudnia 2008 r.	Interes publiczny i wykonywanie władzy publicznej	Artykuł 3 ust. 4 lit. b) zalecenia w sprawie profilowania
Artykuł 7 lit. f), art. 8 ust. 2 i art. 8 ust. 3 dyrektywy o ochronie danych 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.	Uzasadnione interesy innych osób	Artykuł 3 ust. 4 lit. b) zalecenia w sprawie profilowania

UE	Omówione zagadnienia	RE
Przepisy dotyczące przetwarzania danych szczególnie chronionych zgodnie z prawem		
Artykuł 8 ust. 1 dyrektywy o ochronie danych	Ogólny zakaz przetwarzania	Artykuł 6 konwencji nr 108
Artykuł 8 ust. 2–4 dyrektywy o ochronie danych	Wyłączenia z ogólnego zakazu	Artykuł 6 konwencji nr 108
Artykuł 8 ust. 5 dyrektywy o ochronie danych	Przetwarzanie danych na temat wyroków skazujących	Artykuł 6 konwencji nr 108
Artykuł 8 ust. 7 dyrektywy o ochronie danych	Przetwarzanie numerów identyfikacyjnych	
Przepisy dotyczące bezpiecznego przetwarzania		
Artykuł 17 dyrektywy o ochronie danych	Obowiązek zapewnienia bezpiecznego przetwarzania	Artykuł 7 konwencji nr 108 ETPC, *I. przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.
Artykuł 4 ust. 2 dyrektywy o prywatności i łączności elektronicznej	Zawiadomienia o naruszeniu danych	
Artykuł 16 dyrektywy o ochronie danych	Obowiązek zachowania poufności	
Przepisy dotyczące przejrzystości przetwarzania		
	Ogólna przejrzystość	Artykuł 8 lit. a) konwencji nr 108
Artykuły 10 i 11 dyrektywy o ochronie danych	Informacje	Artykuł 8 lit. a) konwencji nr 108
Artykuły 10 i 11 dyrektywy o ochronie danych	Zwolnienia z obowiązku informowania	Artykuł 9 konwencji nr 108
Artykuły 18 i 19 dyrektywy o ochronie danych	Zawiadomienie	Artykuł 9 ust. 2 lit. a) zalecenia w sprawie profilowania
Przepisy dotyczące promowania przestrzegania przepisów		
Artykuł 20 dyrektywy o ochronie danych	Kontrola wstępna	
Artykuł 18 ust. 2 dyrektywy o ochronie danych	Urzędnicy do spraw ochrony danych osobowych	Artykuł 8 ust. 3 zalecenia w sprawie profilowania
Artykuł 27 dyrektywy o ochronie danych	Kodeksy postępowania	

Zasady mają z konieczności charakter ogólny, a ich zastosowanie w konkretnych sytuacjach pozostawia pewien margines dla interpretacji i wyboru użytych środków. Na mocy **prawa RE** strony konwencji nr 108 powinny dokonać ich wykładni 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 dyrektywie o ochronie danych ustanowiono, na mocy zasad określonych w art. 6, szczegółowe przepisy, które muszą zostać wiernie wdrożone w prawie krajowym. Poniższe uwagi na temat szczegółowych przepisów dotyczących ochrony danych na szczeblu europejskim dotyczą zatem przede wszystkim prawa UE.

4.1. Przepisy dotyczące przetwarzania danych zgodnie z prawem

Najważniejsze kwestie

- Dane osobowe mogą być przetwarzane zgodnie z prawem, jeżeli:
  - przetwarzanie następuje na podstawie zgody osoby, której dane dotyczą; lub
  - przetwarzania danych wymagają żywotne interesy osób, których dane dotyczą; lub
  - przyczyną przetwarzania danych są uzasadnione interesy innych osób, jednak tylko jeżeli interes związany z ochroną praw podstawowych osób, których dane dotyczą, nie jest nadrzędny.
- Przetwarzanie szczególnie chronionych danych osobowych zgodnie z prawem podlega specjalnym, ściślejszym zasadom.

W dyrektywie o ochronie danych zawarto dwa różne zestawy przepisów dotyczących przetwarzania danych zgodnie z prawem: jeden dotyczy danych innych niż szczególnie chronione (art. 7), drugi zaś danych szczególnie chronionych (art. 8).

4.1.1. Przetwarzanie danych innych niż szczególnie chronione zgodnie z prawem

W rozdziale II dyrektywy 95/46/WE, zatytułowanym „Ogólne zasady legalności przetwarzania danych osobowych", stwierdza się, że z zastrzeżeniem wyjątków dozwolonych na mocy art. 13 wszystkie czynności przetwarzania danych osobowych muszą być zgodne, po pierwsze, z zasadami dotyczącymi jakości danych określonymi w art. 6 dyrektywy o ochronie danych, a po drugie, z jednym z kryteriów legalności przetwarzania danych wymienionych w art. 7[130]. W ten sposób wyjaśnia się, w jakich przypadkach przetwarzanie danych osobowych innych niż szczególnie chronione jest zgodne z prawem.

Zgoda

W prawie RE zgody nie wymieniono w art. 8 EKPC ani w konwencji nr 108. Wspomniano o niej jednak w orzecznictwie ETPC i w kilku zaleceniach RE. **W prawie UE** zgoda jako podstawa zgodnego z prawem przetwarzania danych jest dobrze ugruntowana na mocy art. 7 lit. a) dyrektywy o ochronie danych, wprost odniesiono się do niej także w art. 8 karty praw podstawowych.

Stosunek umowny

Kolejną podstawą zgodnego z prawem przetwarzania danych osobowych **w prawie UE**, wymienioną w art. 7 lit. b) dyrektywy o ochronie danych, jest przypadek, gdy jest ono „konieczne dla realizacji umowy, której stroną jest osoba, której dane dotyczą". Przepis ten obejmuje także stosunki przedumowne. Może tu chodzić o sytuację, w której 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 przetwarzanie jest zgodne z prawem, jeżeli ma na celu podjęcie „działań na życzenie osoby, której dane dotyczą, przed zawarciem umowy".

W **prawie RE** w art. 8 ust. 2 EKPC jest mowa o „ochronie praw i wolności osób" jako przyczynie uzasadnionej ingerencji w prawo do ochrony danych.

130 TSUE, Sprawy połączone C-465/00, C-138/01 i C-139/01, *Rechnungshof przeciwko Österreichischer Rundfunk i innym oraz Neukomm i Lauermann przeciwko Österreichischer Rundfunk*, 20 maja 2003 r., pkt 65; TSUE, C-524/06, *Huber przeciwko Bundesrepublik Deutschland*, 16 grudnia 2008 r., pkt 48; 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 26.

Obowiązki prawne administratora

W **prawie UE** wyraźnie wymienia się też kolejne kryterium przetwarzania danych zgodnie z prawem, a mianowicie jeżeli jest ono „konieczne dla wykonania zobowiązania prawnego, któremu administrator danych podlega" (art. 7 lit. c) dyrektywy o ochronie danych). Przepis ten odnosi się do administratorów z sektora prywatnego; obowiązki prawne administratorów danych z sektora publicznego określono w art. 7 lit. e) dyrektywy. Istnieje wiele przypadków, w których administratorzy z sektora prywatnego mają obowiązek prawny przetwarzania danych na temat innych osób, np. lekarze i szpitale mają obowiązek przechowywania przez kilka lat danych o leczeniu pacjentów, pracodawcy muszą przetwarzać dane o swoich pracownikach do celów ubezpieczeń społecznych i podatkowych, a przedsiębiorstwa muszą przetwarzać dane swoich klientów do celów podatkowych.

W kontekście obowiązkowego przekazywania danych pasażerów zagranicznym organom imigracyjnym przez linie lotnicze pojawiło się pytanie, czy zobowiązania prawne na mocy prawa *zagranicznego* mogą stanowić uzasadnioną podstawę przetwarzania danych na mocy prawa UE (kwestię tę omówiono bardziej szczegółowo w sekcji 6.2).

Zobowiązania prawne administratora stanowią podstawę przetwarzania danych zgodnie z prawem także **w prawie RE**. Jak wspomniano już wcześniej, zobowiązania prawne administratora z sektora prywatnego są tylko jednym konkretnym przypadkiem uzasadnionych interesów innych osób, o których mowa jest w art. 8 ust. 2 EKPC. W związku z tym powyższy przykład ma także zastosowanie do prawa RE.

Żywotne interesy osoby, której dane dotyczą

W prawie UE, w art. 7 lit. d) **dyrektywy o ochronie danych** stwierdza się, że przetwarzanie danych osobowych jest zgodne z prawem, jeżeli „jest konieczne dla ochrony żywotnych interesów osób, których dane dotyczą". Takie interesy, które są ściśle związane z przeżyciem osoby, której dane dotyczą, mogą być na przykład podstawą zgodnego z prawem wykorzystania danych dotyczących zdrowia lub danych na temat osób zaginionych.

W prawie RE, w art. 8 EKPC nie wspomina się o żywotnych interesach osoby, której dane dotyczą, jako przyczynie uzasadnionej ingerencji w prawo do ochrony danych. W niektórych zaleceniach RE uzupełniających konwencję nr 108 w poszczególnych dziedzinach wspomina się jednak wprost o żywotnych interesach osoby, której dane

dotyczą, jako podstawie przetwarzania danych zgodnie z prawem[131]. Żywotne interesy osoby, której dane dotyczą, najwyraźniej uznaje się za dorozumiane w wykazie przyczyn uzasadniających przetwarzanie danych: ochrona praw podstawowych nie powinna w żadnym przypadku zagrażać żywotnym interesom chronionej osoby.

Interes publiczny i wykonywanie władzy publicznej

Ze względu na wiele możliwych sposobów zorganizowania spraw publicznych w art. 7 lit. e) **dyrektywy o ochronie danych** stwierdza się, że dane osobowe mogą być przetwarzane zgodnie z prawem, jeżeli jest to „konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania władzy publicznej przekazanej administratorowi danych lub osobie trzeciej, przed którą ujawnia się dane [...]"[132].

Przykład: W sprawie *Huber przeciwko Niemcom*[133] 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 krajowy 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.

TSUE stwierdza po pierwsze, że na mocy art. 7 lit. e) dyrektywy o ochronie danych dane osobowe mogą być przetwarzane zgodnie z prawem tylko, jeżeli jest to konieczne dla realizacji zadania wykonywanego w interesie publicznym lub dla wykonywania 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 [...] nie może mieć różnego

131 Zalecenie w sprawie profilowania, art. 3 ust. 4 lit. b).

132 Zob. też dyrektywę o ochronie danych, motyw 32.

133 TSUE, C-524/06, *Huber przeciwko Niemcom*, 16 grudnia 2008 r.

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"[134].

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 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 stwierdza, 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) dyrektywy 95/46/WE[135].

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"[136].

134 *Tamże*, pkt 52.

135 *Tamże*, pkt 54, 58, 59, 66–68.

136 *Tamże*, pkt 78 i 81.

Korzystanie z danych osobowych przez organy publiczne podlega także art. 8 **EKPC**.

Uzasadnione interesy administratora lub strony trzeciej

Uzasadnione interesy ma nie tylko osoba, której dane dotyczą. W art. 7 lit. f) **dyrektywy o ochronie danych** stwierdza się, że dane osobowe mogą być przetwarzane zgodnie z prawem, jeżeli jest to „konieczne dla potrzeb wynikających z uzasadnionych interesów administratora danych lub osoby trzeciej, lub osobom, którym dane są ujawniane, z wyjątkiem sytuacji, kiedy interesy takie podporządkowane są interesom związanym z podstawowymi prawami i wolnościami osoby, której dane dotyczą, które gwarantują ochronę […]".

Poniższy wyrok TSUE dotyczył bezpośrednio art. 7 lit. f) dyrektywy:

Przykład: W sprawie *ASNEF i FECEMD*[137] TSUE wyjaśnił, że w prawie krajowym nie można zapisać dodatkowych warunków przetwarzania danych zgodnie z prawem oprócz wymienionych w art. 7 lit. f) dyrektywy. Wyrok dotyczył przepisu w hiszpańskim prawie o ochronie danych, na mocy którego inne podmioty prywatne mogły twierdzić, że mają uzasadniony interes w przetwarzaniu danych osobowych tylko wówczas, gdy dana informacja pojawiła się wcześniej w źródłach publicznych.

Trybunał zauważył, po pierwsze, że celem dyrektywy 95/46/WE 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[138]. W związku z tym TSUE stwierdził, że „z celu polegającego na zapewnieniu równoważnego poziomu ochrony we wszystkich państwach członkowskich wynika, że art. 7 dyrektywy95/46 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

137 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.

138 *Tamże*, pkt 28. Zob. dyrektywę o ochronie danych, motywy 8 i 10.

w art. 7 dyrektywy 95/46 ani też ustanawiać dodatkowych wymogów, które doprowadziłyby do modyfikacji zakresu jednego z sześciu kryteriów przewidzianych we wspomnianym artykule”[139].Trybunał przyznał, że „co się tyczy ważenia niezbędnego na mocy art. 7 lit. f) dyrektywy 95/46, możliwe jest uwzględnienie faktu, że powaga naruszenia praw podstawowych osoby, której przetwarzanie dotyczy, 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”.

W świetle tych rozważań Trybunał stwierdził, że „art. 7 lit. f) dyrektywy 95/46 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”[140].

Podobne sformułowania można znaleźć 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”[141].

139 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 30 i 32.

140 *Tamże*, pkt 40, 44, 48 i 49.

141 Zalecenie w sprawie profilowania, art. 3 ust. 4 lit. b).

4.1.2. 4.1.2 Przetwarzanie danych szczególnie chronionych zgodnie z prawem

Podczas gdy **w prawie RE** określenie odpowiednich zabezpieczeń dotyczących wykorzystania danych szczególnie chronionych pozostawia się przepisom prawa krajowego, **w prawie UE** w art. 8 dyrektywy o ochronie danych określono szczegółowe zasady przetwarzania kategorii danych, które ujawniają pochodzenie rasowe lub etniczne, opinie polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych lub informacje dotyczące zdrowia i życia seksualnego. Przetwarzanie danych szczególnie chronionych jest co do zasady zabronione[142]. Stworzono jednak wyczerpujący wykaz wyłączeń od tego zakazu, który znajduje się w art. 8 ust. 2 i 3 dyrektywy. Wśród wyłączeń znalazły się wyraźna zgoda osoby, której dane dotyczą, żywotne interesy osoby, której dane dotyczą, uzasadnione interesy innych osób i interes publiczny.

W przeciwieństwie do przypadku przetwarzania danych innych niż szczególnie chronione, stosunek umowny z osobą, której dane dotyczą, nie jest uważany za ogólną podstawę przetwarzania danych szczególnie chronionych zgodnie z prawem. Dlatego też jeżeli dane szczególnie chronione mają być przetwarzane w związku z umową z osobą, której dane dotyczą, wykorzystanie tych danych wymaga – oprócz zgody na zawarcie umowy – odrębnej wyraźnej zgody osoby, której dane dotyczą. Wyraźne życzenie osoby, której dane dotyczą, odnoszące się do towarów lub usług, które nieodłącznie wiążą się z ujawnieniem danych szczególnie chronionych, powinno wszakże być uważane za równoznaczne z wyraźną zgodą.

Przykład: Jeżeli pasażer linii lotniczych podczas rezerwacji lotu żąda, aby linie lotnicze zapewniły mu wózek inwalidzki i koszerny posiłek, linia lotnicza może wykorzystać te dane, nawet jeżeli pasażer nie podpisał dodatkowej klauzuli zgody stwierdzającej, że zgadza się na wykorzystanie danych ujawniających informacje dotyczące jego zdrowia i przekonań religijnych.

Wyraźna zgoda osoby, której dane dotyczą

Pierwszym warunkiem przetwarzania jakichkolwiek danych zgodnie z prawem, niezależnie od tego, czy są to dane szczególnie chronione, czy też nie, jest zgoda osoby, której dane dotyczą. W przypadku danych szczególnie chronionych zgoda taka musi być wyraźna. W prawie krajowym można jednak zawrzeć zapis, że zgoda na wykorzystanie danych szczególnie chronionych nie jest wystarczającą podstawą prawną

142 Dyrektywa o ochronie danych, art. 8 ust. 1.

umożliwiającą ich przetwarzanie[143], na przykład w wyjątkowych przypadkach, gdy przetwarzanie wiąże się ze szczególnym ryzykiem dla osoby, której dane dotyczą.

W jednym szczególnym przypadku za podstawę prawną przetwarzania danych szczególnie chronionych uznawana jest nawet zgoda dorozumiana: W art. 8 ust. 2 lit. e) dyrektywy stwierdza się, że przetwarzanie nie jest zabronione, jeżeli dotyczy danych, które są podawane do wiadomości publicznej przez osobę, której dane dotyczą. W przepisie tym wyraźnie zakłada się, że działanie osoby, której dane dotyczą, skutkujące podaniem tych danych do wiadomości publicznej musi być interpretowane jako oznaczające zgodę osoby, której dane dotyczą, na wykorzystanie tych danych.

Żywotne interesy osoby, której dane dotyczą

Podobnie jak w przypadku danych innych niż szczególnie chronione, dane szczególnie chronione mogą być przetwarzane ze względu na żywotne interesy osoby, której dane dotyczą[144].

Aby przetwarzanie danych szczególnie chronionych na tej podstawie było zgodne z prawem, niezbędne jest, aby zadanie pytania o decyzję osobie, 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.

Uzasadnione interesy innych osób

Podobnie jak w przypadku danych innych niż szczególnie chronione, podstawą przetwarzania danych szczególnie chronionych mogą być uzasadnione interesy innych osób. W przypadku danych szczególnie chronionych oraz zgodnie z art. 8 ust. 2 dyrektywy o ochronie danych dotyczy to jednak tylko następujących przypadków:

- gdy przetwarzanie danych jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby[145], w przypadku gdy osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do udzielenia zgody;

- gdy dane szczególnie chronione są istotne z punktu widzenia prawa pracy, jak na przykład dane dotyczące zdrowia, np. w kontekście szczególnie

143 *Tamże*, art. 8 ust. 2 lit. a).

144 *Tamże*, art. 8 ust. 2 lit. c).

145 *Tamże*.

niebezpiecznego miejsca pracy, bądź dane na temat przekonań religijnych, np. w kontekście świąt[146];

- gdy fundacje, stowarzyszenia lub inne podmioty niekomercyjne dążące do celów politycznych, filozoficznych, religijnych lub związkowych przetwarzają dane swoich członków i sponsorów bądź innych zainteresowanych stron (takie dane są szczególnie chronione, gdyż mogą ujawniać przekonania religijne lub polityczne danych osób)[147];

- gdy dane szczególnie chronione są wykorzystywane w kontekście postępowania przed sądem lub organem administracyjnym w celu ustalenia, wykonania lub ochrony roszczeń prawnych[148].

- Ponadto, zgodnie z art. 8 ust. 3 dyrektywy o ochronie danych, w przypadku gdy dane dotyczące stanu zdrowia są wykorzystywane do celów badań lekarskich i leczenia przez podmioty świadczące opiekę zdrowotną, zarządzanie tymi usługami jest objęte wyłączeniem. Specjalnym zabezpieczeniem jest fakt, że osoby są uznawane za „podmioty świadczące opiekę zdrowotną" tylko wtedy, jeżeli podlegają obowiązkowi zachowania poufności w związku z wykonywanym zawodem.

Interes publiczny

Dodatkowo zgodnie z art. 8 ust. 4 dyrektywy o ochronie danych państwa członkowskie mogą wprowadzić dalsze cele, w których mogą być przetwarzane dane szczególnie chronione, o ile:

- przetwarzanie danych następuje ze względu na istotny interes publiczny; oraz

- jest przewidziane na mocy ustawy krajowej lub decyzji organu nadzorczego; oraz

- ustawa krajowa lub decyzja organu nadzorczego zawiera niezbędne środki zabezpieczające w celu skutecznej ochrony interesów osób, których dane dotyczą[149].

146 *Tamże, art.* 8 ust. 2 lit. b).

147 *Tamże, art.* 8 ust. 2 lit. d).

148 *Tamże,* art. 8 ust. 2 lit. e).

149 *Tamże, art.* 8 ust. 4.

Ważnym przykładem są elektroniczne kartoteki zdrowotne, które mają zostać ustanowione w wielu państwach członkowskich. 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 na podstawie art. 8 ust. 3 dyrektywy o ochronie danych. Przy założeniu, że funkcjonowanie takich elektronicznych kartotek zdrowotnych stanowi istotny interes publiczny, można je jednak oprzeć na art. 8 ust. 4 dyrektywy, co będzie wymagać dla ich ustanowienia wyraźnej podstawy prawnej, a także niezbędnych zabezpieczeń w celu zapewnienia bezpiecznego działania systemu[150].

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:
  - zabezpieczeń dostępnych na rynku w odniesieniu do konkretnego rodzaju przetwarzania; oraz
  - kosztów; oraz
  - wrażliwości przetwarzanych danych.
- Kolejnym mechanizmem służącym bezpiecznemu przetwarzaniu danych jest ogólny obowiązek zapewnienia poufności danych przez wszystkie osoby – administratorów i podmioty przetwarzające.

150 Grupa Robocza Art. 29 (2007), *Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR)*, WP 131, Bruksela, 15 lutego 2007 r.

Obowiązek wdrożenia odpowiednich środków w celu zapewnienia bezpieczeństwa danych przez administratorów i podmioty przetwarzające zapisano zatem zarówno **w prawie RE o ochronie danych**, jak i **w prawie UE o ochronie danych**.

4.2.1. Elementy bezpieczeństwa danych

Zgodnie z odpowiednimi przepisami **prawa UE**:

> *„Państwa Członkowskie zapewniają, aby administrator danych wprowadził odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych przed przypadkowym lub nielegalnym zniszczeniem lub przypadkową utratą, zmianą, niedozwolonym ujawnieniem lub dostępem, szczególnie wówczas gdy przetwarzanie danych obejmuje transmisję danych w sieci, jak również przed wszelkimi innymi nielegalnymi formami przetwarzania"*[151].

Podobny przepis istnieje **w prawie RE**:

> *„Należy podjąć odpowiednie środki bezpieczeństwa w odniesieniu do danych osobowych zgromadzonych w zbiorach zautomatyzowanych, aby zapobiec przypadkowemu zniszczeniu lub zniszczeniu bez zezwolenia albo przypadkowemu zagubieniu, jak również aby zapobiec niepowołanemu dostępowi do danych oraz ich zmienianiu lub rozpowszechnianiu bez upoważnienia"*[152].

Często istnieją też normy przemysłowe, krajowe i międzynarodowe opracowane, aby zapewnić bezpieczne przetwarzanie danych. Na przykład europejski certyfikat ochrony prywatności (EuroPriSe) 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. Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji 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[153].

151 Dyrektywa o ochronie danych, art. 17 ust. 1.

152 Konwencja nr 108, art. 7.

153 Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji, Dz.U. L 77 z 13.3.2004.

Agencja regularnie publikuje analizy aktualnych zagrożeń i zalecenia dotyczące radzenia sobie z nimi.

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;
- 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;
- 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 urzędników do spraw ochrony danych osobowych, edukację pracowników pod kątem bezpieczeństwa, regularne audyty, testy penetracyjne i znaki jakości.

Przykład: W sprawie *I. przeciwko Finlandii*[154] 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.

Zawiadomienia o naruszeniu danych

W prawie o ochronie danych kilku krajów europejskich wprowadzono nowe narzędzie wykorzystywane w przypadku naruszenia bezpieczeństwa danych: zobowiązanie dostawców usług łączności elektronicznej do zawiadamiania prawdopodobnych pokrzywdzonych i organów nadzorczych o naruszeniach danych. Na mocy prawa UE jest to obowiązek operatorów telekomunikacyjnych[155]. Celem zawiadamiania osób, których dane dotyczą, o naruszeniu danych, jest zapobieganie szkodom: zawiadomienie o naruszeniu danych i jego możliwych konsekwencjach minimalizuje ryzyko negatywnych skutków dla takich osób. W przypadku poważnych zaniedbań usługodawcom mogą też grozić grzywny.

154 ETPC, *I. przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.

155 Zob. dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (*dyrektywę o prywatności i łączności elektronicznej*), Dz.U. L 201 z 31.7.2002, art. 4 ust. 3 w brzmieniu zmienionym dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE 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.

Niezbędne będzie ustanowienie z wyprzedzeniem wewnętrznych procedur mających na celu skuteczne zarządzanie naruszeniami bezpieczeństwa oraz ich zgłaszanie, gdyż termin obowiązkowego zawiadomienia osób, których dane dotyczą, lub organu nadzorczego zgodnie z prawem krajowym jest zazwyczaj dość krótki.

4.2.2. Poufność

W prawie UE kolejnym mechanizmem służącym bezpiecznemu przetwarzaniu danych jest ogólny obowiązek zapewnienia poufności danych przez wszystkie osoby – administratorów i podmioty przetwarzające.

Przykład: Pracownik zakładu ubezpieczeniowego 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.

W art. 16 dyrektywy o ochronie danych poufność jest rozważana tylko w kontekście relacji między administratorem a podmiotem przetwarzającym. Przepisy dotyczące obowiązku zachowania poufności danych przez administratorów (nieujawniania ich stronom trzecim) znajdują się w art. 7 i 8 dyrektywy.

Obowiązek zachowania poufności nie dotyczy sytuacji, gdy osoba poznaje dane jako osoba prywatna, nie zaś jako pracownik administratora lub podmiotu przetwarzającego. W tym przypadku art. 16 dyrektywy o ochronie danych nie znajduje zastosowania, gdyż wykorzystanie danych osobowych przez osoby prywatne jest całkowicie wyłączone z zakresu stosowania dyrektywy, jeżeli mieści się ono w granicach tzw. zwolnienia dotyczącego danych o charakterze domowym[156]. Zwolnienie dotyczące danych o charakterze domowym odnosi się do wykorzystania danych osobowych „przez osobę fizyczną w trakcie czynności o czysto osobistym lub domowym charakterze”[157]. Od czasu orzeczenia TSUE w sprawie *Bodil Lindqvist*[158] wyjątek ten trzeba jednak interpretować wąsko, zwłaszcza w odniesieniu do ujawniania danych.

156 Dyrektywa o ochronie danych, art. 3 ust. 2 tiret drugie.

157 Tamże.

158 TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.

W szczególności zwolnienie dotyczące danych o charakterze domowym nie obejmuje publikacji danych osobowych do użytku nieograniczonej liczby odbiorców w internecie (więcej szczegółów dotyczących sprawy – zob. sekcje 2.1.2, 2.2, 2.3.1 i 6.1).

W prawie RE zobowiązanie do zachowania poufności wynika z pojęcia bezpieczeństwa danych, o którym mowa jest w art. 7 konwencji nr 108 dotyczącym bezpieczeństwa danych.

W przypadku podmiotów przetwarzających poufność oznacza, że mogą one korzystać z danych osobowych powierzonych przez administratora tylko zgodnie z poleceniami administratora. W przypadku pracowników administratora lub podmiotu przetwarzającego zachowanie poufności wymaga wykorzystywania danych osobowych wyłącznie zgodnie z poleceniami właściwych przełożonych.

Zobowiązanie do zachowania poufności musi być zapisane 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 karnemu w wielu państwach członkowskich UE i państwach-stronach konwencji nr 108.

4.3. Przepisy dotyczące przejrzystości przetwarzania

Najważniejsze kwestie

- Przed przystąpieniem do przetwarzania danych osobowych administrator musi co najmniej poinformować osoby, których dane dotyczą, o tożsamości administratora i celu przetwarzania danych, chyba że osoba, której dane dotyczą, już posiada te informacje.
- W przypadku gdy dane są pozyskiwane od stron trzecich, obowiązek dostarczenia informacji nie ma zastosowania, jeżeli:
  - przetwarzanie danych przewidziano ustawą; lub

  - przekazanie informacji jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.
- Przed przystąpieniem do przetwarzania danych osobowych administrator musi dodatkowo:
  - zawiadomić organ nadzorczy o zamierzonych czynnościach przetwarzania; lub
  - zapewnić udokumentowanie przetwarzania w obrębie jego organizacji przez niezależnego urzędnika do spraw ochrony danych osobowych, jeżeli prawo krajowe przewiduje takie postępowanie.

Zasada rzetelnego przetwarzania wymaga przejrzystości przetwarzania. W związku z tym na mocy **prawa RE** każda osoba musi mieć możliwość ustalenia, czy są przetwarzane dane o niej, sprawdzić cel przetwarzania oraz tożsamość odpowiedzialnego za nie administratora[159]. Sposób osiągnięcia tych celów pozostawiono do rozstrzygnięcia w prawie krajowym. **Prawo UE** jest bardziej szczegółowe, gwarantując przejrzystość osobie, której dane dotyczą, przez nałożenie na administratora obowiązku informowania osoby, której dane dotyczą; ogółowi społeczeństwa przejrzystość ma zapewnić obowiązek zawiadomienia.

W obydwu systemach prawnych w prawie krajowym można ustanowić wyłączenia i ograniczenia dotyczące obowiązku zapewnienia przejrzystości przez administratora w sytuacji, kiedy ograniczenie takie stanowi środek konieczny dla zabezpieczenia pewnych interesów publicznych bądź dla ochrony osoby, której dane dotyczą, lub praw i wolności innych osób, jeżeli jest to konieczne w demokratycznym społeczeństwie[160]. Takie wyłączenia mogą na przykład być konieczne w kontekście dochodzeń w sprawach karnych, ale mogą też być uzasadnione w innych okolicznościach.

4.3.1. Informacje

Zgodnie zarówno z prawem RE, jak i prawem UE administratorzy wykonujący czynności przetwarzania mają obowiązek informowania z wyprzedzeniem osoby, której dane dotyczą, o zamierzonym przetwarzaniu[161]. 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.

159 Konwencja nr 108, art. 8 lit. a)

160 *Tamże*, art. 9 ust. 2; oraz dyrektywa o ochronie danych, art. 13 ust. 1.

161 Konwencja nr 108, art. 8 lit. a); oraz dyrektywa o ochronie danych, art. 10 i 11.

Treść informacji

Informacje muszą obejmować cel przetwarzania, jak też tożsamość i dane kontaktowe administratora[162]. Na mocy dyrektywy o ochronie danych wymagane są dalsze informacje, o ile „są potrzebne, biorąc pod uwagę szczególne okoliczności, w których dane są gromadzone, w celu zagwarantowania rzetelnego przetwarzania danych w stosunku do osoby, której dane dotyczą". W art. 10 i 11 dyrektywy wśród tych informacji wymieniono między innymi kategorie przetwarzanych danych i odbiorców tych danych, jak również informacje o prawie dostępu i poprawienia danych. W przypadku gdy dane są gromadzone od osób, których dane dotyczą, należy wyjaśnić, czy odpowiedzi na pytania są obowiązkowe czy dobrowolne, oraz ewentualne konsekwencje nieudzielenia odpowiedzi[163].

Z punktu widzenia **prawa RE** przekazanie takich informacji może zostać uznane za dobrą praktykę na mocy zasady rzetelnego przetwarzania danych, więc w tym zakresie jest ono także elementem prawa RE.

Zasada rzetelnego przetwarzania wymaga, aby informacje były łatwo zrozumiałe dla osób, których dane dotyczą. Użyty język musi być odpowiedni z punktu widzenia adresatów. Poziom 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.

Niektóre osoby, których dane dotyczą, będą chcieć tylko ogólnych informacji o sposobie i przyczynie przetwarzania danych, inne natomiast zażądają szczegółowych wyjaśnień. Wyważone podejście do tego aspektu rzetelnego informowania opisano w opinii Grupy Roboczej Art. 29, w której proponuje się tzw. warstwowe noty informacyjne[164] pozwalające osobie, której dane dotyczą, wybrać pożądany poziom szczegółowości.

Czas przekazania informacji

Przepisy dotyczące czasu przekazania informacji zawarte w dyrektywie o ochronie danych różnią się nieznacznie w zależności od tego, czy dane zostały uzyskane od

162 Konwencja nr 108, art. 8 lit. a); oraz dyrektywa o ochronie danych, art. 10 lit. a) i b).

163 Dyrektywa o ochronie danych, art. 10 lit. c).

164 Grupa Robocza Art. 29 (2004), *Opinia 10/2004 w sprawie dalszej harmonizacji zasad informowania*, WP 100, Bruksela, 25 listopada 2004 r.

osoby, której dane dotyczą (art. 10), czy też od strony trzeciej (art. 11). Gdy dane uzyskano od osoby, której dane dotyczą, informacje należy przekazać najpóźniej w chwili gromadzenia danych. Gdy dane uzyskano od strony trzeciej, informacje należy przekazać najpóźniej w chwili zarejestrowania danych przez administratora lub przed ujawnieniem danych po raz pierwszy stronie trzeciej.

Zwolnienia z obowiązku informowania

W prawie UE istnieje ogólne zwolnienie z obowiązku informowania osoby, której dane dotyczą, w sytuacji, gdy osoba, której dane dotyczą, już posiada takie informacje[165]. Odnosi się to do sytuacji, gdy osoba, której dane dotyczą, wie już w związku z okolicznościami sprawy, że jej dane będą przetwarzane w określonym celu przez określonego administratora.

W art. 11 dyrektywy dotyczącym obowiązku informowania osoby, której dane dotyczą, w sytuacji, gdy dane nie zostały uzyskane od tej osoby, stwierdza się również, że takiego obowiązku nie ma, w szczególności przy przetwarzaniu do celów statystycznych bądź badań historycznych lub naukowych, jeżeli:

- dostarczenie takich informacji jest niemożliwe; lub
- wymagałoby niewspółmiernie dużego wysiłku; lub
- rejestracja lub ujawnianie danych jest wyraźnie przewidziane przez prawo[166].

Tylko w art. 11 ust. 2 dyrektywy o ochronie danych stwierdza się, że osoby, których dane dotyczą, nie muszą być informowane o czynnościach przetwarzania, jeśli są one przewidziane przez prawo. Ze względu na ogólne założenie prawne, że osoby podlegające przepisom prawa znają te przepisy, można twierdzić, że gdy dane są uzyskiwane na mocy art. 10 dyrektywy od osoby, której dane dotyczą, wówczas osoba, której dane dotyczą, posiada te informacje. Ze względu jednak na fakt, że znajomość przepisów prawa jest jedynie założeniem, na mocy zasady rzetelnego przetwarzania przepisy art. 10 nakładają wymóg informowania osoby, której dane dotyczą, nawet jeżeli przetwarzanie jest przewidziane przez prawo, zwłaszcza dlatego, iż poinformowanie osoby, której dane dotyczą, nie jest szczególnie uciążliwe, gdy dane są uzyskiwane bezpośrednio od niej.

165 Dyrektywa o ochronie danych, art. 10 i art. 11 ust. 1.

166 *Tamże*, motyw 40 i art. 11 ust. 2.

Jeżeli chodzi o prawo RE, w konwencji nr 108 przewidziano wprost wyłączenia od przepisów art. 8. Wyłączenia określone w art. 10 i 11 dyrektywy o ochronie danych ponownie można postrzegać jako przykłady dobrej praktyki dotyczącej wyłączeń na podstawie art. 9 konwencji nr 108.

Różne sposoby przekazywania informacji

Najlepszym sposobem przekazania informacji byłoby zwrócenie się z osobna ustnie lub w formie pisemnej do każdej osoby, której dane dotyczą. Jeżeli dane są uzyskiwane od osoby, której dane dotyczą, przekazanie informacji powinno następować równocześnie z gromadzeniem danych. Niemniej, zwłaszcza w sytuacji, gdy dane są uzyskiwane od stron trzecich, ze względu na oczywiste trudności praktyczne związane z osobistym kontaktem z osobami, których dane dotyczą, informacje można także przekazać w odpowiedniej publikacji.

Jednym z najbardziej efektywnych sposobów przekazania informacji jest zamieszczenie odpowiednich klauzul informacyjnych, np. 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.

4.3.2. Zawiadomienie

Na mocy prawa krajowego administratorów można zobowiązać do zawiadamiania właściwego organu nadzorczego o czynnościach przetwarzania, aby informacje o nich mogły zostać opublikowane. Alternatywnie w prawie krajowym można przewidzieć zatrudnienie przez administratorów urzędników do spraw ochrony danych osobowych, którzy będą w szczególności odpowiedzialni za prowadzenie rejestru czynności przetwarzania wykonywanych przez administratora[167]. Ten wewnętrzny rejestr musi być udostępniany osobom, które zgłaszają stosowny wniosek.

Przykład: W zawiadomieniu, a także w dokumentacji prowadzonej przez wewnętrznego urzędnika do spraw ochrony danych osobowych trzeba określić główne cechy czynności przetwarzania danych. Obejmują one informacje na temat administratora, celu przetwarzania, podstawy prawnej przetwarzania, kategorii przetwarzanych danych, prawdopodobnych stron trzecich będących

167 *Tamże*, art. 18 ust. 2 tiret drugie.

odbiorcami oraz tego, czy przewidywany jest transgraniczny przepływ danych, a jeżeli tak, to jaki.

Organ nadzorczy musi publikować zawiadomienia w formie specjalnego rejestru. Aby spełniał on swój cel, dostęp do tego rejestru powinien być łatwy i bezpłatny. To samo dotyczy dokumentacji prowadzonej przez urzędnika do spraw ochrony danych osobowych danego administratora.

W prawie krajowym można ustanowić wyłączenia od obowiązków zawiadamiania właściwego organu nadzorczego lub zatrudnienia wewnętrznego urzędnika do spraw ochrony danych w odniesieniu do czynności przetwarzania, w przypadku których mało prawdopodobne jest, aby stwarzały zagrożenie dla osób, których dane dotyczą; wyłączenia takie wyliczono w art. 18 ust. 2 dyrektywy o ochronie danych[168].

4.4. Przepisy dotyczące promowania przestrzegania przepisów

Najważniejsze kwestie

- Rozwijając zasadę rozliczalności, w dyrektywie o ochronie danych wymieniono kilka instrumentów promujących przestrzeganie przepisów:
  - kontrola wstępna planowanych czynności przetwarzania przez krajowy organ nadzorczy;
  - dysponujący specjalistyczną wiedzą w dziedzinie ochrony danych urzędnicy do spraw ochrony danych osobowych administratora;
  - kodeksy postępowania wskazujące przepisy dotyczące ochrony danych, które mają zastosowanie w danej dziedzinie życia społecznego, zwłaszcza w działalności biznesowej.
- W prawie RE podobne narzędzia mające na celu promowanie przestrzegania przepisów zawarto w zaleceniu w sprawie profilowania.

168 *Tamże*, art. 18 ust. 2 tiret pierwsze.

4.4.1. Kontrola wstępna

Zgodnie z art. 20 dyrektywy o ochronie danych organ nadzorczy ma obowiązek skontrolować czynności przetwarzania, które mogą stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą – ze względu na cel lub okoliczności przetwarzania – przed rozpoczęciem przetwarzania. W prawie krajowym należy określić, które czynności przetwarzania kwalifikują się do kontroli wstępnej. Taka kontrola może skutkować zakazem czynności przetwarzania lub nakazem wprowadzenia zmian w proponowanym przebiegu czynności przetwarzania. Celem art. 20 dyrektywy jest zapobieganie niepotrzebnie ryzykownemu przetwarzaniu jeszcze przed jego rozpoczęciem, gdyż organ nadzorczy jest uprawniony do wydania zakazu takich czynności. Warunkiem wstępnym skuteczności tego mechanizmu jest zawiadamianie organu nadzorczego. Aby zapewnić dopełnienie obowiązku zawiadomienia przez administratorów, organy nadzorcze muszą posiadać środki przymusu, na przykład możliwość nakładania kar na administratorów.

Przykład: Jeżeli przedsiębiorstwo wykonuje czynności przetwarzania, które zgodnie z prawem krajowym podlegają kontroli wstępnej, musi ono przedstawić organowi nadzorczemu dokumentację dotyczącą planowanych czynności przetwarzania. Przedsiębiorstwo nie może rozpocząć czynności przetwarzania przed otrzymaniem pozytywnej odpowiedzi od organu nadzorczego.

W niektórych państwach członkowskich prawo krajowe stanowi z kolei, że czynności przetwarzania można rozpocząć w przypadku braku reakcji ze strony organu nadzorczego w określonym czasie, na przykład trzech miesięcy.

4.4.2. Urzędnicy do spraw ochrony danych osobowych

W dyrektywie o ochronie danych umożliwiono wprowadzenie w prawie krajowym przepisów przewidujących wyznaczenie przez administratorów urzędnika pełniącego funkcję urzędnika do spraw ochrony danych osobowych[169]. Taki urzędnik ma obowiązek zapewnić niskie prawdopodobieństwo wywierania przez czynności przetwarzania niekorzystnego wpływu na prawa i wolności osób, których dane dotyczą[170].

169 *Tamże*, art. 18 ust. 2 tiret drugie.

170 Tamże.

Przykład: W Niemczech zgodnie z § 4f, ust. 1 federalnej ustawy o ochronie danych (*Bundesdatenschutzgesetz*) prywatne przedsiębiorstwa mają obowiązek wyznaczyć wewnętrznego urzędnika do spraw ochrony danych osobowych, jeżeli zatrudniają na stałe 10 lub więcej osób zajmujących się zautomatyzowanym przetwarzaniem danych osobowych.

Jak wyraźnie wskazano w dyrektywie, zdolność do osiągnięcia tego celu wymaga pewnej niezależności stanowiska urzędnika w ramach organizacji administratora. Aby umożliwić skuteczne funkcjonowanie tego urzędu, niezbędna jest też daleko idąca ochrona stanowiska urzędnika przed np. nieuzasadnionym zwolnieniem.

W celu promowania przestrzegania krajowego prawa o ochronie danych koncepcję wewnętrznych urzędników do spraw ochrony danych osobowych przyjęto też w niektórych zaleceniach Rady Europy[171].

4.4.3. Kodeksy postępowania

Aby promować przestrzeganie przepisów, sektor biznesowy i inne mogą opracować szczegółowe zasady dotyczące typowych czynności przetwarzania, kodyfikując w ten sposób najlepsze praktyki. Wiedza specjalistyczna członków sektora ułatwi określenie wytycznych, które będą praktyczne, a zatem przestrzegane. W związku z tym państwa członkowskie i Komisję zachęca się, aby promowały opracowywanie kodeksów postępowania, których celem będzie usprawnienie procesu prawidłowego wprowadzania krajowych przepisów przyjętych przez państwa członkowskie na mocy dyrektywy, uwzględniając szczególne cechy różnych sektorów[172].

Aby zapewnić zgodność tych kodeksów postępowania z krajowymi przepisami przyjętymi na podstawie dyrektywy o ochronie danych, państwa członkowskie muszą ustanowić procedurę oceny kodeksów. Procedura taka wymaga zwykle zaangażowania krajowego organu, stowarzyszeń branżowych oraz innych podmiotów reprezentujących pozostałe kategorie administratorów[173].

Projekty kodeksów wspólnotowych, jak również zmiany i uzupełnienia istniejących kodeksów wspólnotowych mogą zostać przedstawione do oceny Grupie Roboczej

171 Zob. na przykład Zalecenie w sprawie profilowania, art. 8 ust. 3.

172 Zob. dyrektywę o ochronie danych, art. 27 ust. 1.

173 *Tamże*, art. 27 ust. 2.

Art. 29. Po zatwierdzeniu przez Grupę Roboczą Komisja Europejska może zapewnić odpowiednie rozpowszechnienie takich kodeksów[174].

Przykład: Europejska Federacja Stowarzyszeń Marketingu Bezpośredniego (FEDMA) opracowała europejski kodeks postępowania dotyczący wykorzystania danych osobowych do marketingu bezpośredniego. Kodeks ten pomyślnie przeszedł ocenę Grupy Roboczej Art. 29. W 2010 r. dodano do niego załącznik odnoszący się do elektronicznej komunikacji marketingowej[175].

174 *Tamże*, art. 27 ust. 3.

175 Grupa Robocza Art. 29 (2010), Opinia 4/2010 na temat europejskiego kodeksu postępowania Europejskiej Federacji Stowarzyszeń Marketingu Bezpośredniego (FEDMA) w sprawie ochrony danych osobowych wykorzystywanych w marketingu bezpośrednim, WP 174, Bruksela, 13 lipca 2010 r.

5

Prawa osób, których dane dotyczą, oraz ich egzekwowanie

UE	Omówione zagadnienia	RE
Prawo dostępu		
Artykuł 12 dyrektywy o ochronie danych TSUE, C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M.E.E. Rijkeboer*, 7 maja 2009 r.	**Prawo dostępu do własnych danych**	Artykuł 8 lit. b) konwencji nr 108
	Prawo do poprawienia danych, ich skasowania (usunięcia) lub zablokowania	Artykuł 8 lit. c) konwencji nr 108 ETPC, *Cemalettin Canli przeciwko Turcji*, nr 22427/04, 18 listopada 2008 r. ETPC, *Segerstedt-Wiberg i inni przeciwko Szwecji*, nr 62332/00, 6 czerwca 2006 r. ETPC, *Ciubotaru przeciwko Mołdawii*, nr 27138/04, 27 kwietnia 2010 r.
Prawo sprzeciwu		
Artykuł 14 ust. 1 lit. a) dyrektywy o ochronie danych	**Prawo sprzeciwu ze względu na konkretną sytuację osoby, której dane dotyczą**	Artykuł 5 ust. 3 zalecenia w sprawie profilowania
Artykuł 14 ust. 1 lit. b) dyrektywy o ochronie danych	**Prawo sprzeciwu wobec dalszego wykorzystania danych w celach marketingowych**	Artykuł 4 ust. 1 zalecenia w sprawie marketingu bezpośredniego

UE	Omówione zagadnienia	RE
Artykuł 15 dyrektywy o ochronie danych	**Prawo sprzeciwu wobec zautomatyzowanego procesu decyzyjnego**	Artykuł 5 ust. 5 zalecenia w sprawie profilowania
Niezależny nadzór		
Artykuł 8 ust. 3 karty praw podstawowych Artykuł 28 dyrektywy o ochronie danych Rozdział V rozporządzenia o ochronie danych przez instytucje UE Rozporządzenia o ochronie danych TSUE, C-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec*, 9 marca 2010 r. TSUE, C-614/10, *Komisja Europejska przeciwko Republice Austrii*, 16 października 2012 r. TSUE, C-288/12, *Komisja Europejska przeciwko Węgrom*, 8 kwietnia 2014 r.	**Krajowe organy nadzorcze**	Artykuł 1 protokołu dodatkowego do konwencji nr 108
Środki prawne i sankcje		
Artykuł 12 dyrektywy o ochronie danych	**Wniosek kierowany do administratora**	Artykuł 8 lit. b) konwencji nr 108
Artykuł 28 ust. 4 dyrektywy o ochronie danych Artykuł 32 ust. 2 rozporządzenia o ochronie danych przez instytucje UE	**Skargi zgłaszane do organu nadzorczego**	Artykuł 1 ust. 2 lit. b) protokołu dodatkowego do konwencji nr 108
Artykuł 47 karty praw podstawowych	**Sądy (ogólnie)**	Artykuł 13 EKPC
Artykuł 28 ust. 3 dyrektywy o ochronie danych	**Sądy krajowe**	Artykuł 1 ust. 4 protokołu dodatkowego do konwencji nr 108
Artykuł 263 akapit 4 TFUE Artykuł 32 ust. 1 rozporządzenia o ochronie danych przez instytucje UE Artykuł 267 TFUE	**TSUE**	
	ETPC	Artykuł 34 EKPC

UE	Omówione zagadnienia	RE
Środki prawne i sankcje		
Artykuł 47 karty praw podstawowych Artykuły 22 i 23 dyrektywy o ochronie danych TSUE, C-14/83, *Sabine von Colson i Elisabeth Kamann przeciwko Land Nordrhein-Westfalen*, 10 kwietnia 1984 r. TSUE, C-152/84, *M.H. Marshall przeciwko Southampton i South-West Hampshire Area Health Authority*, 26 lutego 1986 r.	**Z tytułu naruszenia krajowego prawa o ochronie danych**	Artykuł 13 EKPC (tylko w przypadku państw członkowskich RE) Artykuł 10 konwencji nr 108 ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2 grudnia 2008 r. ETPC, *Biriuk przeciwko Litwie*, nr 23373/03, 25 listopada 2008 r.
Artykuły 34 i 49 rozporządzenia o ochronie danych przez instytucje UE TSUE, C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*, 29 czerwca 2010 r.	**Z tytułu naruszenia prawa UE przez instytucje i organy UE**	

Skuteczność ogólnie przepisów prawnych, a w szczególności odnoszących się do ochrony praw osób, których dane dotyczą, zależy w dużym stopniu od istnienia odpowiednich mechanizmów ich egzekwowania. W europejskim prawie o ochronie danych osoba, której dane dotyczą, musi mieć możliwość ochrony swoich danych na mocy prawa krajowego. Konieczne jest też ustanowienie prawem krajowym niezależnych organów nadzorczych pomagających osobom, których dane dotyczą, w wykonywaniu swoich praw oraz sprawujących nadzór nad przetwarzaniem danych osobowych. Ponadto zagwarantowane na mocy EKPC i karty praw podstawowych prawo do skutecznego środka prawnego wymaga udostępnienia każdej osobie środków sądowych.

5.1. Prawa osób, których dane dotyczą

Najważniejsze kwestie

- Każda osoba ma na mocy prawa krajowego prawo żądać od dowolnego administratora informacji, czy administrator ten przetwarza jej dane.
- Na mocy prawa krajowego osoby, których dane dotyczą, mają prawo:
  - żądać dostępu do swoich danych od dowolnego administratora, który przetwarza te dane;

  - żądać, aby ich dane zostały poprawione (lub w stosownych przypadkach zablokowane) przez przetwarzającego je administratora, jeżeli są one nieprawidłowe;
  - żądać, aby ich dane zostały usunięte lub w stosownych przypadkach zablokowane przez administratora, jeżeli administrator przetwarza ich dane niezgodnie z prawem.
- Ponadto osoby, których dane dotyczą, mają prawo zgłosić administratorowi sprzeciw wobec:
  - zautomatyzowanych decyzji (podejmowanych z wykorzystaniem danych osobowych przetwarzanych wyłącznie w sposób automatyczny);
  - przetwarzania ich danych, jeżeli prowadzi ono do niewspółmiernych wyników;
  - wykorzystania ich danych do celów marketingu bezpośredniego.

5.1.1. Prawo dostępu

W prawie UE w art. 12 dyrektywy o ochronie danych wskazano elementy prawa dostępu osoby, której dane dotyczą, w tym prawo do uzyskania od administratora „potwierdzenia, czy dotyczące jej dane są przetwarzane oraz co najmniej informacji o celach przetwarzania danych, kategoriach danych oraz odbiorcach lub kategoriach odbiorców, którym dane te są ujawniane", a także „sprostowania, usunięcia lub zablokowania danych, których przetwarzanie nie jest zgodne z przepisami niniejszej dyrektywy, w szczególności ze względu na niekompletność lub niedokładność danych".

W prawie RE zapisano te same prawa i muszą one zostać zapewnione prawem krajowym (art. 8 konwencji nr 108). W kilku zaleceniach RE użyto terminu „dostęp" oraz opisano różne aspekty prawa dostępu, proponując ich wdrożenie w prawie krajowym w taki sam sposób, jak wskazano to w powyższym ustępie.

Zgodnie z art. 9 konwencji nr 108 i art. 13 dyrektywy o ochronie danych obowiązek stosowania się do wniosku o dostęp ze strony osoby, której dane dotyczą, przez administratora może być ograniczony nadrzędnymi interesami prawnymi innych osób. Nadrzędnym interesem prawnym może być interes publiczny, np. bezpieczeństwo narodowe, bezpieczeństwo publiczne czy ściganie przestępstw, a także interes prywatny, który przeważa nad interesem ochrony danych. Wszelkie wyłączenia lub ograniczenia muszą być niezbędne w demokratycznym społeczeństwie i proporcjonalne do zamierzonego celu. W zupełnie wyjątkowych przypadkach, na przykład ze względu na wskazania medyczne, ochrona osoby, której dane dotyczą, może

wymagać ograniczenia przejrzystości; odnosi się to w szczególności do ograniczenia prawa dostępu każdej osoby, której dane dotyczą.

W każdym przypadku, gdy dane są przetwarzane wyłącznie do celów badań naukowych lub do celów statystycznych, w dyrektywie o ochronie danych dopuszcza się ograniczenie praw dostępu prawem krajowym, jednak niezbędne są odpowiednie zabezpieczenia prawne. W szczególności trzeba zapewnić niepodejmowanie środków ani decyzji dotyczących konkretnej osoby w kontekście takiego przetwarzania danych oraz upewnić się, że „wyraźnie nie występuje ryzyko naruszenia prywatności osoby, której dane dotyczą”[176]. Podobne zapisy zawarto w art. 9 ust. 3 konwencji nr 108.

Prawo dostępu do własnych danych

W prawie RE prawo dostępu do własnych danych wyraźnie potwierdzono w art. 8 konwencji nr 108. ETPC wielokrotnie uznawał, że osobie przysługuje prawo dostępu do informacji o jej danych osobowych przechowywanych lub wykorzystywanych przez innych, i że to prawo wynika z potrzeby poszanowania życia prywatnego[177]. W sprawie *Leander*[178] ETPC uznał jednak, że prawo dostępu do danych osobowych przechowywanych przez organy publiczne może w pewnych okolicznościach zostać ograniczone.

W prawie UE prawo dostępu do własnych danych potwierdzono wprost w art. 12 dyrektywy o ochronie danych oraz, jako prawo podstawowe, w art. 8 ust. 2 karty praw podstawowych.

W art. 12 lit. a) dyrektywy stanowi się, że państwa członkowskie gwarantują każdej osobie, której dane dotyczą, prawo dostępu do swoich danych osobowych i informacji. W szczególności każda osoba, której dane dotyczą, ma prawo uzyskać od administratora potwierdzenie, czy są przetwarzane dotyczące jej dane, oraz informacje obejmujące co najmniej:

- cele przetwarzania;

176 Dyrektywa o ochronie danych, art. 13 ust. 2.

177 ETPC, *Gaskin przeciwko Zjednoczonemu Królestwu*, nr 10454/83, 7 lipca 1989 r.; ETPC, *Odièvre przeciwko Francji* [Wielka Izba], nr 42326/98, 13 lutego 2003 r.; ETPC, *K.H. i inni przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.; ETPC, *Godelli przeciwko Włochom*, nr 33783/09, 25 września 2012 r.

178 ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.

- kategorie przetwarzanych danych;
- dane podlegające przetwarzaniu;
- odbiorców lub kategorie odbiorców, którym dane są ujawniane;
- wszelkie dostępne informacje o źródłach danych podlegających przetwarzaniu;
- w przypadku zautomatyzowanego procesu decyzyjnego zasady automatycznego przetwarzania danych.

W prawie krajowym można określić dodatkowe informacje, które powinien podać administrator, na przykład podstawę prawną upoważniającą do przetwarzania danych.

Przykład: Uzyskując dostęp do swoich danych osobowych, osoba jest w stanie określić, czy dane te są prawidłowe. W związku z tym niezbędne jest poinformowanie osoby, której dane dotyczą, o kategoriach przetwarzanych danych, a także o treści tych danych. Niewystarczające jest zatem podanie przez administratora, że przetwarza nazwisko, adres, datę urodzenia i informacje o zainteresowaniach osoby, której dane dotyczą. Administrator musi także ujawnić osobie, której dane dotyczą, że przetwarza „nazwisko: N.N.; adres: 1040 Wien, Schwarzenbergplatz 11, Austria; datę urodzenia: 10.10.1974 r.; oraz zainteresowania (zgodnie z deklaracją osoby, której dane dotyczą): muzyka klasyczna". Ostatnia pozycja zawiera dodatkowo informacje o źródle danych.

Informacje przekazywane osobie, której dane dotyczą, na temat danych podlegających przetwarzaniu oraz ich źródeł (jeżeli są dostępne) muszą zostać podane w zrozumiałej formie, co może oznaczać obowiązek bardziej szczegółowego wyjaśnienia przez administratora osobie, której dane dotyczą, co jest przetwarzane. Na przykład podanie jedynie skrótów technicznych lub terminów medycznych w odpowiedzi na wniosek o dostęp nie jest zazwyczaj wystarczające, nawet jeżeli przechowywane są tylko takie skróty lub terminy.

W odpowiedzi na wniosek o dostęp muszą zostać podane informacje o źródle danych przetwarzanych przez administratora, jeżeli informacje takie są dostępne. Przepis ten należy rozumieć w świetle zasad rzetelności i rozliczalności. Administrator nie może zniszczyć informacji o źródle danych, aby zwolnić się z obowiązku ich

ujawnienia, ani też nie może zignorować typowych standardów i uznanych potrzeb dotyczących dokumentacji w zakresie jego działalności. Nieprowadzenie dokumentacji dotyczącej źródła przetwarzanych danych zazwyczaj oznacza niedopełnienie obowiązków administratora związanych z prawem dostępu.

W przypadku gdy przeprowadzane są zautomatyzowane oceny, konieczne jest wyjaśnienie ogólnych zasad oceny, w tym konkretnych kryteriów uwzględnionych przy ocenie osoby, której dane dotyczą.

W dyrektywie nie wskazano wyraźnie, czy prawo dostępu do informacji dotyczy przeszłości, a jeżeli tak, jakiego okresu w przeszłości. Pod tym względem, jak podkreślono w orzecznictwie TSUE, prawo dostępu do własnych danych nie może być w nadmierny sposób ograniczane terminami. Osoby, których dane dotyczą, muszą mieć w racjonalnym zakresie możliwość uzyskania informacji na temat czynności przetwarzania danych dokonywanych w przeszłości.

Przykład: W sprawie[179] *Rijkeboer* TSUE miał rozstrzygnąć, czy zgodnie z art. 12 lit. a) dyrektywy 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 art. 12 lit. a) dyrektywy dopuszcza się takie ograniczenie czasowe, Trybunał postanowił dokonać wykładni tego artykułu 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 poprawił, usunął lub zablokował jej dane (art. 12 lit. b)), bądź zawiadomił strony trzecie, którym ujawniono dane, o takim poprawieniu, usunięciu lub zablokowaniu (art. 12 lit. c)). Prawo dostępu jest również niezbędne, aby umożliwić osobie, której dane dotyczą, wykonanie prawa sprzeciwu wobec przetwarzania jej danych osobowych (art. 14) bądź prawa do skorzystania ze środków prawnych, jeżeli poniosła szkody (art. 22 i 23).

Aby zapewnić w praktyce skuteczność przepisów, o których mowa powyżej, Trybunał 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

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

danych potencjalnie nielegalnych lub nieprawidłowych, ani też do wniesienia środków prawnych i uzyskania naprawienia poniesionej szkody".

Prawo poprawienia, usunięcia i zablokowania danych

„Każda osoba musi mieć możliwość skorzystania z prawa dostępu do dotyczących jej danych, które poddane są przetwarzaniu, w celu zweryfikowania zwłaszcza prawidłowości danych oraz legalności ich przetwarzania"[180]. Zgodnie z tymi zasadami osoby, których dane dotyczą, muszą mieć na mocy prawa krajowego prawo żądania od administratora, aby poprawił, usunął lub zablokował ich dane, jeżeli uważają, że ich przetwarzanie jest niezgodne z przepisami dyrektywy, szczególnie ze względu na nieprawidłowość lub niekompletność danych[181].

Przykład: W sprawie *Cemalettin Canli przeciwko Turcji*[182] 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. ETPC uznał, że informacje zawarte w raporcie policyjnym wchodziły w zakres art. 8 EKPC, gdyż systematycznie gromadzone i przechowywane w aktach będących w posiadaniu organów władz informacje publiczne mogą również dotyczyć „życia prywatnego". Ponadto raport policyjny był błędny, a sposób jego sporządzenia i przedłożenia sądowi karnemu nie był zgodny z prawem. Trybunał stwierdził, że doszło do naruszenia art. 8.

180 Dyrektywa o ochronie danych, motyw 41.

181 *Tamże*, art. 12 lit. b).

182 ETPC, *Cemalettin Canli przeciwko Turcji*, nr 22427/04, 18 listopada 2008 r., pkt 33, 42 i 43; ETPC, *Dalea przeciwko Francji*, nr 964/07, 2 lutego 2010 r.

Przykład: W sprawie *Segerstedt-Wiberg i inni przeciwko Szwecji*[183] skarżący należeli do liberalnych i komunistycznych partii politycznych. Podejrzewali oni, że informacje na ich temat znalazły się w aktach policyjnych. ETPC stwierdził, że przechowywanie tych danych miało podstawę prawną i służyło uzasadnionemu celowi. W odniesieniu do niektórych skarżących ETPC uznał, że dalsze zatrzymywanie danych stanowiło nieproporcjonalną ingerencję w ich życie prywatne. Na przykład w przypadku p. Schmida władze przechowywały informacje o tym, jakoby w 1969 r. miał on namawiać do przemocy w reakcji na działania policji podczas demonstracji. ETPC 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.

W niektórych przypadkach wystarcza, aby osoba, której dane dotyczą, po prostu zażądała poprawienia np. pisowni nazwiska, zmiany adresu lub numeru telefonu. Jeżeli jednak takie wnioski dotyczą zagadnień prawnych, jak np. tożsamości prawnej osoby, której dane dotyczą, bądź prawidłowego miejsca zamieszkania do celów doręczeń dokumentów prawnych, wnioski o poprawienie 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, poprawienie swoich danych. ETPC stwierdził naruszenie art. 8 EKPC w kilku przypadkach, gdy skarżący nie był w stanie zakwestionować nieprawidłowości informacji przechowywanych w tajnych rejestrach[184].

Przykład: W sprawie *Ciubotaru przeciwko Mołdawii*[185] 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

183 ETPC, *Segerstedt-Wiberg i inni przeciwko Szwecji*, nr 62332/00, 6 czerwca 2006 r., pkt 89 i 90; zob. też na przykład ETPC, *M.K. przeciwko Francji*, nr 19522/09, 18 kwietnia 2013 r.

184 ETPC, *Rotaru przeciwko Rumunii*, nr 28341/95, 4 maja 2000 r.

185 ETPC, *Ciubotaru przeciwko Mołdawii*, nr 27138/04, 27 kwietnia 2010 r., pkt 51 i 59.

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.

Podczas postępowania cywilnego lub postępowania przed organem władzy publicznej prowadzonego w celu ustalenia, czy dane są poprawne, 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. W tym okresie administrator nie może przedstawiać danych jako pewnych lub ostatecznych, zwłaszcza wobec stron trzecich.

Wniosek osoby, której dane dotyczą, o ich skasowanie lub usunięcie, często opiera się na twierdzeniu, że przetwarzanie danych nie ma uzasadnionych podstaw. Takie twierdzenia często pojawiają się, gdy zgodę cofnięto lub pewne dane nie są już potrzebne, aby zrealizować cel gromadzenia danych. Ciężar udowodnienia, że przetwarzanie danych jest zgodne z prawem, spoczywa na administratorze danych, gdyż to on jest odpowiedzialny za zgodność przetwarzania z prawem. Zgodnie z zasadą odpowiedzialności administrator musi w każdej chwili być w stanie wykazać należytą podstawę prawną przetwarzania danych, a w razie jej braku przetwarzanie musi zostać wstrzymane.

Jeżeli przetwarzanie danych zostaje zakwestionowane ze względu na rzekomą niepoprawność danych lub ich przetwarzanie niezgodnie z prawem, osoba, której dane dotyczą, zgodnie z zasadą rzetelnego przetwarzania, może zażądać, aby sporne dane zostały zablokowane. Oznacza to, że dane nie zostają usunięte, ale administrator musi powstrzymać się od korzystania z nich w okresie blokady. Jest to szczególnie konieczne w przypadkach, gdy dalsze wykorzystanie danych nieprawidłowych lub przechowywanych niezgodnie z prawem mogłoby zaszkodzić osobie, której dane dotyczą. W prawie krajowym należy określić w sposób bardziej szczegółowy, kiedy może powstać obowiązek zablokowania korzystania z danych, i w jaki sposób powinno to nastąpić.

Osoby, których dane dotyczą, mają dodatkowo prawo żądać, aby administrator zawiadomił strony trzecie o jakiejkolwiek blokadzie, poprawieniu lub usunięciu danych, jeżeli otrzymały one dane przed tymi operacjami przetwarzania. Ujawnienie danych stronom trzecim powinno zostać udokumentowane przez administratora, więc powinna być możliwa identyfikacja odbiorców danych i żądanie ich usunięcia. Jeśli dane zostały jednak tymczasem opublikowane, na przykład w internecie, spowodowanie ich usunięcia we wszystkich przypadkach może być niemożliwe ze względu na niemożność odnalezienia odbiorców danych. Zgodnie z dyrektywą o ochronie danych kontakt z odbiorcami danych w celu poprawienia usunięcia lub zablokowania danych jest obowiązkowy, „o ile nie okaże się to niemożliwe lub nie będzie wymagało niewspółmiernie dużego wysiłku”[186].

5.1.2. Prawo sprzeciwu

Prawo sprzeciwu obejmuje prawo sprzeciwu wobec zautomatyzowanych decyzji indywidualnych, prawo sprzeciwu ze względu na konkretną sytuację osoby, której dane dotyczą, oraz prawo sprzeciwu wobec dalszego wykorzystania danych do celów marketingu bezpośredniego.

Prawo sprzeciwu wobec zautomatyzowanych decyzji indywidualnych

Decyzje zautomatyzowane to decyzje podejmowane z wykorzystaniem danych osobowych przetwarzanych wyłącznie w sposób automatyczny. Jeżeli takie decyzje mogą wywierać znaczny wpływ na życie jednostek ze względu na to, że dotyczą na przykład zdolności kredytowej, wyników osiąganych w pracy, sposobu zachowania lub wiarygodności, niezbędna jest specjalna ochrona, aby uniknąć niepożądanych konsekwencji. W dyrektywie o ochronie danych stwierdza się, że zautomatyzowane decyzje nie powinny przesądzać o kwestiach ważnych dla danej osoby, oraz wymaga się, aby dana osoba miała prawo do przeglądu zautomatyzowanej decyzji[187].

Przykład: Ważnym przykładem praktycznym zautomatyzowanego podejmowania decyzji jest ocena zdolności kredytowej. Aby szybko podjąć decyzję o zdolności kredytowej przyszłego klienta, uzyskuje się od niego pewne dane, dotyczące np. zawodu i sytuacji rodzinnej, po czym łączy się je z danymi na

186 Dyrektywa o ochronie danych, art. 12 lit. c) *in fine*.

187 *Tamże, art.* 15 ust. 1.

jego temat dostępnymi z innych źródeł, takich jak systemy informacji kredytowej. Dane te są automatycznie wprowadzane do algorytmu punktującego, który oblicza ogólną wartość reprezentującą zdolność kredytową potencjalnego klienta. W ten sposób pracownik przedsiębiorstwa może w ciągu kilku sekund podjąć decyzję, czy osobę, której dane dotyczą, można zaakceptować jako klienta, czy też nie.

Niemniej jednak zgodnie z dyrektywą państwa członkowskie mają obowiązek zapewnić możliwość podjęcia zautomatyzowanej decyzji indywidualnej w stosunku do osoby w przypadku, gdy interesy osoby, której dane dotyczą, nie są zagrożone, gdyż decyzja ta jest korzystna dla osoby, której dane dotyczą, lub też są one zabezpieczone przy wykorzystaniu innych odpowiednich środków[188]. Prawo do sprzeciwu wobec zautomatyzowanych decyzji jest również nieodłącznym elementem **prawa RE**, czego dowodzi treść zalecenia w sprawie profilowania[189].

Prawo sprzeciwu ze względu na konkretną sytuację osoby, której dane dotyczą

Osobie, której dane dotyczą, nie przysługuje ogólne prawo sprzeciwu wobec przetwarzania jej danych[190]. W art. 14 lit. a) dyrektywy o ochronie danych przyznaje się jednak osobie, której dane dotyczą, prawo wniesienia sprzeciwu z ważnych i uzasadnionych przyczyn wynikających z jej konkretnej sytuacji. Podobne prawo zapisano w zaleceniu RE w sprawie profilowania[191]. Takie przepisy mają na celu należyte wyważenie prawa do ochrony danych osoby, której dane dotyczą, oraz uzasadnionych praw innych osób związanych z przetwarzaniem danych osoby, której dane dotyczą.

Przykład: Bank przechowuje przez siedem lat dane na temat klientów, którzy nie wykonali zobowiązań z tytułu spłaty kredytu. Klient, którego dane są przechowywane w tej bazie danych, składa wniosek o kolejny kredyt. Bank dokonuje sprawdzenia bazy danych i oceny sytuacji finansowej klienta, po czym odmawia kredytu. Klient może jednak sprzeciwić się przechowywaniu danych

188 *Tamże*, art. 15 ust. 2.

189 Zalecenie w sprawie profilowania, art. 5 ust. 5.

190 Zob. też ETPC, *M.S. przeciwko Szwecji*, nr 20837/92, 27 sierpnia 1997 r., gdzie bez zgody lub możliwości sprzeciwu przekazano dane medyczne; lub ETPC, *Leander przeciwko Szwecji*, nr 9248/81, 26 marca 1987 r.; lub ETPC, *Mosley przeciwko Zjednoczonemu Królestwu*, nr 48009/08, 10 maja 2011 r.

191 Zalecenie w sprawie profilowania, art. 5 ust. 3.

osobowych w bazie danych i żądać usunięcia danych, jeżeli jest w stanie wykazać, że niewykonanie zobowiązań było jedynie wynikiem błędu, który został skorygowany niezwłocznie po tym, gdy klient dowiedział się o nim.

W rezultacie skutecznego sprzeciwu administrator nie może dalej przetwarzać omawianych danych. Operacje przetwarzania wykonywane na danych osoby, której dane dotyczą, przed wniesieniem sprzeciwu pozostają jednak zgodne z prawem.

Prawo sprzeciwu wobec dalszego wykorzystania danych do celów marketingu bezpośredniego

W art. 14 lit. b) dyrektywy o ochronie danych zapisano konkretne prawo sprzeciwu wobec wykorzystania danych do celów marketingu bezpośredniego. Prawo takie zawarto również w zaleceniu w sprawie marketingu bezpośredniego RE[192]. Ten rodzaj sprzeciwu powinien zostać wniesiony przed udostępnieniem danych stronom trzecim do celów marketingu bezpośredniego. Dlatego też osoba, której dane dotyczą, musi mieć możliwość sprzeciwu przed przekazaniem tych danych.

5.2. Niezależny nadzór

Najważniejsze kwestie

- Aby zapewnić skuteczną ochronę danych, na mocy prawa krajowego muszą zostać ustanowione niezależne organy nadzorcze.
- Krajowe organy nadzorcze muszą działać w sposób całkowicie niezależny, co trzeba zagwarantować w ustanawiającym je prawie i musi to znaleźć odzwierciedlenie w strukturze organizacyjnej organu nadzorczego.
- 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;

192 RE, Komitet Ministrów (1985), Recommendation Rec(85)20 to member states on the protection of personal data used for the purposes of direct marketing [„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.

- 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 interwencja przez:
  - ostrzeganie, upominanie bądź nawet karanie administratorów i podmiotów przetwarzających;
  - nakazywanie poprawienia, zablokowania lub usunięcia danych;
  - nakładanie zakazu przetwarzania;
- kierowanie spraw do sądu.

Na mocy dyrektywy o ochronie danych wymagany jest niezależny nadzór jako ważny mechanizm zapewniający skuteczną ochronę danych. W dyrektywie wprowadzono narzędzie egzekwowania ochrony danych, które nie występowało pierwotnie w konwencji nr 108 ani w wytycznych OECD w zakresie prywatności.

Ze względu na to, że niezależny nadzór okazał się niezbędnym elementem skutecznej ochrony danych, w nowym zapisie przyjętych w 2013 r. zmienionych wytycznych OECD w zakresie ochrony prywatności kraje członkowskie wzywa się do „ustanowienia i utrzymania organów egzekwujących przepisy w zakresie prywatności, które będą cechować się zarządzaniem, zasobami i wiedzą techniczną niezbędnymi w celu skutecznego korzystania z przyznanych im uprawnień oraz podejmowania decyzji w obiektywny, bezstronny i konsekwentny sposób”[193].

W prawie RE ustanowienie organów nadzorczych jest obowiązkowe na mocy protokołu dodatkowego do konwencji nr 108. W art. 1 tego aktu prawnego określono ramy prawne funkcjonowania niezależnych organów nadzorczych, które umawiające się strony muszą wdrożyć w swoim prawie krajowym. Przy opisie zadań i uprawnień tych organów użyto sformułowań podobnych do zawartych w dyrektywie o ochronie danych. Co do zasady organy nadzorcze powinny zatem funkcjonować w ten sam sposób na mocy zarówno prawa UE, jak i RE.

W prawie UE kompetencje i strukturę organizacyjną organów nadzorczych określono po raz pierwszy w art. 28 ust. 1 dyrektywy o ochronie danych. W

193 OECD (2013), *Guidelines on governing the Protection of Privacy and transborder flows of personal data* [„Wytyczne w zakresie ochrony prywatności i przepływu danych osobowych przez granice”], pkt 19 lit. c).

rozporządzeniu o ochronie danych przez instytucje UE[194] ustanowiono EIOD jako organ nadzorczy w odniesieniu do przetwarzania danych przez organy i instytucje UE. Określając role i obowiązki organu nadzorczego, w rozporządzeniu tym oparto się na doświadczeniach zgromadzonych od chwili ogłoszenia dyrektywy o ochronie danych.

Niezależność organów ochrony danych zagwarantowano w art. 16 ust. 2 TFUE oraz art. 8 ust. 3 karty praw podstawowych. W tym ostatnim przepisie kontrolę niezależnego organu wyraźnie wskazano jako niezbędny element podstawowego prawa do ochrony danych. Ponadto w dyrektywie o ochronie danych na państwa członkowskie nałożono obowiązek ustanowienia organów nadzorczych w celu monitorowania stosowania dyrektywy przy zachowaniu całkowitej niezależności[195]. 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 nadzorujących ochronę danych[196]. Rozumowanie Trybunału obrazują poniższe przykłady.

Przykład: W sprawie *Komisja przeciwko Niemcom*[197] 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 polegało na tym, że Niemcy poddały nadzorowi państwa organy odpowiedzialne za monitorowanie przetwarzania danych osobowych poza sektorem publicznym w poszczególnych krajach związkowych.

194 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, art. 41–48.

195 Dyrektywa o ochronie danych, art. 28 ust. 1 *in fine*; protokół dodatkowy do konwencji nr 108, art. 1 ust. 3.

196 Zob. FRA (2010), *Fundamental rights: challenges and achievements in 2010, Annual report 2010* [„Prawa podstawowe: wyzwania i osiągnięcia w 2010 r. Sprawozdanie za 2010 r."], s. 59. FRA omówiła tę kwestię bardziej szczegółowo w opublikowanym w maju 2010 r. sprawozdaniu *Data protection in the European Union: the role of National Data Protection Authorities* [„Ochrona danych w Unii Europejskiej: rola krajowych organów ochrony danych"].

197 TSUE, C-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec*, 9 marca 2010 r., pkt 27.

Według Trybunału ocena zasadności skargi zależy od zakresu wymogu niezależności zawartego w tym przepisie, a zatem od jego wykładni.

Trybunał podkreślił, że słowa „całkowicie niezależne" w art. 28 ust. 1 dyrektywy trzeba interpretować w oparciu o rzeczywiste brzmienie tego przepisu oraz cele i systematykę dyrektywy o ochronie danych[198].Trybunał podkreślił, że organy nadzorcze są „strażnikami" zapisanych w dyrektywie praw związanych z przetwarzaniem danych osobowych, w związku z czym ich ustanowienie w państwach członkowskich jest uznawane za „istotny element ochrony osób w związku z przetwarzaniem danych osobowych"[199].Trybunał stwierdził, że „przy wykonywaniu swoich obowiązków organy kontroli powinny działać w sposób obiektywny i bezstronny. W tym celu powinny pozostawać poza jakimkolwiek wpływem z zewnątrz, w tym bezpośrednim czy pośrednim wpływem państwa czy krajów związkowych, a nie tylko poza wpływem organów kontrolowanych"[200].

TSUE ustalił również, że pojęcie „całkowitej niezależności" należy interpretować w świetle niezależności EIOD zgodnie z definicją w rozporządzeniu o ochronie danych przez instytucje UE. Jak podkreślił Trybunał, w art. 44 ust. 2 tego rozporządzenia wyjaśniono pojęcie niezależności, dodając, że podczas wykonywania swoich obowiązków EIOD nie oczekuje i nie przyjmuje instrukcji od nikogo. Wyklucza to nadzór państwa nad niezależnym organem nadzorującym ochronę danych[201].

W związku z tym TSUE uznał, że niemieckie instytucje ochrony danych na szczeblu federalnym odpowiedzialne za monitorowanie przetwarzania danych osobowych przez podmioty niepubliczne nie są wystarczająco niezależne, gdyż podlegają nadzorowi ze strony państwa.

Przykład: W sprawie *Komisja przeciwko Austrii*[202] TSUE wskazał podobne problemy dotyczące sytuacji niektórych członków i pracowników austriackiego urzędu ochrony danych (Komisji Ochrony Danych – DSK). W tej sprawie Trybunał stwierdził, że ustawodawstwo austriackie uniemożliwia austriackiemu urzędowi

198 *Tamże*, pkt 17 i 29.

199 *Tamże*, pkt 23.

200 *Tamże*, pkt 25.

201 *Tamże*, pkt 27.

202 TSUE, C-614/10, *Komisja Europejska przeciwko Republice Austrii*, 16 października 2012 r., pkt 59 i 63.

ochrony danych wykonywanie jego funkcji w sposób całkowicie niezależny w rozumieniu dyrektywy o ochronie danych. Niezależności austriackiego urzędu nie zagwarantowano w wystarczający sposób, gdyż Kancelaria Federalna zapewnia personel DSK, sprawuje nad nią nadzór i ma prawo do uzyskiwania w każdym czasie informacji o jej działaniach.

Przykład: W sprawie *Komisja Europejska przeciwko Węgrom*[203] TSUE 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 uznał także, iż „Węgry uchybiły zobowiązaniom, które na nich ciążą na mocy dyrektywy 95/46, w ten sposób, że skróciły kadencję organu nadzorczego ochrony danych osobowych [...]."

Organy nadzorcze dysponują na mocy prawa krajowego pewnymi uprawnieniami i możliwościami, między innymi mogą[204]:

- doradzać administratorom i osobom, których dane dotyczą, we wszystkich kwestiach związanych z ochroną danych;
- badać czynności przetwarzania i podejmować stosowne interwencje;
- ostrzegać lub upominać administratorów;
- nakazać poprawienie, zablokowanie, skasowanie lub zniszczenie danych;
- nałożyć czasowy lub ostateczny zakaz przetwarzania;
- skierować sprawę do sądu.

Aby móc wykonywać swoje funkcje, organ nadzorczy musi mieć dostęp do wszelkich danych osobowych i informacji niezbędnych dla prowadzonego dochodzenia, jak też dostęp do wszystkich pomieszczeń, w których administrator przechowuje stosowne informacje.

203 TSUE, C-288/12, *Komisja Europejska przeciwko Węgrom,* 8 kwietnia 2014 r., pkt 50 i 67.

204 Dyrektywa o ochronie danych, art. 28; zob. ponadto protokół dodatkowy do konwencji nr 108, art. 1.

Między jurysdykcjami występują znaczne różnice w odniesieniu do procedur i skutków prawnych ustaleń organu nadzorczego. Te ostatnie mogą wahać się od zaleceń podobnych do kierowanych przez rzeczników do decyzji o rygorze natychmiastowej wykonalności. W związku z tym przy analizie efektywności środków prawnych dostępnych w danej jurysdykcji instrumenty naprawcze trzeba oceniać w odpowiednim kontekście.

5.3. Środki prawne i sankcje

Najważniejsze kwestie

- Zgodnie z zarówno konwencją nr 108, jak i dyrektywą o ochronie danych w prawie krajowym trzeba określić odpowiednie środki prawne i sankcje w przypadku naruszenia prawa do ochrony danych.
    - W systemie UE potrzeba zapewnienia prawa do skutecznego środka prawnego skutkuje wymogiem określenia w prawie krajowym – niezależnie od możliwości zwrócenia się do organu nadzorczego – środków sądowych w przypadku naruszenia prawa do ochrony danych.
    - W prawie krajowym trzeba określić sankcje, które będą skuteczne, równoważne, proporcjonalne i odstraszające.
- Przed skierowaniem sprawy do sądu należy najpierw zwrócić się do administratora. Do prawa krajowego należy uregulowanie, czy przed skierowaniem sprawy do sądu obowiązkowe jest też zwrócenie się do organu nadzorczego.
- Osoby, których dane dotyczą, mogą kierować sprawy dotyczące naruszenia prawa o ochronie danych do ETPC – po wyczerpaniu wszystkich innych środków i pod pewnymi warunkami.
- Ponadto osoby, których dane dotyczą, mogą zwracać się do TSUE, ale tylko w niewielkiej liczbie przypadków.

Prawa wynikające z prawa o ochronie danych mogą być wykonywane tylko przez osobę, której prawa są zagrożone; chodzi tu o kogoś, kto jest osobą, której dane dotyczą, bądź przynajmniej twierdzi, że nią jest. Osoby takie mogą być reprezentowane w związku z wykonywaniem ich praw przez osoby, które spełniają niezbędne wymagania na mocy prawa krajowego. Osoby małoletnie muszą być reprezentowane przez rodziców lub opiekunów. Przed organami nadzorczymi osobę mogą też reprezentować stowarzyszenia, których celem statutowym jest promowanie prawa do ochrony danych.

5.3.1. Wnioski kierowane do administratora

Prawa, o których mowa jest w sekcji 3.2, należy wykonywać najpierw wobec administratora. Bezpośrednie zwrócenie się do krajowego organu nadzorczego lub sądu nie jest właściwe, gdyż organ mógłby jedynie wskazać, że najpierw należy zwrócić się do administratora, a sąd uznałby wniosek za niedopuszczalny. Wymogi formalne dotyczące skutecznego prawnie wniosku kierowanego do administratora, a zwłaszcza tego, czy musi on zostać skierowany w postaci pisemnej, powinny zostać uregulowane w prawie krajowym.

Podmiot, do którego zwrócono się jako do administratora, musi odpowiedzieć na wniosek, nawet jeżeli nie jest administratorem. Odpowiedź musi w każdym przypadku zostać dostarczona osobie, której dane dotyczą, w terminie określonym w prawie krajowym, nawet jeżeli stwierdza się w niej jedynie, że nie są przetwarzane dane o wnioskodawcy. Zgodnie z postanowieniami art. 12 lit. a) dyrektywy o ochronie danych i art. 8 lit. b) konwencji nr 108 wniosek taki musi zostać rozpatrzony „bez nadmiernego opóźnienia". W prawie krajowym należy zatem określić termin odpowiedzi, który będzie wystarczająco krótki, umożliwiając niemniej administratorowi należyte rozpatrzenie wniosku.

Przed udzieleniem odpowiedzi na wniosek podmiot, do którego zwrócono się jako do administratora, musi ustalić tożsamość wnioskodawcy w celu ustalenia, czy jest on rzeczywiście osobą, za którą się podaje, a tym samym uniknięcia poważnego naruszenia poufności. Jeżeli wymogi co do ustalenia tożsamości nie zostały szczegółowo uregulowane w prawie krajowym, decyzję ich dotyczącą musi podjąć administrator. Zasada rzetelnego przetwarzania wymaga jednak, aby administrator nie nakładał nadmiernie uciążliwych wymogów w zakresie identyfikacji (oraz autentyczności wniosku, o której mowa jest w sekcji 2.1.1).

W prawie krajowym trzeba również rozstrzygnąć kwestię tego, czy administrator, przed udzieleniem odpowiedzi na wnioski, może wymagać wniesienia opłaty przez wnioskodawcę: w art. 12 lit. a) dyrektywy o ochronie danych i art. 8 lit. b) konwencji nr 108 stwierdza się, że odpowiedź na wniosek o dostęp musi zostać udzielona „bez nadmiern[ych] [...] kosztów". W prawie wielu krajów Europy stwierdza się, że odpowiedzi na wnioski na mocy prawa o ochronie danych muszą być udzielane bezpłatnie, jeżeli odpowiedź nie wymaga nadmiernego i szczególnie dużego nakładu pracy; administratorzy są z kolei zazwyczaj chronieni prawem krajowym przed nadużywaniem prawa do uzyskania odpowiedzi na wnioski.

Jeżeli osoba, instytucja lub organ, do którego zwrócono się jako do administratora, nie zaprzecza, że nim jest, musi w terminie określonym w prawie krajowym:

- zaakceptować wniosek i zawiadomić wnioskodawcę, w jaki sposób zastosował się do niego; lub
- poinformować wnioskodawcę, dlaczego nie zastosował się do jego wniosku.

5.3.2. Skargi zgłaszane do organu nadzorczego

Gdy osoba, która złożyła wniosek o dostęp lub wniosła sprzeciw do administratora, nie otrzymała w terminie zadowalającej odpowiedzi, może ona zwrócić się do krajowego organu nadzorującego ochronę danych z wnioskiem o udzielenie pomocy. W trakcie postępowania przed organem nadzorczym należy wyjaśnić, czy osoba, instytucja lub organ, do którego zwrócił się wnioskujący, miał rzeczywiście obowiązek zareagować na wniosek oraz czy jego reakcja była prawidłowa i wystarczająca. Organ nadzorczy ma obowiązek poinformować osobę o wyniku postępowania dotyczącego jej wniosku[205]. Skutki prawne postępowania przed krajowymi organami nadzorczymi zależą od prawa krajowego: od tego, czy decyzje organu podlegają wykonaniu, co oznacza, że mogą być egzekwowane przez władze publiczne, czy też niezbędne jest zwrócenie się do sądu, jeżeli administrator nie postępuje zgodnie z decyzją (opinią, upomnieniem itp.) organu nadzorczego.

W przypadku gdy naruszenia prawa do ochrony danych zagwarantowanego na mocy art. 16 TFUE miały dopuścić się instytucje lub organy UE, osoba, której dane dotyczą, może złożyć skargę do EIOD[206] – niezależnego organu nadzorującego ochronę danych ustanowionego rozporządzeniem o ochronie danych przez instytucje UE, w którym to rozporządzeniu określono obowiązki i uprawnienia EIOD. W przypadku braku odpowiedzi EIOD w ciągu sześciu miesięcy uznaje się, że skarga została odrzucona.

Od decyzji krajowego organu nadzorczego musi istnieć możliwość odwołania się do sądu. Dotyczy to zarówno osoby, której dane dotyczą, jak i administratorów, którzy byli stroną postępowania przed organem nadzorczym.

205 Dyrektywa o ochronie danych, art. 28 ust. 4.

206 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 dniu 24 lipca 2013 r. Rzecznik Ochrony Informacji w Zjednoczonym Królestwie wydał skierowaną do policji hrabstwa Hertfordshire decyzję nakazującą zaprzestanie korzystania z systemu śledzenia tablic rejestracyjnych pojazdów, który uznał za niezgodny z prawem. Dane gromadzone przez kamery były przechowywane zarówno w lokalnych bazach danych policji, jak i w centralnej bazie danych. Zdjęcia tablic rejestracyjnych były przechowywane przez okres dwóch lat, a zdjęcia samochodów przez 90 dni. Uznano, że tak szerokie wykorzystanie kamer i innych form nadzoru nie jest proporcjonalne do problemu, który miało rozwiązać.

5.3.3. Skargi zgłaszane do sądu

Zgodnie z dyrektywą o ochronie danych jeżeli osoba, która złożyła wniosek do administratora na mocy prawa o ochronie danych, nie jest zadowolona z odpowiedzi administratora, musi jej przysługiwać uprawnienie do wniesienia skargi do sądu krajowego[207].

Do prawa krajowego należy uregulowanie, czy przed skierowaniem sprawy do sądu obowiązkowe jest zwrócenie się do organu nadzorczego. Jednak w większości przypadków zwrócenie się w pierwszej kolejności do organu nadzorczego jest korzystne dla osób wykonujących swoje prawa w zakresie ochrony danych, gdyż postępowanie związane z wnioskiem o pomoc powinno być niebiurokratyczne i bezpłatne. Wiedza specjalistyczna udokumentowana w decyzji organu nadzorczego (opinii, upomnieniu itp.) może także pomóc osobie, której dane dotyczą, w dochodzeniu swoich praw przed sądem.

Na mocy prawa RE naruszenia prawa do ochrony danych, których popełnienie zarzuca się na szczeblu krajowym umawiającej się strony EKPC i które stanowią jednocześnie naruszenie art. 8 EKPC, można dodatkowo zaskarżyć do ETPC po wyczerpaniu wszystkich dostępnych krajowych środków prawnych. Skargi na naruszenie art. 8 EKPC kierowane do ETPC muszą także spełniać inne kryteria dopuszczalności (art. 34–37 EKPC)[208].

Chociaż skargi do ETPC mogą być kierowane tylko przeciwko umawiającym się stronom, mogą one też wynikać pośrednio z działań lub zaniechań osób prywatnych w

207 Dyrektywa o ochronie danych, art. 22.

208 EKPC, art. 34–37, dokument dostępny pod adresem: www.echr.coe.int/Pages/home.aspx?p=caselaw/analysis&c=#n1347458601286_pointer.

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*[209] małoletni skarżący zarzucił, że w internetowym serwisie randkowym zamieszczono dotyczący go anons o charakterze seksualnym. Usługodawca nie ujawnił tożsamości osoby, która opublikowała informacje, ze względu na obowiązek zachowania poufności na mocy prawa fińskiego. Skarżący zarzucił, że prawo fińskie nie zapewnia wystarczającej ochrony przed takimi działaniami osoby prywatnej zamieszczającej kompromitujące skarżącego dane w internecie. 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 identyfikacji 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*[210] 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 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 państwo-strona naruszyło którekolwiek z praw chronionych na mocy EKPC, państwo-strona jest zobowiązane wykonać wyrok ETPC. 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.

209 ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2 grudnia 2008 r.

210 ETPC, *Köpke przeciwko Niemcom* (odrzucona), nr 420/07, 5 października 2010 r.

W przypadku gdy ETPC stwierdzi naruszenie EKPC, może zgodnie z art. 41 EKPC przyznać skarżącemu słuszne zadośćuczynienie na koszt państwa-strony.

Na mocy prawa UE[211] ofiary naruszenia krajowego prawa o ochronie danych, które wdraża prawo UE o ochronie danych, mogą w niektórych przypadkach wnieść sprawę do TSUE. Istnieją dwa przypadki, w których skarga osoby, której dane dotyczą, że zostało naruszone jej prawo do ochrony danych, może prowadzić do postępowania przed TSUE.

W pierwszym przypadku osoba, której dane dotyczą, musi być bezpośrednio pokrzywdzona aktem administracyjnym lub regulacyjnym UE, który narusza prawa jednostki do ochrony danych. Zgodnie z art. 263 akapit 4 TFUE:

> *„Każda osoba fizyczna lub prawna może wnieść [...] skargę na akty, których jest adresatem lub które dotyczą jej bezpośrednio i indywidualnie oraz na akty regulacyjne, które dotyczą jej bezpośrednio i nie obejmują środków wykonawczych".*

Tak więc osoby będące ofiarami niezgodnego z prawem przetwarzania danych przez organ UE mogą wnieść skargę bezpośrednio do Sądu TSUE, który jest ciałem właściwym do rozstrzygania w sprawach rozporządzenia o ochronie danych przez instytucje UE. Możliwość wniesienia skargi bezpośrednio do TSUE istnieje także, jeżeli przepis prawny UE wpływa bezpośrednio na sytuację prawną danej osoby.

Drugi przypadek ma związek z właściwością TSUE (Trybunału Sprawiedliwości) do orzekania w trybie prejudycjalnym zgodnie z art. 267 TFUE.

Osoby, których dane dotyczą, mogą podczas postępowania krajowego zwrócić się do sądu krajowego z wnioskiem, aby ten zwrócił się do Trybunału Sprawiedliwości o wyjaśnienie w sprawie wykładni traktatów UE oraz w sprawach dotyczących 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.

211 UE (2007), Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską podpisany w Lizbonie dnia 13 grudnia 2007 r., Dz.U. C 306 z 17.12.2007. Zob. też skonsolidowane wersje Traktatu o Unii Europejskiej, Dz.U. C 326 z 26.10.2012 i TFUE, Dz.U. C 326 z 26.10.2012.

Jeżeli strona w postępowaniu przed sądem krajowym wnosi o skierowanie pytania do TSUE, obowiązek zastosowania się do wniosku mają tylko sądy krajowe stanowiące ostatnią instancję, której orzeczenia nie podlegają zaskarżeniu.

Przykład: W sprawie *Kärntner Landesregierung i inni*[212] austriacki Trybunał Konstytucyjny zadał TSUE pytania dotyczące ważności art. 3–9 dyrektywy 2006/24/WE (dyrektywy o zatrzymywaniu danych) w świetle art. 7, 9 i 11 karty praw podstawowych oraz tego, czy pewne przepisy austriackiej ustawy federalnej o telekomunikacji transponującej dyrektywę o zatrzymywaniu danych są niezgodne z pewnymi aspektami dyrektywy o ochronie danych oraz rozporządzenia o ochronie danych przez instytucje UE.

Jeden ze skarżących w postępowaniu toczącym się przed Trybunałem Konstytucyjnym, p. 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. P. Seitlinger zdaje sobie sprawę, że takie gromadzenie i przechowywanie jego danych osobowych nie jest w żaden sposób niezbędne do celów technicznych związanych z przesłaniem informacji z punktu A do punktu B w sieci. Gromadzenie i przechowywanie tych danych nie jest też w żadnej mierze niezbędne do celów rozliczeń. P. Seitlinger nie udzielił w żadnym wypadku zgody na takie wykorzystanie jego danych osobowych. Jedynym powodem gromadzenia i przechowywania wszystkich tych dodatkowych danych była austriacka ustawa o telekomunikacji z 2003 r.

P. 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.

TSUE orzeka jedynie w przedmiocie elementów skierowanego do niego wniosku o wydanie orzeczenia w trybie prejudycjalnym. Pierwotną sprawę rozstrzyga natomiast sąd krajowy.

212 TSUE, sprawy połączone C-293/12 oraz C-594/12, *Digital Rights Ireland i Seitling i inni,* 8 kwietnia 2014 r.

Co do zasady Trybunał Sprawiedliwości musi odpowiedzieć na zadane mu pytania. Nie może on 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.

Wreszcie, jeżeli prawa do ochrony danych zagwarantowane na mocy art. 16 TFUE są rzekomo naruszane przez instytucję lub organ UE w trakcie przetwarzania danych osobowych, osoba, której dane dotyczą, może wnieść sprawę przed Sąd TSUE (art. 32 ust. 1 i 4 rozporządzenia o ochronie danych przez instytucje UE). To samo dotyczy decyzji EIOD w sprawie takich naruszeń (art. 32 ust. 3 rozporządzenia o ochronie danych przez instytucje UE).

Chociaż Sąd TSUE jest właściwy do rozstrzygania w sprawach rozporządzenia o ochronie danych przez instytucje UE, jeżeli środek prawny dotyczy osoby będącej pracownikiem instytucji lub organu UE, osoba ta musi wnieść skargę do Sądu do spraw Służby Publicznej Unii Europejskiej.

Przykład: Sprawa *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*[213] ilustruje środki prawne dostępne w przypadku działań lub decyzji instytucji i organów UE odnoszących się do ochrony danych.

Spółka Bavarian Lager zwróciła do Komisji Europejskiej z wnioskiem o dostęp do pełnego protokołu spotkania zorganizowanego przez Komisję i dotyczącego rzekomo kwestii prawnych istotnych dla spółki. Komisja odrzuciła wniosek spółki o dostęp ze względu na nadrzędny interes ochrony danych[214]. Na podstawie art. 32 rozporządzenia o ochronie danych przez instytucje UE spółka Bavarian Lager wniosła przeciwko tej decyzji skargę do TSUE, a konkretnie do Sądu Pierwszej Instancji (poprzednika Sądu). Wyrokiem w sprawie T-194/04 *Bavarian Lager przeciwko Komisji* Sąd Pierwszej Instancji stwierdził nieważność decyzji Komisji o odrzuceniu wniosku o dostęp. Komisja Europejska odwołała się od tego wyroku do Trybunału Sprawiedliwości. Zasiadając jako Wielka Izba, Trybunał Sprawiedliwości uchylił wyrok Sądu Pierwszej Instancji i potwierdził odmowę Komisji Europejskiej dotyczącą wniosku o dostęp.

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

214 Analizę sprawy można znaleźć w dokumencie: EDPS (2011), *Public access to documents containing personal data after the* Bavarian Lager *ruling* [„Dostęp publiczny do dokumentów zawierających dane osobowe po orzeczeniu *Bavarian Lager*"], Bruksela, EIOD, dokument dostępny pod adresem: www.secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/Publications/Papers/BackgroundP/11-03-24_Bavarian_Lager_EN.pdf.

5.3.4. Sankcje

Jeżeli chodzi o prawo RE, zgodnie z art. 10 konwencji nr 108 każda ze stron ma obowiązek wprowadzić odpowiednie sankcje karne i środki prawne w przypadku naruszenia przepisów prawa wewnętrznego wprowadzających w życie podstawowe zasady ochrony danych ustanowione w konwencji nr 108[215]**. Jeżeli chodzi o prawo UE**, w art. 24 dyrektywy o ochronie danych stwierdza się, że państwa członkowskie „przyjmą odpowiednie środki w celu zapewnienia pełnej realizacji przepisów niniejszej dyrektywy oraz w szczególności określą sankcje, jakie należy nałożyć w przypadku naruszenia przepisów przyjętych […]".

Obydwa akty prawne dają państwom członkowskim szeroki zakres swobody w wyborze odpowiednich sankcji i środków prawnych. W żadnym z nich nie zawarto konkretnych wskazówek dotyczących charakteru lub rodzaju odpowiednich sankcji ani też nie podano przykładów takich sankcji.

Jednakże:

> *„mimo że państwa członkowskie UE dysponują pewnym zakresem swobody w określeniu, jakie środki są najbardziej odpowiednie dla zabezpieczenia praw przysługujących jednostkom na mocy prawa UE, zgodnie z zasadą lojalnej współpracy określoną w art. 4 ust. 3 TUE należy przestrzegać minimalnych wymagań w zakresie skuteczności, równoważności, proporcjonalności i odstraszania"*[216].

TSUE wielokrotnie powtarzał, że nie istnieje całkowita swoboda określenia sankcji w prawie krajowym.

Przykład: W sprawie *Von Colson i Kamann przeciwko Land Nordrhein-Westfalen*[217] TSUE wskazał, że wszystkie państwa członkowskie, do których skierowana jest dyrektywa, są zobowiązane do przyjęcia w swoich krajowych systemach prawnych wszelkich niezbędnych środków w celu zapewnienia jej

215 ETPC, *I. przeciwko Finlandii*, nr 20511/03, 17 lipca 2008 r.; ETPC, *K.U. przeciwko Finlandii*, nr 2872/02, 2 grudnia 2008 r.

216 FRA (2012), *Opinion of the European Union Agency for Fundamental Rights on the proposed data protection reform package* [„Opinia Agencji Praw Podstawowych Unii Europejskiej na temat proponowanego pakietu dotyczącego reform w zakresie ochrony danych"], 2/2012, Wiedeń, 1 października 2012 r., s. 27.

217 TSUE, C-14/83, *Sabine von Kolson i Elisabeth Kammann przeciwko Land Nordrhein-Westfalan,* 10 kwietnia 1984 r.

pełnej skuteczności zgodnie z celem, który realizuje dyrektywa. Trybunał uznał, że chociaż wybór sposobów i środków zapewniających wdrożenie dyrektywy należy do państw członkowskich, swoboda ta nie wpływa na nałożone na nie obowiązki. W szczególności niezbędne są skuteczne środki prawne umożliwiające jednostce dochodzenie i egzekwowanie danego prawa w pełnym zakresie. Aby zapewnić prawdziwą i skuteczną ochronę, środki prawne muszą skutkować postępowaniami karnymi i/lub odszkodowawczymi prowadzącymi do sankcji mających odstraszający skutek.

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 [...]".

6

Transgraniczny przepływ danych

UE	Omówione zagadnienia	RE
Transgraniczny przepływ danych		
Artykuł 25 ust. 1 dyrektywy o ochronie danych TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.	Definicja	Artykuł 2 ust. 1 protokołu dodatkowego do konwencji nr 108
Swobodny przepływ danych		
Artykuł 1 ust. 2 dyrektywy o ochronie danych	Między państwami członkowskimi UE	
	Między umawiającymi się stronami konwencji nr 108	Artykuł 12 ust. 2 konwencji nr 108
Artykuł 25 dyrektywy o ochronie danych	Do państw trzecich o prawidłowym stopniu ochrony danych	Artykuł 2 ust. 1 protokołu dodatkowego do konwencji nr 108
Artykuł 26 ust. 1 dyrektywy o ochronie danych	Do państw trzecich w konkretnych przypadkach	Artykuł 2 ust. 2 lit. a) protokołu dodatkowego do konwencji nr 108
Ograniczony przepływ danych do państw trzecich		
Artykuł 26 ust. 2 dyrektywy o ochronie danych Artykuł 26 ust. 4 dyrektywy o ochronie danych	Klauzule umowne	Artykuł 2 ust. 2 lit. b) protokołu dodatkowego do konwencji nr 108 Wskazówki dotyczące sporządzania klauzul umownych

UE	Omówione zagadnienia	RE
Artykuł 26 ust. 2 dyrektywy o ochronie danych	Wiążące reguły korporacyjne	
Przykłady: Umowa PNR UE-USA Umowa SWIFT UE-USA	Specjalne umowy międzynarodowe	

W dyrektywie o ochronie danych zawarto nie tylko przepisy dotyczące swobodnego przepływu danych między państwami członkowskimi, ale także przepisy dotyczące wymagań w odniesieniu do przekazywania danych osobowych do państw trzecich spoza UE. RE również uznała znaczenie przepisów wykonawczych dotyczących transgranicznego przepływu danych do państw trzecich i przyjęła w 2001 r. protokół dodatkowy do konwencji nr 108. W protokole powtórzono najważniejsze elementy regulacji dotyczących transgranicznego przepływu danych od stron konwencji i państw członkowskich UE.

6.1. Charakter transgranicznego przepływu danych

Najważniejsze kwestie

- Transgraniczny przepływ danych to przekazanie danych osobowych do odbiorcy, który podlega jurysdykcji zagranicznej.

W art. 2 ust. 1 protokołu dodatkowego do konwencji nr 108 transgraniczny przepływ danych określa się jako przekazanie danych osobowych do odbiorcy, który podlega jurysdykcji zagranicznej. W art. 25 ust. 1 dyrektywy o ochronie danych reguluje się „przekazywanie do państwa trzeciego danych osobowych poddawanych przetwarzaniu lub przeznaczonych do przetwarzania po ich przekazaniu […]". Takie przekazywanie danych jest dopuszczalne tylko na zasadach określonych w art. 2 protokołu dodatkowego do konwencji nr 108, a w przypadku państw członkowskich UE dodatkowo w art. 25 i 26 dyrektywy o ochronie danych.

Przykład: W sprawie *Bodil Lindqvist*[218] TSUE uznał, 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".

Trybunał wskazał następnie, że w dyrektywie ustanowiono również szczegółowe przepisy mające na celu umożliwienie państwom członkowskim monitorowanie przekazywania danych osobowych do państw trzecich.

Uwzględniając jednak, po pierwsze, stan rozwoju internetu w okresie trwania prac nad dyrektywą, a po drugie, brak w dyrektywie kryteriów mających zastosowanie do korzystania z internetu, „nie można przypisać prawodawcy wspólnotowemu zamiaru objęcia w przyszłości pojęciem przekazywania danych do państw trzecich faktu zamieszczenia [...] danych na stronie internetowej, nawet jeżeli stały się one w ten sposób dostępne dla osób znajdujących się w państwach trzecich i posiadających środki techniczne pozwalające na dostęp do nich".

W przeciwnym razie, gdyby dyrektywę „interpretować w ten sposób, że »przekazywanie danych do państw trzecich« ma miejsce w każdym przypadku, w którym dane osobowe zostały umieszczone na stronie internetowej, to przekazywanie stanowiłoby w sposób konieczny przekazywanie do wszystkich państw trzecich, w których istnieją środki techniczne niezbędne do uzyskania dostępu do internetu. Szczególny system przewidziany [w dyrektywie] stałby się nieuchronnie – w odniesieniu do operacji w internecie – systemem ogólnym. W rezultacie, gdyby Komisja stwierdziła [...], że tylko jedno państwo trzecie nie zapewnia odpowiedniego stopnia ochrony, państwa członkowskie byłyby zobowiązane uniemożliwić jakiekolwiek zamieszczanie danych osobowych w internecie".

Zasada, że samej publikacji danych (osobowych) nie należy traktować jako transgranicznego przepływu danych, ma zastosowanie również do publicznych rejestrów online lub środków masowego przekazu, takich jak (elektroniczne) gazety i

218 TSUE, C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r., pkt 27, 68 i 69.

telewizja. Jedynie komunikacja skierowana do konkretnych odbiorców wchodzi w zakres pojęcia „transgranicznego przepływu danych".

6.2. Swobodny przepływ danych między państwami członkowskimi lub między umawiającymi się stronami

Najważniejsze kwestie

- Przekazanie danych osobowych do innego państwa członkowskiego Europejskiego Obszaru Gospodarczego lub innej umawiającej się strony konwencji nr 108 musi być wolne od ograniczeń.

Zgodnie z art. 12 ust. 2 konwencji nr 108 na **mocy prawa RE** musi istnieć swobodny przepływ danych osobowych między stronami konwencji. Prawo krajowe nie może ograniczać przekazania danych osobowych do umawiającej się strony, chyba że:

- wymaga tego szczególny charakter tych danych[219]; lub
- ograniczenie jest konieczne, aby nie dopuścić do obejścia krajowych przepisów prawnych dotyczących transgranicznego przepływu danych do stron trzecich[220].

Na mocy prawa UE ograniczenia lub zakazy dotyczące swobodnego przepływu danych między państwami członkowskimi ze względu na ochronę danych są zabronione zgodnie z art. 1 ust. 2 dyrektywy o ochronie danych. Obszar swobodnego przepływu danych poszerzono na mocy Porozumienia o Europejskim Obszarze Gospodarczym (EOG)[221], które włączyło do rynku wewnętrznego Islandię, Liechtenstein i Norwegię.

Przykład: Jeżeli podmiot stowarzyszony międzynarodowej grupy prowadzącej działalność w kilku państwach członkowskich UE, w tym w Słowenii i we Francji,

219 Konwencja nr 108, art. 12 ust. 3 lit. a).

220 *Tamże*, art. 12 ust. 3 lit. b).

221 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.

przekazuje dane osobowe ze Słowenii do Francji, krajowe prawo słoweńskie nie może ograniczać ani zakazywać takiego przepływu danych.

Jeżeli jednak ten sam słoweński podmiot stowarzyszony pragnie przekazać te same dane osobowe spółce dominującej w Stanach Zjednoczonych, słoweński podmiot przekazujący dane musi postępować zgodnie z procedurą określoną w prawie słoweńskim w odniesieniu do transgranicznego przepływu danych do państw trzecich niezapewniających prawidłowej ochrony danych, chyba że spółka dominująca przestrzega zasad ochrony prywatności w ramach „bezpiecznej przystani" (ang. Safe Harbor Privacy Principles) – dobrowolnego kodeksu postępowania w zakresie zapewnienia prawidłowego stopnia ochrony danych (zob. sekcję 6.3.1).

Transgraniczny przepływ danych do państw członkowskich EOG w celach wychodzących poza zakres rynku wewnętrznego, np. w celach dochodzeń karnych, nie podlega jednak przepisom dyrektywy o ochronie danych, a zatem nie jest objęty zasadą swobodnego przepływu danych. Jeżeli chodzi o prawo RE, konwencja nr 108 oraz protokół dodatkowy do konwencji nr 108 obejmują wszystkie obszary, chociaż umawiające się strony mogą dokonać wyłączeń. Wszystkie państwa członkowskie EOG są również stronami konwencji nr 108.

6.3. Swobodny przepływ danych do państw trzecich

Najważniejsze kwestie

- Przekazywanie danych osobowych do państw trzecich jest wolne od ograniczeń na mocy krajowego prawa o ochronie danych, jeżeli:
  - stwierdzono, że odbiorca zapewnia prawidłową ochronę danych; lub
  - jest ono konieczne ze względu na określony interes osoby, której dane dotyczą, lub uzasadniony interes ogólny innych, zwłaszcza z uwagi na ważny interes publiczny.
- Prawidłowy stopień ochrony danych w państwie trzecim oznacza, że w prawie krajowym tego państwa zostały skutecznie wdrożone podstawowe zasady ochrony danych.

- Na mocy prawa UE prawidłowość ochrony danych w państwie trzecim podlega ocenie Komisji Europejskiej. W prawie RE sposób oceny prawidłowości pozostawiono do uregulowania w prawie krajowym.

6.3.1. Swobodny przepływ danych ze względu na prawidłową ochronę

W prawie RE dopuszcza się umożliwienie w prawie krajowym swobodnego przepływu danych do państw niebędących stronami umawiającymi się, jeżeli docelowe państwo lub organizacja zapewnia prawidłowy stopień ochrony danych, które mają zostać przekazane[222]. Sposób oceny stopnia ochrony danych w innym kraju oraz podmiot dokonujący oceny są określane w prawie krajowym.

Na mocy prawa UE swobodny przepływ danych do państw trzecich zapewniających prawidłowy stopień ochrony danych przewidziano w art. 25 ust. 1 dyrektywy o ochronie danych. Wymóg prawidłowości zamiast równoważności umożliwia uznanie różnych sposobów wdrożenia ochrony danych. Zgodnie z art. 25 ust. 6 dyrektywy do oceny stopnia ochrony danych w innych krajach właściwa jest Komisja Europejska, która dokonuje sprawdzenia jej prawidłowości i konsultuje się w sprawie oceny z Grupą Roboczą Art. 29, która wniosła znaczny wkład w wykładnię art. 25 i 26[223].

Ustalenie prawidłowości dokonane przez Komisję Europejską ma charakter wiążący. Po publikacji przez Komisję Europejską ustalenia prawidłowości dotyczącego danego kraju w Dzienniku Urzędowym Unii Europejskiej wszystkie kraje członkowskie EOG i ich organy mają obowiązek zastosować się do tej decyzji, co oznacza, że dane mogą przepływać do tego kraju bez procedur sprawdzających lub uzyskiwania pozwoleń przed organami krajowymi[224].

222 Protokół dodatkowy do konwencji nr 108, art. 2 ust. 1.

223 Zob. na przykład Grupa Robocza Art. 29 (2003), *Working document on transfers of personal data to third countries: applying Article 26 (2) of the EU Data Protection Directive to binding corporate rules for international data transfers* [„Dokument roboczy w sprawie przekazywania danych osobowych do państw trzecich: zastosowanie art. 26 ust. 2 dyrektywy o ochronie danych do wiążących reguł korporacyjnych w odniesieniu do przekazywania danych za granicę"], WP 74, Bruksela, 3 czerwca 2003 r.; oraz Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*, WP 114, Bruksela, 25 listopada 2005 r.

224 Stale aktualizowana lista krajów, w odniesieniu do których dokonano ustalenia prawidłowości, znajduje się na stronie Dyrekcji Generalnej ds. Sprawiedliwości Komisji Europejskiej pod adresem: http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm.

Komisja Europejska może także oceniać elementy systemu prawnego danego kraju bądź ograniczyć się do konkretnych zagadnień. Komisja dokonała na przykład ustalenia prawidłowości odnoszącego się wyłącznie do prywatnego prawa handlowego Kanady[225]. Wydała także kilka ustaleń prawidłowości odnoszących się do przekazywania danych na podstawie umów między UE a innymi państwami. Decyzje te odnoszą się wyłącznie do jednego rodzaju przekazywania danych, np. przekazywania danych dotyczących przelotu pasażera przez linie lotnicze zagranicznym organom kontroli granicznej przy lotach z UE na niektóre lotniska zagraniczne (zob. sekcję 6.4.3). Stosowana ostatnio praktyka przekazywania danych na podstawie specjalnych umów między UE a państwami trzecimi generalnie eliminuje potrzebę ustalenia prawidłowości przy założeniu, że sama umowa zapewnia prawidłowy stopień ochrony danych[226].

Jedna z najważniejszych decyzji o prawidłowości nie odnosi się w rzeczywistości do zbioru przepisów prawnych[227], lecz do przypominających kodeks postępowania zasad znanych pod nazwą zasad ochrony prywatności w ramach „bezpiecznej przystani' (ang. *Safe Harbor Privacy Principles*). UE i USA wspólnie wypracowały te zasady w odniesieniu do amerykańskich przedsiębiorstw. Przystąpienie do programu bezpiecznej przystani polega na złożeniu Departamentowi Handlu USA dobrowolnego zobowiązania, które zostaje udokumentowane w wykazie publikowanym przez Departament. Jednym z ważnych elementów prawidłowości jest skuteczne wdrożenie ochrony danych, więc w zasadach bezpiecznej przystani przewidziano także pewien nadzór ze strony państwa: do systemu zasad przystąpić mogą tylko przedsiębiorstwa podlegające nadzorowi Federalnej Komisji Handlu USA.

225 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.

226 Na przykład Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Dz.U. L 215 z 11.8.2012, s. 5–14; lub Umowa 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 8 z 13.1.2010, s. 11–16.

227 Komisja Europejska (2000), 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.

6.3.2. Swobodny przepływ danych w określonych przypadkach

Na mocy prawa RE w art. 2 ust. 2 protokołu dodatkowego do konwencji 108 zezwala się na przekazywanie danych osobowych do państw trzecich, w których nie zapewniono prawidłowej ochrony danych, o ile ich przekazanie przewidziano w prawie krajowym i jest ono niezbędne ze względu na:

- określony interes osoby, której dane dotyczą; lub
- uzasadniony interes ogólny, zwłaszcza z uwagi na ważny interes publiczny.

Na mocy prawa UE w art. 26 ust. 1 dyrektywy o ochronie danych zawarto przepisy podobne do zapisanych w protokole dodatkowym do konwencji nr 108.

Na mocy dyrektywy interes osoby, której dane dotyczą, może uzasadniać swobodny przepływ danych do państwa trzeciego, jeżeli:

- osoba, której dane dotyczą, udzieliła jednoznacznej zgody na przekazanie danych; lub
- osoba, której dane dotyczą, weszła – lub przygotowuje się do wejścia – w stosunek umowny, który w oczywisty sposób wymaga przekazania danych do odbiorcy za granicą; lub
- zawarto umowę między administratorem danych a stroną trzecią w interesie osoby, której dane dotyczą; lub
- przekazanie jest konieczne dla ochrony żywotnych interesów osoby, której dane dotyczą;
- w przypadku przekazywania danych z rejestrów publicznych jest to przypadek, w którym ogólnym interesem społecznym jest możliwość dostępu do informacji przechowywanych w rejestrach publicznych.

Uzasadnione interesy innych osób mogą uzasadniać swobodny transgraniczny przepływ danych[228]:

228 Dyrektywa o ochronie danych, art. 26 ust. 1 lit. d).

- z ważnych względów publicznych innych niż bezpieczeństwo narodowe lub publiczne, gdyż te zagadnienia nie wchodzą w zakres dyrektywy o ochronie danych; lub

- w celu ustanowienia, wykonania lub obrony tytułu prawnego.

Przypadki, o których mowa jest powyżej, należy rozumieć jako wyłączenia od zasady, że swobodne przekazywanie danych do innych krajów wymaga prawidłowego stopnia ochrony danych w kraju odbiorcy. Wyłączenia muszą zawsze być interpretowane w sposób zawężający. Wielokrotnie podkreślała to Grupa Robocza Art. 29 w związku z art. 26 ust. 1 dyrektywy o ochronie danych, w szczególności jeżeli podstawę przekazania danych ma stanowić zgoda[229]. Grupa Robocza Art. 29 stwierdziła, że ogólne przepisy dotyczące znaczenia prawnego zgody mają zastosowanie również do art. 26 ust. 1 dyrektywy. Jeżeli – na przykład w kontekście stosunku pracy – nie jest oczywiste, że zgoda wyrażona przez pracowników miała rzeczywiście charakter dobrowolny, do przekazania danych nie może dojść na podstawie art. 26 ust. 1 lit. a) dyrektywy. W takich przypadkach zastosowanie ma art. 26 ust. 2, w którym wymaga się, aby pozwolenie na przekazanie danych wydały krajowe organy ochrony danych.

6.4. Ograniczony przepływ danych do państw trzecich

Najważniejsze kwestie

- Przed przekazaniem danych do państw trzecich, które nie zapewniają prawidłowego stopnia ochrony danych, administrator może być zobowiązany do przedstawienia planowanego przepływu danych do oceny organu nadzorczego.

- Administrator, który chce przekazać dane do państwa trzeciego, musi podczas tej oceny wykazać, że:

  - istnieje podstawa prawna przekazania danych odbiorcy; oraz

  - wdrożono środki w celu zapewnienia prawidłowej ochrony danych u odbiorcy.

229 Zob. zwłaszcza Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*, WP 114, Bruksela, 25 listopada 2005 r.

- Środki mające na celu ustanowienie prawidłowej ochrony danych u odbiorcy mogą obejmować:
  - postanowienia umowne między przekazującym dane administratorem a odbiorcą zagranicznym; lub
  - wiążące reguły korporacyjne, zwykle stosowane w przypadku przekazywania danych w obrębie wielonarodowych grup.
- Przekazywanie danych organom zagranicznym może też następować na podstawie specjalnych umów międzynarodowych.

W dyrektywie o ochronie danych i protokole dodatkowym do konwencji nr 108 zezwolono na ustanowienie w prawie krajowym zasad transgranicznego przepływu danych do państw trzecich niezapewniających prawidłowego stopnia ochrony danych, o ile administrator wdrożył specjalne rozwiązania w celu zapewnienia prawidłowych zabezpieczeń służących ochronie danych u odbiorcy i o ile administrator potrafi to wykazać wobec właściwego organu. Wymóg ten wyraźnie wskazano tylko w protokole dodatkowym do konwencji nr 108, jest on jednak także uważany za standardową procedurę na mocy dyrektywy o ochronie danych.

6.4.1. Klauzule umowne

Zarówno **w prawie RE**, jak i **w prawie UE** jest mowa o klauzulach umownych między administratorem dokonującym przekazania danych i odbiorcą w państwie trzecim jako możliwym sposobie zapewnienia wystarczającego stopnia ochrony danych u odbiorcy.

Na **szczeblu UE** Komisja Europejska z pomocą Grupy Roboczej Art. 29 wypracowała standardowe klauzule umowne, które zostały oficjalnie uznane decyzją Komisji za dowód prawidłowej ochrony danych[230]. Jako że decyzje Komisji są w całości wiążące w państwach członkowskich, organy krajowe odpowiedzialne za nadzorowanie transgranicznego przepływu danych muszą uwzględnić te standardowe klauzule umowne w swoich procedurach[231]. 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 prawidłowe zabezpieczenia.

230 Dyrektywa o ochronie danych, art. 26 ust. 4.

231 TFUE, art. 288.

Istnienie standardowych klauzul umownych w ramach prawnych UE nie uniemożliwia administratorom sformułowania innych doraźnych klauzul umownych. Muszą one jednak skutkować takim samym stopniem ochrony, jak zapewniany przez standardowe klauzule umowne. 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;

- zgoda odbiorcy lub podmiotu odbierającego dane na poddanie się procedurom 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[232]. W przypadku przekazywania danych przez administratora podmiotowi przetwarzającemu dostępny jest tylko jeden zestaw standardowych klauzul umownych[233].

W kontekście **prawa RE** Komitet Konsultacyjny Konwencji nr 108 opracował wskazówki dotyczące sporządzania klauzul umownych[234].

232 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.

233 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.

234 RE, Komitet Konsultacyjny Konwencji 108 (2002*), Guide to the preparation of contractual clauses governing data protection during the transfer of personal data to third parties not bound by an adequate level of data protection* [„Wskazówki co do sporządzania klauzul umownych dotyczących ochrony danych podczas przekazywania danych osobowych stronom trzecim niezapewniającym prawidłowego stopnia ochrony danych"].

6.4.2. Wiążące reguły korporacyjne

Wielostronne wiążące reguły korporacyjne (WRK) bardzo często dotyczą jednocześnie kilku europejskich organów ochrony danych[235]. Aby WRK mogły zostać zatwierdzone, ich projekt należy przesłać wraz ze standardowymi formularzami wniosków do organu wiodącego[236]. Organ wiodący można zidentyfikować na podstawie standardowego formularza wniosku. Informuje on następnie wszystkie organy nadzorcze w państwach członkowskich EOG, w których działalność prowadzą podmioty stowarzyszone grupy, chociaż ich udział w procesie oceny WRK jest dobrowolny. Chociaż ocena ta nie ma charakteru wiążącego, wszystkie zainteresowane organy ochrony danych powinny uwzględnić jej wyniki w swoich formalnych procedurach udzielania zezwoleń.

6.4.3. Specjalne umowy międzynarodowe

UE zawarła specjalne umowy dotyczące dwóch rodzajów przekazywanych danych:

Dane dotyczące przelotu pasażera

Dane dotyczące przelotu pasażera (dane PNR) są gromadzone przez przewoźników lotniczych podczas procesu rezerwacyjnego i obejmują nazwiska, adresy, dane kart kredytowych oraz numery miejsc pasażerów. Na mocy prawa USA linie lotnicze są zobowiązane udostępnić te dane Departamentowi Bezpieczeństwa Wewnętrznego przed odlotem pasażerów. Wymóg ten odnosi się do lotów do Stanów Zjednoczonych lub z ich terytorium.

235 Treść i strukturę odpowiednich wiążących reguł korporacyjnych wyjaśniono w: Grupa Robocza Art. 29 (2008), *Working document setting up a framework for the structure of Binding Corporate Rules* [„Dokument roboczy ustanawiający ramy struktury wiążących reguł korporacyjnych"], WP 154, Bruksela, 24 czerwca 2008 r.; oraz Grupa Robocza Art. 29 (2008), *Working document setting up a table with the elements and principles to be found in Binding Corporate Rules* [„Dokument roboczy ustanawiający tabelę zawierającą elementy i zasady, które powinny zostać uwzględnione w wiążących regułach korporacyjnych"], WP 153, Bruksela, 24 czerwca 2008 r.

236 Grupa Robocza Art. 29 (2007), *Recommendation 1/2007 on the standard application for approval of binding corporate rules for the transfer of personal data* [„Rekomendacja nr 1/2007 w sprawie standardowego wniosku o zatwierdzenie wiążących reguł korporacyjnych w odniesieniu do przekazywania danych osobowych"], WP 133, Bruksela, 10 stycznia 2007 r.

W celu zapewnienia prawidłowej ochrony danych PNR zgodnie z przepisami dyrektywy 95/46/WE, w 2004 r. przyjęto 'pakiet PNR'[237]. Pakiet ten dotyczył prawidłowości przetwarzania danych prowadzonego przez Departament Bezpieczeństwa Wewnętrznego USA (DHS).

Po unieważnieniu przez TSUE pakietu PNR[238] UE i Stany zjednoczone podpisały dwie odrębne umowy mające dwojaki cel: po pierwsze, mają stanowić podstawę prawną udostępnienia danych PNR organom USA, a po drugie, mają ustanowić prawidłową ochronę w kraju odbiorcy.

Pierwsza umowa podpisana w 2012 r. między między krajami UE i Stanami Zjednoczonymi o sposobie udostępniania danych i zarządzania nimi została zastąpiona w tym samy roku inną umową w celu zapewnienia większej pewności prawnej[239]. Nowa umowa została znacząco udoskonalona. Ogranicza się w niej i wyjaśnia cele, dla których mogą być wykorzystywane informacje, takie jak zwalczanie poważnej przestępczości międzynarodowej i terroryzmu. W umowie określono okres przechowywania danych: po sześciu miesiącach dane należy zanonimizować. W przypadku niewłaściwego wykorzystania danych każdej osobie przysługuje prawo do administracyjnych i sądowych środków zaskarżenia zgodnie z prawem Stanów Zjednoczonych. Osoby mają też prawo dostępu do swoich danych PNR i ubiegania się o ich poprawienie przez Departament Bezpieczeństwa Wewnętrznego, w tym możliwość usunięcia danych, jeżeli informacje są niedokładne.

Umowa, która weszła w życie dnia 1 lipca 2012 r., pozostanie w mocy przez siedem lat, do 2019 r.

237 Decyzja Rady 2004/496/WE z 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dotyczących przelotu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic, Dz.U. L 183, str. 83, oraz decyzja Komisji 2004/535/WE z 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Ceł i Ochrony Granic Stanów Zjednoczonych, Dz.U. L 235, str. 11-22.

238 Sprawy połaczone TSUE C-317/04 I C-318/04, *Parlament Europejski przeciwko Radzie Unii Europejskiej*, 30 maja 2006 r. pkt. 57, 58 i 59, w którym Trybunał orzekł, że zarówno decyzja o prawidłowości, jak i umowa dotycząca przetwarzania danych są wyłączone z zakresu dyrektywy.

239 Decyzja Rady 2012/472/UE z dnia 26 kwietnia 2012 r. w sprawie zawarcia Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Dz.U. L 215 z 11.8.2012, s. 4. Tekst umowy dołączono do decyzji, Dz.U. L 215 z 11.8.2012, s. 5–14.

W grudniu 2011 r. Rada Unii Europejskiej zatwierdziła zawarcie zaktualizowanej umowy UE-Australia o przetwarzaniu i przekazywaniu danych PNR[240]. Umowa między UE a Australią w sprawie danych PNR jest kolejnym krokiem realizacji programu UE, który obejmuje globalne wytyczne w sprawie danych PNR[241], ustanowienie systemu UE-PNR[242] oraz wynegocjowanie umów z państwami trzecimi[243].

Dane z komunikatów finansowych

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 w związku z dochodzeniem dotyczącym terroryzmu[244].

240 Decyzja Rady 2012/381/UE z dnia 13 grudnia 2011 r. w sprawie zawarcia Umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), Dz.U. L 186 z 14.7.2012, s. 3. Tekst umowy, która zastąpiła poprzednią umowę z 2008 r., dołączono do decyzji, Dz.U. L 186 z 14.7.2012, s. 4–16.

241 Zob. w szczególności komunikat Komisji z dnia 21 września 2010 r. w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, COM(2010) 492 final, Bruksela, 21 września 2010 r. oraz *Opinia 7/2010 dotycząca komunikatu Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim*, WP 178, Bruksela, 12 listopada 2010 r.

242 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. W kwietniu 2011 r. Parlament Europejski zwrócił się do APP o wydanie opinii w sprawie tego wniosku i jego zgodności z Kartą praw podstawowych Unii Europejskiej. Zob.: FRA (2011), *Opinion 1/2011 – Passenger Name Record* [„Opinia 1/2011 – dane dotyczące przelotu pasażera"], Wiedeń, 14 czerwca 2011 r.

243 UE negocjuje obecnie nową umowę dotyczącą PNR z Kanadą, która zastąpi obecnie obowiązującą umowe z 2006 r. .

244 W tym kontekście zob. Grupa Robocza Art. 29 (2011), *Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing* [„Opinia 14/2001 w sprawie zagadnień ochrony danych związanych z przeciwdziałaniem praniu pieniędzy i finansowaniu 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* [„Procedura kontroli i wydania rekomendacji zainicjowana w odniesieniu do spółki SWIFT scrl"], decyzja, 9 grudnia 2008 r.

Z punktu widzenia UE nie było wystarczających podstaw prawnych ujawnienia tych danych o charakterze zasadniczo europejskim, które były dostępne w Stanach Zjednoczonych 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 zapewnić prawidłowy stopień ochrony danych[245].

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:

- identyfikuje dane finansowe w możliwie jasny sposób;
- wyraźnie uzasadnia konieczność udostępnienia danych;
- posiada zakres określony w możliwie wąski sposób, aby zminimalizować ilość wnioskowanych danych;
- nie odnosi się do żadnych danych dotyczących jednolitego obszaru płatności w euro (SEPA).

Europol musi otrzymać kopię każdego wniosku skierowanego przez Departament Skarbu USA i zweryfikować, czy zasady umowy SWIFT są przestrzegane[246]. 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. Generalnie dane finansowe

245 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.

246 Wspólny Organ Nadzorczy Europolu przeprowadza kontrole działań Europolu w tym obszarze, których wyniki dostępne są pod adresem: http://europoljsb.consilium.europa.eu/reports/inspection-report.aspx?lang=en.

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.

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 poprawienia, 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, do sierpnia 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.

7

Ochrona danych w kontekście współpracy policyjnej i sądowej w sprawach karnych

UE	Omówione zagadnienia	RE
	Ogólne	Konwencja nr 108
	Policja	Zalecenie w sprawie policji
		ETPC, *B.B. przeciwko Francji*, nr 5335/06, 17 grudnia 2009 r.
		ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu*, nr 30562/04 i 30566/04, 4 grudnia 2008 r.
		ETPC, *Vetter przeciwko Francji*, nr 59842/00, 31 maja 2005 r.
	Cyberprzestępczość	Konwencja o cyberprzestępczości
Ochrona danych w kontekście transgranicznej współpracy policji i organów wymiaru sprawiedliwości		
Decyzja ramowa o ochronie danych	Ogólne	Konwencja nr 108 Zalecenie w sprawie policji
Decyzja w sprawie konwencji z Prüm	W odniesieniu do danych specjalnych: odciski palców, DNA, chuligaństwo itp.	Konwencja nr 108 Zalecenie w sprawie policji
Decyzja w sprawie Europolu Decyzja w sprawie Eurojustu Rozporządzenie w sprawie Fronteksu	Przez specjalne agencje	Konwencja nr 108 Zalecenie w sprawie danych policyjnych

UE	Omówione zagadnienia	RE
Decyzja w sprawie Schengen II Rozporządzenie w sprawie VIS Rozporządzenie Eurodac Decyzja w sprawie CIS	Przez specjalne wspólne systemy informacji	Konwencja nr 108 Zalecenie w sprawie policji ETPC, *Dalea przeciwko Francji*, nr 964/07, 2 lutego 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.

7.1. Prawo RE o ochronie danych w kontekście działań policji i organów wymiaru sprawiedliwości w sprawach karnych

Najważniejsze kwestie

- Konwencja nr 108 i zalecenie w sprawie policji RE 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.

Na szczeblu europejskim konwencja nr 108 obejmuje wszystkie dziedziny przetwarzania danych osobowych, a jej postanowienia mają w zamierzeniu regulować całość przetwarzania danych osobowych. W związku z tym konwencja nr 108 ma zastosowanie do ochrony danych w kontekście działań policji i orgnów wymiaru sprawiedliwości w sprawach karnych, choć umawiające się strony mogą ograniczyć zakres jej zastosowania.

Zadania prawne policji i orgnaów wymiaru sprawiedliwości w sprawach karnych często wymagają przetwarzania danych osobowych, co może pociągać za sobą

poważne konsekwencje dla osób, których dane są przetwarzane. Przyjęte przez RE w 1987 r. zalecenie w sprawie danych policyjnych zawiera wskazówki dla umawiających się stron, w jaki sposób powinny wprowadzić w życie zasady konwencji nr 108 w związku z przetwarzaniem danych osobowych przez organy ścigania[247].

7.1.1. Zalecenie w sprawie policji

ETPC konsekwentnie uznaje, że przechowywanie i zatrzymywanie danych osobowych przez policję lub organy bezpieczeństwa narodowego stanowi ingerencję w art. 8 ust. 1 EKPC. Wiele wyroków ETPC dotyczy uzasadnienia takiej ingerencji[248].

Przykład: W sprawie *B.B. przeciwko Francji*[249] ETPC uznał, że art. 8 EKPC ma zastosowanie do umieszczenia osoby skazanej za przestępstwa seksualne w krajowej bazie danych sądowych. Uwzględniając jednak fakt, że wdrożono wystarczające zabezpieczenia służące ochronie danych, takie jak prawo osoby, której dane dotyczą, do żądania skasowania danych, ograniczony okres przechowywania danych i ograniczony dostęp do takich danych, właściwa równowaga między konkurencyjnymi interesami prywatnym i publicznym została zachowana. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *S. i Marper przeciwko Zjednoczonemu Królestwu*[250] 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. ETPC uznał, że ogólne, masowe przechowywanie danych osobowych, które nie jest ograniczone w czasie, przy jednoczesnym przyznaniu osobom uniewinnionym jedynie ograniczonych możliwości żądania ich usunięcia,

247 RE, Komitet Ministrów (1987), Recommendation Rec(87)15 to member states regulating the use of personal data in the police sector [„Zalecenie Rec(87)15 dla państw członkowskich regulujące wykorzystywanie danych osobowych przez policję"], 17 września 1987 r.

248 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.

249 ETPC, *B.B. przeciwko Francji*, nr 5335/06, 17 grudnia 2009 r.

250 ETPC, *S. i Marper przeciwko Zjednoczonemu Królestwu*, nr 30562/04 i 30566/04, 4 grudnia 2008 r., pkt 119 i 125.

stanowi nieproporcjonalną ingerencję w prawa skarżących do poszanowania życia prywatnego. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Wiele innych wyroków ETPC dotyczy uzasadnienia ingerencji w prawo do ochrony danych wynikającej z nadzoru.

Przykład: W sprawie *Allan przeciwko Zjednoczonemu Królestwu*[251] władze potajemnie nagrały prywatne rozmowy więźnia ze znajomym w sali odwiedzin oraz ze współoskarżonym w więziennej celi. ETPC 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 wykorzystanie przez policję tajnych urządzeń nagrywających, ingerencja ta nie była zgodna z prawem. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

Przykład: W sprawie *Klass i inni przeciwko Niemcom*[252] skarżący zarzucili, że pewne niemieckie akty prawne umożliwiające tajny nadzór nad pocztą i połączeniami telekomunikacyjnymi naruszają art. 8 EKPC, w szczególności dlatego, że zainteresowana osoba nie jest informowana o środkach nadzoru i nie może dochodzić swoich praw w sądzie po zakończeniu nadzoru przy użyciu takich środków. ETPC uznał, że groźba nadzoru z natury ingeruje w swobodę komunikacji między użytkownikami usług pocztowych i telekomunikacyjnych. Ustalił jednak, że wdrożono wystarczające zabezpieczenia przed nadużyciami. Niemiecki ustawodawca słusznie uznał takie środki za niezbędne w społeczeństwie demokratycznym w interesie bezpieczeństwa narodowego i dla zapobiegania zakłóceniu porządku lub przestępstwom. Trybunał stwierdził, że nie doszło do naruszenia art. 8 EKPC.

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 baz danych związanych z tym obszarem. W zaleceniu RE w sprawie 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 zagranicznym

251 ETPC, *Allan przeciwko Zjednoczonemu Królestwu*, nr 48539/99, 5 listopada 2002 r.

252 ETPC, *Klass i inni przeciwko Niemcom*, nr 5029/71, 6 września 1978 r.

organom policyjnym; sposobu wykonywania praw do ochrony danych przez osoby, których dane dotyczą; sposobu sprawowania kontroli przez niezależne organy. Uwzględniono także obowiązek zapewnienia prawidłowego stopnia bezpieczeństwa danych.

W zaleceniu nie dopuszcza się nieograniczonego, masowego gromadzenia danych 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. Wszelkie dodatkowe dane muszą być gromadzone na podstawie konkretnego ustawodawstwa krajowego. 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 w prowadzeniu dochodzenia. Gromadzenie danych wskutek nadzoru przy wykorzystaniu środków technicznych lub innych zautomatyzowanych środków powinno również opierać się na konkretnych przepisach.

Przykład: W sprawie *Vetter przeciwko Francji*[253] anonimowi świadkowie oskarżyli skarżącego o zabójstwo. Skarżący regularnie odwiedzał mieszkanie znajomego, więc policja zainstalowała tam za zgodą sędziego śledczego urządzenia podsłuchowe. Na podstawie zarejestrowanych rozmów skarżący został aresztowany i postawiono mu zarzut zabójstwa. Wniósł on o uznanie nagrania za dowód niedopuszczalny, podnosząc w szczególności, że nagrywanie nie zostało dopuszczone prawem. ETPC musiał rozstrzygnąć kwestię, czy wykorzystanie urządzeń podsłuchowych było „zgodne z prawem". Podsłuch prywatnych pomieszczeń w oczywisty sposób nie wchodził w zakres art. 100 i nast. francuskiego kodeksu postępowania karnego, gdyż przepisy te dotyczyły przechwytywania rozmów telefonicznych. W art. 81 kodeksu nie określono wystarczająco jasno zakresu swobody władz ani sposobu, w jaki mogą one z niego korzystać, dopuszczając monitorowanie prywatnych rozmów. W związku z tym skarżący nie dysponował minimalnym stopniem ochrony, który przysługuje obywatelom zgodnie z zasadami praworządności w demokratycznym społeczeństwie. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

253 ETPC, *Vetter przeciwko Francji*, nr 59842/00, 31 maja 2005 r.

W zaleceniu stwierdza się, że podczas przechowywania danych osobowych należy uczynić wyraźne rozróżnienie między: danymi administracyjnymi i danymi policyjnymi; różnymi rodzajami osób, których dane dotyczą, np. podejrzanymi, skazanymi, pokrzywdzonymi i świadkami; a także danymi uważanymi za fakty oraz opartymi na podejrzeniach lub przypuszczeniach.

Cele wykorzystania danych policyjnych powinny być ściśle ograniczone. Ma to konsekwencje dla przesyłania danych policyjnych stronom trzecim: przekazywanie lub przesyłanie takich danych w obrębie organów policyjnych powinno być uwarunkowane tym, czy istnieje uzasadniony interes w udostępnieniu informacji. Przekazywanie lub przesyłanie takich danych poza obręb organów policyjnych powinno być dopuszczalne tylko wtedy, gdy istnieje wyraźny obowiązek prawny lub upoważnienie. Przekazywanie lub przesyłanie danych za granicę 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 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, osobie, której dane dotyczą, musi na mocy prawa krajowego przysługiwać prawo odwołania się do krajowego organu nadzorującego ochronę danych lub do innego niezależnego organu.

7.1.2. 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 też RE przyjęła międzynarodowy akt prawny – konwencję o cyberprzestępczości, znaną również jako konwencję budapeszteńską – dotyczący przestępstw popełnianych przeciwko sieciom elektronicznym oraz z ich wykorzystaniem[254]. Do konwencji mogą przystąpić także państwa niebędące członkami Rady Europy; do połowy

254 Rada Europy, Komitet Ministrów (2001), Konwencja o cyberprzestępczości, CETS nr 185, Budapeszt, 23 listopada 2001 r., weszła w życie 1 lipca 2004 r.

2013 r. stronami konwencji stały się cztery państwa spoza RE – Australia, Republika Dominikany, Japonia i Stany Zjednoczone – a 12 innych państw niebędących członkami RE podpisało ją lub zostało zaproszone 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 hackingu 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, kryminalizuje ona działania mogące naruszać prawo osoby, której dane dotyczą, do ochrony swoich danych. 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[255].

7.2. Prawo UE o ochronie danych w kontekście działań policji i organów wymiaru sprawiedliwości w sprawach karnych

Najważniejsze kwestie

- Na szczeblu UE ochrona danych w obrębie policji i organów wymiaru sprawiedliwości w sprawach karnych została uregulowana jedynie w kontekście współpracy transgranicznej organów ścigania i wymiaru sprawiedliwości.

255 *Tamże, art.* 15 ust. 1.

- Istnieją specjalne zasady ochrony danych w odniesieniu do Europejskiego Urzędu Policji (Europol) i Europejskiej Jednostki Współpracy Sądowej (Eurojust), które są organami UE wspomagającymi i wspierającymi transgraniczną współpracę organów ścigania.
- Specjalne zasady ochrony danych obowiązują też w odniesieniu do wspólnych systemów informacyjnych, które ustanowiono na szczeblu UE w celu transgranicznej wymiany informacji między właściwymi organami policyjnymi i sądowymi. Ważnymi przykładami są Schengen II, wizowy system informacyjny (VIS) oraz Eurodac – scentralizowany system zawierający dane o odciskach palców obywateli państw trzecich ubiegających się o azyl w jednym z państw członkowskich UE.

Dyrektywa o ochronie danych nie ma zastosowania do organów policji i wymiaru sprawiedliwości w sprawach karnych. Najważniejsze akty prawne w tym obszarze opisano w sekcji 7.2.1.

7.2.1. Decyzja ramowa o ochronie danych

Celem decyzji ramowej Rady 2008/977/WSiSW w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (decyzji ramowej o ochronie danych)[256] jest zapewnienie ochrony danych osobowych osób fizycznych w sytuacji, gdy ich dane osobowe są przetwarzane w celu zapobiegania przestępstwom, prowadzenia dochodzeń w sprawach przestępstw, wykrywania lub ścigania przestępstw bądź wykonywania sankcji karnych. W imieniu państw członkowskich lub UE działają właściwe organy z obszaru policji i wymiaru sprawiedliwości w sprawach karnych. Organy te są agencjami lub organami UE, jak również organami państw członkowskich[257]. Zakres stosowania decyzji ramowej jest ograniczony do zapewnienia ochrony danych osobowych w związku ze współpracą transgraniczną między tymi organami i nie obejmuje bezpieczeństwa narodowego.

Decyzję ramową o ochronie danych oparto w dużym stopniu na zasadach i definicjach zawartych w konwencji nr 108 oraz dyrektywie o ochronie danych.

Dane mogą być wykorzystywane jedynie przez właściwy organ i tylko do celów, do których zostały przekazane lub udostępnione. Przyjmujące państwo członkowskie musi przestrzegać wszelkich ograniczeń wymiany danych przewidzianych w prawie przekazującego państwa członkowskiego. Pod pewnymi warunkami dopuszczalne

256 Rada Unii Europejskiej (2008), Decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (decyzja ramowa o ochronie danych), Dz.U. L 350 z 30.12.2008.

257 *Tamże*, art. 2 lit. h).

jest wszakże wykorzystanie danych w innym celu przez państwo przyjmujące. Rejestrowanie i dokumentowanie przypadków przekazania danych jest obowiązkiem właściwych władz, aby możliwe było określenie odpowiedzialności wynikającej ze skarg. Dalsze przekazywanie danych otrzymanych w ramach współpracy transgranicznej stronom trzecim wymaga zgody państwa członkowskiego, z którego pochodzą dane, choć w pilnych przypadkach istnieją wyłączenia od tej zasady.

Właściwe organy muszą podjąć niezbędne środki bezpieczeństwa w celu ochrony danych osobowych przed wszelkim niezgodnym z prawem przetwarzaniem.

Każde państwo członkowskie musi zapewnić, aby co najmniej jeden niezależny krajowy organ nadzorczy odpowiadał za prowadzenie doradztwa i monitorowania w zakresie stosowania przepisów przyjętych zgodnie z decyzją ramową. Taki organ ma również obowiązek rozpatrywać wnioski złożone przez dowolną osobę, dotyczące ochrony jej praw i swobód w odniesieniu do przetwarzania danych osobowych przez właściwe organy.

Osoba, której dane dotyczą, ma prawo do informacji na temat przetwarzania jej danych osobowych oraz ma prawo dostępu, poprawienia, usunięcia lub zablokowania tych danych. W przypadku gdy z istotnych przyczyn odmówiono jej skorzystania z tych praw, osobie, której dane dotyczą, musi przysługiwać prawo odwołania się do właściwego krajowego organu nadzorczego lub sądu. Jeżeli dana osoba poniosła szkody wskutek naruszenia przepisów prawa krajowego wdrażającego decyzję ramową o ochronie danych, osoba ta ma prawo do odszkodowania od administratora[258]. Generalnie osoby, których dane dotyczą, muszą mieć dostęp do środków sądowych w przypadku jakiegokolwiek naruszenia ich praw zagwarantowanych na mocy prawa krajowego wdrażającego decyzję ramową o ochronie danych[259].

Komisja Europejska zaproponowała reformę, która obejmuje wprowadzenie ogólnego rozporządzenia o ochronie danych[260] oraz ogólnej dyrektywy o ochronie

258 *Tamże*, art. 19.

259 *Tamże*, art. 20.

260 Komisja Europejska (2012), *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólnego rozporządzenia o ochronie danych)*, COM(2012) 11 final, Bruksela, 25 stycznia 2012 r.

danych[261]. Nowa dyrektywa zastąpi obecną decyzję ramową o ochronie danych i będzie zawierać ogólne zasady oraz przepisy dotyczące współpracy policyjnej i sądowej w sprawach karnych.

7.2.2. Bardziej szczegółowe akty prawne dotyczące ochrony danych w kontekście transgranicznej współpracy organów policyjnych i innych organów ścigania

Oprócz decyzji ramowej o ochronie danych wymiana informacji będących w posiadaniu państw członkowskich w poszczególnych obszarach jest regulowana innymi aktami prawnymi, takimi jak decyzja ramowa Rady 2009/315/WSiSW w sprawie organizacji wymiany informacji pochodzących z rejestru karnego pomiędzy państwami członkowskimi oraz treści tych informacji oraz decyzja Rady dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego Państw Członkowskich w odniesieniu do wymiany informacji[262].

Co istotne, współpraca transgraniczna[263] między właściwymi organami w coraz większym stopniu wiąże się z wymianą danych dotyczących imigracji. Ta dziedzina prawa nie ma bezpośredniego związku z policją i wymiarem sprawiedliwości w sprawach karnych, ale jest pod wieloma względami istotna dla pracy organów policji i wymiaru sprawiedliwości. To samo dotyczy danych na temat towarów przywożonych do UE lub wywożonych z niej. Zniesienie kontroli na granicach wewnętrznych UE 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.

261 Komisja Europejska (2012), *Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich i ścigania albo wykonywania kar kryminalnych oraz swobodnego przepływu tych danych (ogólnej dyrektywy o ochronie danych)*, COM(2012) 10 final, Bruksela, 25 stycznia 2012 r.

262 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.

263 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.

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 z Prüm*), na mocy której w 2008 r. włączono konwencję z Prüm do prawa UE[264]. Konwencja z Prüm była międzynarodową umową o współpracy policyjnej podpisaną w 2005 r. przez Austrię, Belgię, Francję, Niemcy, Luksemburg, Niderlandy i Hiszpanię[265].

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:

- automatycznego dostępu do profili DNA, danych daktyloskopijnych i niektórych krajowych danych rejestracyjnych pojazdów;
- dostarczania danych w związku z istotnymi wydarzeniami rangi międzynarodowej;
- dostarczania informacji służących zapobieganiu przestępstwom terrorystycznym;
- intensyfikowania transgranicznej współpracy policji za pomocą różnych środków.

Bazy danych udostępniane na mocy decyzji w sprawie konwencji z Prüm podlegają wyłącznie prawu krajowemu, ale wymiana danych podlega dodatkowo omawianej decyzji, a ostatnio też decyzji ramowej o ochronie danych. Organami właściwymi do nadzorowania takiego przepływu danych są krajowe organy nadzorujące ochronę danych.

264 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.

265 Konwencja zawarta między Królestwem Belgii, Republiką Federalną Niemiec, Królestwem Hiszpanii, Republiką Francuską, Wielkim Księstwem Luksemburga, Królestwem Niderlandów i Republiką Austrii w sprawie intensyfikacji współpracy transgranicznej, szczególnie w walce z terroryzmem, przestępczością transgraniczną i nielegalną migracją; dostępna pod adresem: http://register.consilium.europa.eu/pdf/en/05/st10/st10900.en05.pdf.

7.2.3. Ochrona danych w Europolu i Eurojuście

Europol

Europol, czyli organ ścigania UE, ma siedzibę w Hadze, natomiast jego jednostki krajowe znajdują się w każdym państwie członkowskim. Europol ustanowiono w 1998 r., a jego obecny status prawny jako instytucji UE opiera się na decyzji Rady ustanawiającej Europejski Urząd Policji (*decyzji w sprawie Europolu*)[266]. Europol ma na celu pomagać w zapobieganiu przestępczości zorganizowanej, terroryzmowi i innym formom poważnej przestępczości, które wymieniono w załączniku do decyzji w sprawie Europolu, i które dotyczą co najmniej dwóch państw członkowskich, jak też w prowadzeniu dochodzeń w powyższych sprawach.

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 kompetencjom Europolu, bądź osób, w przypadku których istnieją faktyczne oznaki, że popełnią one takie przestępstwa. Europol i jego jednostki krajowe mogą wprowadzać dane bezpośrednio do systemu informacyjnego Europolu oraz pobierać z niego dane. Tylko strona, która wprowadziła dane do systemu, może je zmieniać, korygować lub usuwać.

W zakresie, w jakim jest to niezbędne do wykonywania jego zadań, Europol może przechowywać, zmieniać i wykorzystywać dane dotyczące przestępstw w plikach roboczych do celów analizy. Pliki robocze do celów analizy tworzy się w celach zbierania, przetwarzania lub wykorzystywania danych mającego na celu pomoc w konkretnych dochodzeniach karnych prowadzonych przez Europol wraz z państwami członkowskimi UE.

266 Rada Unii Europejskiej (2009), Decyzja Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji (Europol), Dz.U. L 121 z 15.5.2009. Zob. także wniosek Komisji dotyczący rozporządzenia, w którym określono ramy prawne dla nowego Europolu zastępującego Europol ustanowiony decyzją Rady 2009/371/WSiSW z dnia 6 kwietnia 2009 r. ustanawiającą Europejski Urząd Policji (Europol) oraz CEPOL ustanowiony decyzją Rady 2005/681/WSiSW ustanawiającą Europejskie Kolegium Policyjne (CEPOL), COM(2013) 173 final.

W reakcji na zmiany 1 stycznia 2013 r. ustanowiono w ramach Europolu Europejskie Centrum ds. Walki z Cyberprzestępczością[267]. 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, która:

- jest popełniana przez zorganizowane grupy w celu osiągania dużych zysków z przestępstw, takiej jak oszustwa internetowe;
- skutkuje poważnymi szkodami dla ofiar, takiej jak wykorzystywanie seksualne dzieci w internecie;
- ma wpływ na krytyczną infrastrukturę i systemy informacyjne w UE.

Udoskonalono system ochrony danych, któremu podlega działalność Europolu. W art. 27 decyzji w sprawie Europolu stwierdza się, że zastosowanie mają zasady określone w konwencji nr 108 oraz w zaleceniu w sprawie danych policyjnych w odniesieniu do przetwarzania danych zautomatyzowanych i niezautomatyzowanych. Przesyłanie danych między Europolem a państwami członkowskimi musi także spełniać wymogi określone w decyzji ramowej o ochronie danych.

Aby zapewnić zgodność z obowiązującym prawem o ochronie danych, a w szczególności nienaruszanie praw jednostki przez przetwarzanie danych osobowych, działania Europolu kontroluje i monitoruje niezależny wspólny organ nadzorczy Europolu[268]. Oprócz prawa żądania sprawdzenia, poprawienia lub usunięcia tych danych, każda osoba ma prawo dostępu do wszelkich danych osobowych, które Europol posiada na jej temat. Jeżeli decyzja Europolu dotycząca wykonywania tych praw jest dla niej niezadowalająca, osoba ta może odwołać się do komitetu odwoławczego wspólnego organu nadzorczego.

Jeżeli błędy o charakterze prawnym lub rzeczowym w danych przechowywanych lub przetwarzanych przez Europol skutkują szkodami, poszkodowany może

267 Zob. też 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* [„Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji do Rady i Parlamentu Europejskiego dotyczącego ustanowienia Europejskiego Centrum ds. Walki z Cyberprzestępczością"], Bruksela, 29 czerwca 2012 r.

268 Decyzja w sprawie Europolu, art. 34.

dochodzić roszczeń jedynie przed właściwym sądem państwa członkowskiego, w którym miało miejsce zdarzenie powodujące szkodę[269]. Jeżeli szkoda jest wynikiem niewypełnienia przez Europol jego obowiązków prawnych, Europol zwróci kwotę odszkodowania państwu członkowskiemu.

Eurojust

Ustanowiony w 2002 r. Eurojust jest organem UE z siedzibą w Hadze, który wspiera współpracę sądową w ramach dochodzeń i postępowań w sprawie poważnych przestępstw dotyczących co najmniej dwóch państw członkowskich[270]. Do zakresu 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 posiada niezbędne kompetencje 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 pewne informacje dotyczące świadków lub ofiar przestępstw podlegających kompetencjom Eurojustu[271]. W wyjątkowych przypadkach

269 *Tamże*, art. 52.

270 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 245 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*).

271 Wersja skonsolidowana decyzji Rady 2002/187/WSiSW zmienionej decyzją Rady 2003/659/WSiSW oraz decyzją Rady 2009/426/WSiSW, art. 15 ust. 2.

Eurojust może także, przez ograniczony czas, przetwarzać szersze dane osobowe odnoszące 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 konwencji nr 108 Rady Europy 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[272].

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.

7.2.4. Ochrona danych we wspólnych systemach informacyjnych na szczeblu UE

Oprócz wymiany danych między państwami członkowskimi i utworzenia organów UE wyspecjalizowanych w zwalczaniu przestępczości transgranicznej na szczeblu UE ustanowiono pewną liczbę wspólnych systemów informacyjnych pełniących funkcję platformy wymiany danych między właściwymi organami krajowymi i unijnymi w określonych celach związanych z egzekwowaniem prawa, w tym prawa imigracyjnego oraz celnego. Niektóre z nich wywodzą się z umów wielostronnych, które zostały następnie uzupełnione aktami prawnymi UE i systemami, takimi jak system informacyjny Schengen, wizowy system informacyjny, Eurodac, Eurosur czy system informacji celnej.

272 Przepisy regulaminu wewnętrznego Eurojustu dotyczące przetwarzania i ochrony danych osobowych, 19 marca 2005 r., Dz.U. C 68 z 19.3.2005, s. 1.

Ustanowiona w 2012 r. Europejska Agencja ds. Zarządzania Operacyjnego Wielkoskalowymi Systemami Informatycznymi w Przestrzeni Wolności, Bezpieczeństwa i Sprawiedliwości (eu-LISA)[273] jest odpowiedzialna za długoterminowe zarządzanie operacyjne systemem informacyjnym Schengen drugiej generacji (SIS II), wizowym systemem informacyjnym (VIS) oraz Eurodac. Podstawowym zadaniem eu-LISA jest zapewnienie skutecznej, bezpiecznej i ciągłej eksploatacji systemów informatycznych. Agencja jest też odpowiedzialna za przyjęcie niezbędnych środków w celu zapewnienia bezpieczeństwa systemów i danych.

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[274]. 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[275]. 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 oraz Islandię, Liechtenstein, Norwegię i Szwajcarię.[276] Do SIS II dostęp mają także Europol i Eurojust.

273 Rozporządzenie Parlamentu Europejskiego i Rady (EU) nr 1077/2011 z dnia 25 października 2011 r. ustanawiające europejską agencję do spraw zarządzania operacyjnego wielkoskalowymi systemami informatycznymi w przestrzeni wolności, bezpieczeństwa i sprawiedliwości, Dz.U. L 286 z 1.11.2011.

274 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.

275 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.

276 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; oraz Rada Unii Europejskiej (2007), 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 2005 z 7.8.2007.

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. C-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. N-SIS jest sprawdzany pod kątem wpisów dotyczących następujących sytuacji:

- dana osoba nie ma prawa wjazdu lub pobytu na terytorium strefy Schengen; lub
- dana osoba lub przedmiot jest poszukiwany przez organy sądowe bądź ścigania; 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 krajowych systemów informacyjnych Schengen 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 (ENA), dotyczących osób poszukiwanych w celu aresztowania, wydania lub ekstradycji.

Decyzja Rady 2007/533/WSiSW w sprawie utworzenia, funkcjonowania i użytkowania Systemu Informacyjnego Schengen drugiej generacji (decyzja w sprawie SIS II) uwzględnia zapisy konwencji nr 108: „Dane osobowe przetwarzane na użytek niniejszej decyzji podlegają ochronie zgodnie z Konwencją Rady Europy z dnia 28 stycznia 1981 r."[277]. Gdy krajowe organy policji wykorzystują dane osobowe w zastosowaniu decyzji w sprawie SIS II, konieczne jest wdrożenie do prawa

277 Rada Unii Europejskiej (2007), Decyzja Rady 2007/533/WSiSW z dnia 12 czerwca 2007 r. w sprawie utworzenia, funkcjonowania i użytkowania systemu informacyjnego Schengen drugiej generacji, Dz.U. L 205 z 7.8.2007, art. 57.

krajowego postanowień konwencji nr 108, a także zalecenia w sprawie danych policyjnych.

Krajowy N-SIS w każdym państwie członkowskim nadzoruje właściwy krajowy organ nadzorczy. W szczególności musi on kontrolować jakość danych, które państwo członkowskie wprowadza do C-SIS za pośrednictwem N-SIS. Krajowy organ nadzorczy musi zapewnić przeprowadzenie co najmniej raz na cztery lata audytu czynności przetwarzania danych w krajowym N-SIS. Krajowe organy nadzorcze oraz EIOD współpracują i zapewniają skoordynowany nadzór nadSIS, 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.

Prawa dostępu osób fizycznych dotyczące SIS II mogą być wykonywane w każdym państwie członkowskim, gdyż każdy N-SIS jest dokładną kopią C-SIS.

Przykład: W sprawie *Dalea przeciwko Francji*[278] 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 poprawienie 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.

278 ETPC, *Dalea przeciwko Francji (odrzucona)*, nr 964/07, 2 lutego 2010 r.

Wizowy system informacyjny

Wizowy system informacyjny (VIS), który jest również eksploatowany przez eu-LISA, stworzono, aby wesprzeć wdrożenie wspólnej polityki wizowej UE[279]. VIS umożliwia państwom Schengen wymianę danych wizowych za pośrednictwem systemu, który łączy konsulaty państw 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, czy osoba przedstawiająca wizę jest jej prawowitym posiadaczem, oraz identyfikację osób, które nie posiadają dokumentów lub posiadają fałszywe dokumenty.

Zgodnie z rozporządzeniem (WE) Parlamentu Europejskiego i Rady nr 767/2008 w sprawie Wizowego Systemu Informacyjnego (VIS) oraz wymiany danych pomiędzy państwami członkowskimi na temat wiz krótkoterminowych (*rozporządzeniem w sprawie VIS*) w VIS rejestrowane mogą być tylko dane osoby ubiegającej się o wizę, jej wizy, fotografie, odciski palców, odsyłacze do poprzednich wniosków oraz wnioski towarzyszących jej osób[280]. Dostęp do VIS w celu wprowadzania, korygowania lub usuwania danych jest zarezerwowany wyłącznie dla organów wizowych państw członkowskich, podczas gdy dostęp do celów przeglądania danych jest udostępniany organom wizowym oraz właściwym 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

279 Rada Unii Europejskiej (2004), Decyzja Rady z dnia 8 czerwca 2004 r. w sprawie ustanowienia Wizowego Systemu Informacyjnego (VIS), Dz.U. L 213 z 15.6.2004; rozporządzenie (WE) Parlamentu Europejskiego i Rady nr 767/2008 z dnia 9 lipca 2008 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.

280 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.

zapobiegania terroryzmowi i innym przestępstwom, wykrywania ich oraz prowadzenia dochodzeń w ich sprawie[281].

Eurodac

Nazwa Eurodac odnosi się do daktylogramów, czyli odcisków palców. Jest to scentralizowany system zawierający dane o odciskach palców obywateli państw trzecich ubiegających się o azyl w jednym z państw członkowskich UE[282]. System ten działa od stycznia 2003 r., a jego celem jest pomoc w ustaleniu, które państwo członkowskie powinno być odpowiedzialne za rozpatrzenie danego wniosku o udzielenie azylu na mocy rozporządzenia Rady (WE) nr 343/2003 ustanawiającego kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego (*rozporządzenia Dublin II*)[283]. Dane osobowe przechowywane w systemie Eurodac mogą być wykorzystywane wyłącznie w celu ułatwienia stosowania rozporządzenia Dublin II; wszelkie inne wykorzystanie podlega karom.

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 każdego obywatela państwa spoza UE lub bezpaństwowca w wieku co najmniej 14 lat, który ubiega się o azyl na ich terytorium lub został zatrzymany przy próbie nielegalnego przekroczenia ich zewnętrznej granicy. Państwa członkowskie mogą również pobierać i przesyłać odciski palców obywateli państw spoza UE lub bezpaństwowców, którzy przebywają na ich terytorium bez zezwolenia.

281 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.

282 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*).

283 Rozporządzenie Rady (WE) nr 343/2003 z dnia 18 lutego 2003 r. ustanawiające kryteria i mechanizmy określania państwa członkowskiego właściwego dla rozpatrywania wniosku o azyl, wniesionego w jednym z państw członkowskich przez obywatela państwa trzeciego (*rozporządzenie Dublin II*), Dz.U. L 50 z 25.2.2003.

Dane daktyloskopijne są przechowywane w bazie danych Eurodac wyłącznie w postaci spseudonimizowanej. W przypadku dopasowania pseudonim wraz z nazwą pierwszego państwa członkowskiego, które przekazało dane daktyloskopijne, jest ujawniany drugiemu państwu członkowskiemu. Wspomniane drugie państwo członkowskie zwraca się następnie do pierwszego państwa członkowskiego, gdyż zgodnie z rozporządzeniem Dublin II za rozpatrzenie wniosku o udzielenie azylu odpowiedzialne jest pierwsze państwo członkowskie.

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 skasować. Dane odnoszące się do cudzoziemców zatrzymanych przy próbie nielegalnego przekroczenia granicy zewnętrznej są przechowywane przez dwa lata. Dane te należy niezwłocznie skasować, jeżeli osoba, której dane dotyczą, otrzyma zezwolenie na pobyt, opuści terytorium UE lub uzyska obywatelstwo państwa członkowskiego.

Oprócz wszystkich państw członkowskich UE system Eurodac na podstawie umów międzynarodowych wykorzystują również Islandia, Norwegia, Liechtenstein i Szwajcaria.

Eurosur

Europejski system nadzorowania granic (*Eurosur*)[284] 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 Fronteksem – agencją UE odpowiedzialną za opracowanie i wdrożenie nowej koncepcji zintegrowanego zarządzania granicami[285]. Jego ogólnymi celami są:

- zredukowanie liczby nielegalnych migrantów przedostających się niepostrzeżenie na terytorium UE;

284 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.

285 Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1168/2011 zmieniające rozporządzenie Rady (WE) nr 2007/2004 ustanawiające Europejską Agencję Zarządzania Współpracą Operacyjną na Zewnętrznych Granicach Państw Członkowskich Unii Europejskiej, Dz.U. L 394 z 22.11.2001 (*rozporządzenie w sprawie Fronteksu*).

- 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[286].

System został uruchomiony 2 grudnia 2013 r. we wszystkich państwach członkowskich z granicami zewnętrznymi, w pozostałych zaś wejdzie do eksploatacji 1 grudnia 2014 r. Rozporządzenie będzie miało zastosowanie do nadzoru lądowych, morskich i powietrznych granic zewnętrznych państw członkowskich.

System informacji celnej

Kolejnym ważnym wspólnym systemem informacyjnym ustanowionym na szczeblu UE jest system informacji celnej (CIS)[287]. 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 zawiera informacje obejmujące dane osobowe w odniesieniu do zatrzymanych, zajętych lub skonfiskowanych towarów, środków transportu, przedsiębiorstw, osób, przedmiotów i gotówki. Informacje te mogą być wykorzystywane wyłącznie do celów obserwacji, składania sprawozdań lub prowadzenia kontroli szczególnych lub

286 Zob. też: 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) [„Ocena skutków załączona do wniosku w sprawie rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego europejski system nadzorowania granic (Eurosur)"], dokument roboczy służb, SEC(2011) 1536 final, Bruksela, 12 grudnia 2011 r., s. 18.

287 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: Rada Unii Europejskiej (2009), Rozporządzenie Nr 515/97 z 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*).

też do celów analiz strategicznych bądź operacyjnych dotyczących osób podejrzanych o naruszenie przepisów celnych.

Dostęp do CIS posiadają krajowe organy celne, podatkowe, rolne, władze ds. zdrowia publicznego, policja, Europol i Eurojust.

Przetwarzanie danych osobowych musi odbywać się zgodnie z przepisami szczególnymi zawartymi w Rozporządzeniu Nr 515/917 oraz w konwencji CIS[288] oraz przepisami dyrektywy o ochronie danych, rozporządzenia o ochronie danych przez instytucje UE, konwencji nr 108 i zalecenia w sprawie danych policyjnych. EIOD jest odpowiedzialny za nadzór nad zgodnością CIS z Rozporządzeniem (WE) Nr 45/2001 oraz co najmniej raz w roku organizuje spotkanie ze wszystkimi krajowymi organami nadzorczymi właściwymi do spraw nadzoru nad CIS.

288 Tamże.

8

Inne szczególne europejskie przepisy w zakresie ochrony danych

UE	Omówione zagadnienia	RE
Dyrektywa o ochronie danych Dyrektywa o prywatności i łączności elektronicznej	**Łączność elektroniczna**	Konwencja nr 108 Zalecenie w sprawie usług telekomunikacyjnych
Artykuł 8 ust. 2 lit. b) dyrektywy o ochronie danych	**Stosunki pracy**	Konwencja nr 108 Zalecenie w sprawie zatrudnienia
		ETPC, *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 3 kwietnia 2007 r.
Artykuł 8 ust. 3 dyrektywy o ochronie danych	**Dane medyczne**	Konwencja nr 108 Zalecenie w sprawie danych medycznych
		ETPC, *Z. przeciwko Finlandii*, nr 22009/93, 25 lutego 1997 r.
Dyrektywa w sprawie badań klinicznych	**Badania kliniczne**	
Artykuł 6 ust. 1 lit. b) i e), art. 13 ust. 2 dyrektywy o ochronie danych	**Statystyka**	Konwencja nr 108 Zalecenie w sprawie danych statystycznych
Rozporządzenie (WE) nr 223/2009 w sprawie statystyki europejskiej TSUE, C-524/06, *Huber przeciwkoBundesrepublik Deutschland*, 16 grudnia 2008 r.	**Statystyka urzędowa**	Konwencja nr 108 Zalecenie w sprawie danych statystycznych

UE	Omówione zagadnienia	RE
Dyrektywa 2004/39/WE 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	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, 6 grudnia 2012 r.

W kilku przypadkach na szczeblu europejskim przyjęto specjalne akty prawne, w których określono bardziej szczegółowo zastosowanie ogólnych zasad konwencji nr 108 lub dyrektywy o ochronie danych do konkretnych sytuacji.

8.1. 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 danych o ruchu, 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[289]. 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 wiadomości reklamowych. 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. w celu uzupełnienia i uszczegółowienia przepisów dyrektywy o ochronie danych w odniesieniu do sektora telekomunikacyjnego[290]. 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:

- dane stanowiące treść wiadomości wysyłanych podczas połączenia; dane te są ściśle poufne;

289 RE, 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 [„Zalecenie Rec(95)4 dla państw członkowskich w sprawie ochrony danych osobowych w dziedzinie usług telekomunikacyjnych, ze szczególnym uwzględnieniem usług telefonicznych"], 7 lutego 1995 r.

290 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, w brzmieniu zmienionym dyrektywą Parlamentu Europejskiego i Rady 2009/136/WE 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 niezbędne w celu ustanowienia i utrzymania połączenia, tak zwane dane o ruchu, takie jak informacje dotyczące stron połączenia, czasu jego nawiązania i trwania;

- wśród danych o ruchu 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 dodane, np. dostarczającym na podstawie lokalizacji użytkownika informacje na temat położenia najbliższej stacji metra lub apteki bądź prognozę pogody dla danej lokalizacji.

Dostęp do danych o łączności w sieciach elektronicznych w innych celach, takich jak dochodzenia w sprawie przestępstw, musi zgodnie z art. 15 dyrektywy o prywatności i łączności elektronicznej 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.

W 2009 r. w dyrektywie o prywatności i łączności elektronicznej[291] 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 zgodę. Bez takiej zgody marketingowe wiadomości elektroniczne można kierować jedynie do dotychczasowych klientów, jeżeli ci udostępnili swój adres e-mail i nie zgłosili sprzeciwu.

291 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.

- Na państwa członkowskie nałożono obowiązek zapewnienia środków sądowych w odniesieniu do naruszeń zakazu przesyłania niezamówionych komunikatów[292].

- 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[293].

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 danych[294].

W dyrektywie o zatrzymywaniu danych[295] (unieważnionej 8 kwietnia 2014 r.) zobowiązano dostawców usług łączności do udostępniania danych o ruchu, w szczególności do celów walki z poważną przestępczością, przez okres co najmniej 6, ale nie dłużej niż 24 miesięcy, niezależnie od tego, czy usługodawca nadal potrzebuje tych danych do celów rozliczeniowych lub technicznego świadczenia usługi.

Państwa członkowskie UE mają obowiązek wyznaczyć niezależne organy publiczne odpowiedzialne za monitorowanie bezpieczeństwa zatrzymywanych danych.

---

292 Zob. zmienioną dyrektywę, art. 13.

293 Zob. *Tamże*, art. 5; zob. także Grupa Robocza Art. 29 (2012), *Opinia nr 04/2012 w sprawie wyłączenia zapisywania plików cookie spod zasady pozyskiwania zgody*, WP 194, Bruksela, 7 czerwca 2012 r.

294 Zob. też Grupa Robocza Art. 29 (2011), *Working Document 01/2011 on the current EU personal data breach framework and recommendations for future policy developments* [„Dokument roboczy 01/2011 w sprawie obecnych ram dotyczących naruszeń danych osobowych oraz zaleceń dotyczących przyszłego rozwoju polityki"], WP 184, WP184, Bruksela, 5 kwietnia 2011 r.

295 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.

Zatrzymywanie danych telekomunikacyjnych w oczywisty sposób ingeruje w prawo do ochrony danych[296]. To, czy ta ingerencja jest uzasadniona, zakwestionowano w kilku postępowaniach sądowych w państwach członkowskich UE[297].

> Przykład: W *Digital Ireland i Seitlinger i inni*[298] TSUE uznał dyrektywę w sprawie zatrzymywania danych za nieważną. Zdaniem Trybunału „dyrektywa ta wyjątkowo szeroko i mocno ingeruje w te podstawowe prawa, przy czym przepisy mające zagwarantować to, że ingerencja ta nie będzie rzeczywiście wykraczać poza to, co ściśle niezbędne, nie regulują precyzyjnie tej kwestii".

Podstawowym zagadnieniem w kontekście łączności elektronicznej jest ingerencja organów publicznych. Środki nadzoru lub przechwytywania komunikatów, takie jak urządzenia podsłuchowe lub nagrywające, są dopuszczalne tylko wtedy, gdy są one przewidziane prawem i stanowią środek konieczny w społeczeństwie demokratycznym w celu: ochrony państwa, bezpieczeństwa publicznego, interesów finansowych państwa lub zwalczania przestępczości; bądź ochrony osoby, której dane dotyczą, lub praw i wolności innych osób.

Przykład: W sprawie *Malone przeciwko Zjednoczonemu Królestwu*[299] skarżącego oskarżono o kilka przestępstw związanych z paserstwem. Podczas procesu okazało się, że władze przechwyciły rozmowę telefoniczną skarżącego na mocy nakazu wydanego przez Sekretarza Stanu w Ministerstwie Spraw Wewnętrznych. Chociaż sposób przechwycenia komunikatu skarżącego był zgodny z prawem krajowym, ETPC uznał, że nie istniały żadne przepisy prawne dotyczące zakresu swobody władz publicznych ani sposobu, w jaki mogą one z niego korzystać w tym obszarze, więc ingerencja wynikająca ze stosowania kwestionowanej praktyki nie była „zgodna z prawem". Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

296 EIOD (2011), *Opinion of 31 May 2011 on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC)* [„Opinia z dnia 31 maja 2011 r. w sprawie sprawozdania Komisji dla Rady i Parlamentu Europejskiego oceniającego dyrektywę o zatrzymywaniu danych (dyrektywę 2006/24/WE)"], 31 maja 2011 r.

297 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.

298 TSUE, Sprawy połączone C-293/12 i C-594/12, *Digital Rights Ireland i Seitlinger i inni,* 8 kwietnia 2014 r., pkt 65.

299 ETPC, *Malone przeciwko Zjednoczonemu Królestwu*, nr 8691/79, 2 sierpnia 1984 r.

8.2. Dane o zatrudnieniu

Najważniejsze kwestie

- W zaleceniu RE w sprawie danych o zatrudnieniu zawarto szczegółowe zasady dotyczące ochrony danych w kontekście stosunków pracy.
- W dyrektywie 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.

W UE nie ma konkretnych ram prawnych dotyczących przetwarzania danych w kontekście zatrudnienia. W dyrektywie o ochronie danych konkretnie o stosunkach pracy mowa jest jedynie w art. 8 ust. 2, który dotyczy przetwarzania danych szczególnie chronionych. Jeżeli chodzi o prawo RE, zalecenie w sprawie danych o zatrudnieniu opublikowano w 1989 r. i jest ono obecnie aktualizowane[300].

Przegląd najczęstszych problemów związanych z ochroną danych w kontekście zatrudnienia znajduje się w dokumencie roboczym Grupy Roboczej Art. 29[301]. Grupa robocza przeanalizowała znaczenie zgody jako podstawy prawnej przetwarzania danych o zatrudnieniu[302]. Stwierdziła przy tym, że nierównowaga ekonomiczna między wnioskującym o zgodę pracodawcą a udzielającym jej pracownikiem budzi często wątpliwości, czy zgody udzielono dobrowolnie, czy też nie. Przy ocenie ważności zgody w kontekście zatrudnienia należy zatem starannie rozważyć okoliczności, w których wnioskuje się o zgodę.

300 Rada Europy, Komitet Ministrów (1989), Recommendation Rec(89)2 to member states on the protection of personal data used for employment purposes [„Zalecenie Rec(89)2 dla państw członkowskich w sprawie ochrony danych osobowych wykorzystywanych w związku z zatrudnieniem"], 18 stycznia 1989 r. Zob. ponadto Komitet Konsultacyjny Konwencji nr 108, Study on Recommendation No. R (89) 2 on the protection of personal data used for employment purposes and to suggest proposals for the revision of the above-mentioned Recommendation [„Studium dotyczące Zalecenia Rec(89)2 dla państw członkowskich w sprawie ochrony danych osobowych wykorzystywanych w związku z zatrudnieniem i sugestie zmian dotyczących powyższego Zalecenia"], 9 września 2011 r.

301 Grupa Robocza Art. 29 (2001), *Opinion 8/2001 on the processing of personal data in the employment context* [„Opinia 8/2001 w sprawie przetwarzania danych osobowych w kontekście zatrudnienia"], WP 48, Bruksela, 13 września 2001 r.

302 Grupa Robocza Art. 29 (2005), *Dokument roboczy w sprawie wspólnej wykładni art. 26 ust. 1 dyrektywy 95/46/WE z 24 października 1995 r.*, WP 114, Bruksela, 25 listopada 2005 r.

Częsty problem dotyczący ochrony danych w typowym współczesnym środowisku pracy wiąże się z zakresem uzasadnionego monitorowania komunikacji 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 interesujący w tym kontekście jest przytoczony poniżej wyrok ETPC.

Przykład: W sprawie *Copland przeciwko Zjednoczonemu Królestwu*[303] 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. Dlatego też ingerencja była niezgodna z prawem. Trybunał stwierdził, że doszło do naruszenia art. 8 EKPC.

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.

303 ETPC, *Copland przeciwko Zjednoczonemu Królestwu*, nr 62617/00, 3 kwietnia 2007 r.

Szczególnie chronione dane osobowe 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, tylko jeżeli jest to konieczne w celu: określenia ich przydatności do pracy; spełnienia wymagań medycyny prewencyjnej; lub przyznania świadczeń społecznych. 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. Pracodawcy powinni też informować pracowników z wyprzedzeniem o wprowadzeniu lub adaptacji automatycznych systemów przetwarzania danych osobowych pracowników bądź monitorowania przemieszczania się i wydajności pracowników.

Pracownicy muszą mieć prawo dostępu do swoich danych o zatrudnieniu, jak też ich poprawienia lub skasowania. 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 poprawienia lub usunięcia, prawo krajowe musi zapewniać odpowiednie procedury odwołania się od takiej odmowy.

8.3. Dane medyczne

Najważniejsza kwestia

- Dane medyczne są danymi szczególnie chronionymi i 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. 8 ust. 1 dyrektywy o ochronie danych i na mocy art. 6 konwencji nr 108. Zasady przetwarzania danych medycznych są z kolei bardziej rygorystyczne niż w przypadku danych innych niż szczególnie chronione.

Przykład: W sprawie *Z. przeciwko Finlandii*[304] 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 art. 8 ust. 3 dyrektywy o ochronie danych dopuszcza się przetwarzanie danych medycznych, gdy jest to wymagane do celów medycyny prewencyjnej, diagnostyki medycznej, świadczenia opieki lub leczenia, lub też zarządzania opieką zdrowotną. Przetwarzanie danych jest jednak dopuszczalne tylko wtedy, gdy przetwarza je pracownik służby zdrowia podlegający obowiązkowi zachowania tajemnicy zawodowej lub inna osoba podlegająca równoważnemu obowiązkowi[305].

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[306]. Proponowane przepisy są zgodne z zapisami dyrektywy 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, poprawienia oraz usunięcia danych. Ponadto dane medyczne przetwarzane zgodnie z prawem przez pracowników służby

304 ETPC, *Z. przeciwko Finlandii*, nr 22009/93, 25 lutego 1997 r., pkt 94 i 112; zob. też 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 inni przeciwko Słowacji*, nr 32881/04, 28 kwietnia 2009 r.; ETPC, *Szuluk przeciwko Zjednoczonemu Królestwu*, nr 36936/05, 2 czerwca 2009 r.

305 Zob. też ETPC, *Biriuk przeciwko Litwie*, nr 23373/03, 25 listopada 2008 r.

306 RE, Komitet Ministrów (1997), Recommendation Rec(97)5 to member states on the protection of medical data [„Zalecenie Rec(97)5 dla państw członkowskich w sprawie ochrony danych medycznych"], 13 lutego 1997 r.

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"[307].

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 2.1.3.

Na szczeblu krajowym i europejskim trwa ożywiona dyskusja na temat inicjatyw przechowywania danych o leczeniu pacjentów w elektronicznych kartotekach zdrowotnych[308]. Szczególnym aspektem utrzymywania ogólnokrajowych systemów elektronicznych kartotek zdrowotnych jest ich dostępność za granicą, co jest tematem szczególnego zainteresowania w UE w kontekście transgranicznej opieki zdrowotnej[309].

Kolejnym obszarem, w którym omawiane są nowe przepisy, są badania kliniczne, czyli udokumentowane próby nowych leków na pacjentach; ten temat także ma poważne implikacje dla ochrony danych. Zagadnienia badań klinicznych produktów leczniczych przeznaczonych do stosowania przez człowieka uregulowano w dyrektywie 2001/20/WE Parlamentu Europejskiego i Rady z dnia 4 kwietnia 2001 r. w sprawie zbliżania przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich odnoszących się do wdrożenia zasady dobrej praktyki klinicznej w prowadzeniu badań klinicznych produktów leczniczych przeznaczonych do

307 ETPC, nr 1585/09, *Avilkina i inni przeciwko Rosji*, 6 czerwca 2013 r., pkt 53 (nieprawomocny).

308 Grupa Robocza Art. 29 (2007), *Dokument roboczy w sprawie przetwarzania danych osobowych dotyczących zdrowia w elektronicznej dokumentacji zdrowotnej (EHR)*, WP 131, Bruksela, 15 lutego 2007 r.

309 Dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE z dnia 9 marca 2011 r. w sprawie stosowania praw pacjentów w transgranicznej opiece zdrowotnej, Dz.U. L 88 z 4.4.2011.

stosowania przez człowieka (*dyrektywie w sprawie badań klinicznych*)[310]. W grudniu 2012 r. Komisja Europejska przedstawiła wniosek dotyczący zastąpienia dyrektywy w sprawie badań klinicznych rozporządzeniem, aby ujednolicić procedury badań i zwiększyć ich efektywność[311].

Na szczeblu UE istnieje wiele inicjatyw legislacyjnych i innych w sprawie danych osobowych w sektorze ochrony zdrowia[312].

8.4. Przetwarzanie danych do celów statystycznych

Najważniejsze kwestie

- Danych zgromadzonych do celów statystycznych nie wolno wykorzystywać do żadnych innych celów.
- Dane zgromadzone zgodnie z prawem w dowolnym celu mogą później zostać wykorzystane do celów statystycznych pod warunkiem, że prawo krajowe przewiduje odpowiednie zabezpieczenia, które stosują użytkownicy. W tym celu należy przewidzieć w szczególności anonimizację lub pseudonimizację danych przed przekazaniem ich stronom trzecim.

W dyrektywie o ochronie danych o przetwarzaniu danych do celów statystycznych wspomniano w kontekście możliwych wyłączeń od zasad ochrony danych. Na mocy art. 6 ust. 1 lit. b) dyrektywy zasada ograniczenia celu może zostać uchylona na mocy prawa krajowego, aby umożliwić dalsze wykorzystanie danych do celów statystycznych, choć w prawie krajowym trzeba wówczas ustanowić wszystkie niezbędne zabezpieczenia. W art. 13 ust. 2 dyrektywy zezwala się na ograniczenie praw dostępu na mocy prawa krajowego, jeżeli dane są przetwarzane wyłącznie do

310 Dyrektywa 2001/20/WE Parlamentu Europejskiego i Rady z dnia 4 kwietnia 2001 r. w sprawie zbliżania przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, odnoszących się do wdrożenia zasady dobrej praktyki klinicznej w prowadzeniu badań klinicznych produktów leczniczych, przeznaczonych do stosowania przez człowieka, Dz.U. L 121 z 1.5.2001.

311 Komisja Europejska (2012), Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE, COM(2012) 369 final, Bruksela, 17 lipca 2012 r.

312 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' [„Opinia Europejskiego Inspektora Ochrony Danych w sprawie komunikatu Komisji »Plan działania w dziedzinie e-zdrowia na lata 2012–2020 – Innowacyjna opieka zdrowotna w XXI wieku«"], Bruksela, 27 marca 2013 r.

celów statystycznych; w prawie krajowym trzeba ponownie ustanowić odpowiednie zabezpieczenia. W tym kontekście w dyrektywie o ochronie danych ustanowiono szczegółowy wymóg, że żadne dane uzyskane lub powstałe w trakcie badań statystycznych nie mogą być wykorzystywane w celu podejmowania konkretnych decyzji odnoszących się do osób, których dane dotyczą.

Chociaż dane, które zostały zgromadzone zgodnie z prawem przez administratora do jakichkolwiek celów, mogą zostać ponownie wykorzystane przez tego administratora do jego własnych celów statystycznych – tak zwanej statystyki wtórnej – dane te musiałyby zostać zanonimizowane lub spseudonimizowane, w zależności od kontekstu, przed przekazaniem ich stronom trzecim do celów statystycznych, chyba że osoba, której dane dotyczą, wyraziła na to zgodę lub jest to wyraźnie przewidziane w prawie krajowym. Wynika to z wymogu odpowiednich zabezpieczeń na mocy art. 6 ust. 1 lit. b) dyrektywy o ochronie danych.

Najważniejszymi przypadkami wykorzystania danych do celów statystycznych są urzędowe statystyki sporządzane przez krajowe i unijne urzędy statystyczne na podstawie przepisów krajowych i unijnych dotyczących urzędowych statystyk. Zgodnie z tymi przepisami obywatele i przedsiębiorcy mają zazwyczaj obowiązek ujawnienia danych organom statystycznym. Urzędnicy pracujący w urzędach statystycznych są związani specjalnym obowiązkiem zachowania tajemnicy zawodowej i zasada ta jest skrupulatnie przestrzegana, gdyż jest ona warunkiem wysokiego poziomu zaufania obywateli, który jest niezbędny, aby dane były udostępniane organom statystycznym.

Rozporządzenie (WE) nr 223/2009 w sprawie statystyki europejskiej (*rozporządzenie w sprawie statystyki europejskiej*) zawiera podstawowe przepisy dotyczące ochrony danych w związku z urzędowymi statystykami, dlatego też można je uznać za istotne także z punktu widzenia przepisów o urzędowych statystykach na szczeblu krajowym[313]. W rozporządzeniu utrzymano zasadę, że dla urzędowych działań statystycznych niezbędna jest wystarczająco precyzyjna podstawa prawna[314].

313 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.

314 Zasada ta ma zostać bardziej szczegółowo sformułowana w kodeksie praktyk Eurostatu, który zgodnie z art. 11 rozporządzenia w sprawie statystyki europejskiej będzie zawierać wskazówki etyczne dotyczące sposobu sporządzania statystyk urzędowych, w tym właściwego sposobu wykorzystania danych osobowych; dokument jest dostępny pod adresem: http://epp.eurostat.ec.europa.eu/portal/page/portal/about_eurostat/introduction.

> Przykład: W sprawie *Huber przeciwko Niemcom*[315] TSUE uznał, że gromadzenie i przechowywanie danych osobowych przez organ do celów statystycznych nie było samo w sobie wystarczającą podstawą przetwarzania danych zgodnie z prawem. Przepisy przewidujące przetwarzanie danych osobowych muszą także spełniać wymóg konieczności, a w tym kontekście nie został on spełniony.

Jeżeli chodzi o RE, wydane w 1997 r. zalecenie w sprawie danych statystycznych dotyczy sporządzania statystyk w sektorach publicznym i prywatnym[316]. Zawarto w nim zasady pokrywające się z opisanymi powyżej podstawowymi przepisami dyrektywy o ochronie danych. Bardziej szczegółowe są przepisy dotyczące zagadnień opisanych poniżej.

Podczas gdy danych zgromadzonych do celów statystycznych nie można 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 nawet na przekazywanie danych stronom 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, należy założyć, iż 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 przesłaniem.

Na osoby zajmujące się zawodowo badaniami statystycznymi należy nałożyć na mocy prawa krajowego specjalne obowiązki zachowania tajemnicy zawodowej, co jest powszechne w przypadku statystyk urzędowych. Obowiązki te należy rozszerzyć także na ankieterów, 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, osoby, których dane dotyczą, muszą wyrazić zgodę na wykorzystanie ich danych, aby było ono zgodne z prawem, lub trzeba im co najmniej umożliwić

315 TSUE, C-524/06, *Huber przeciwkoBundesrepublik Deutschland*, 16 grudnia 2008 r.; zob. zwłaszcza pkt 68.

316 Rada Europy, Komitet Ministrów (1997), Recommendation Rec(97)18 to member states on the protection of personal data collected and processed for statistical purposes [„Zalecenie Rec(97)18 dla państw członkowskich w sprawie ochrony danych osobowych gromadzonych i przetwarzanych do celów statystycznych"], 30 września 1997 r.

wyrażenie sprzeciwu. Jeżeli dane osobowe do celów statystycznych są gromadzone za pośrednictwem ankiet, respondentów należy wyraźnie poinformować, czy ujawnianie danych jest obowiązkowe na mocy prawa krajowego, czy też nie. Danych szczególnie chronionych nigdy nie należy gromadzić w sposób umożliwiający identyfikację osób, chyba że jest to wyraźnie dozwolone na mocy prawa krajowego.

W przypadku gdy badań statystycznych nie można przeprowadzić bez 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 dane należy spseudonimizować, a klucz do szyfrowania lub listę identyfikujących synonimów należy przechowywać oddzielnie od spseudonimizowanych danych.

8.5. Dane finansowe

Najważniejsze kwestie

- Chociaż dane finansowe nie są danymi szczególnie chronionymi w rozumieniu konwencji nr 108 lub dyrektywy 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.
- Szczególne problemy związane z ochroną danych w tym obszarze wynikają z potrzeby wdrożenia odpowiednich mechanizmów uwierzytelnienia.

Przykład: W sprawie *Michaud przeciwko Francji*[317] skarżący, który był francuskim prawnikiem, zakwestionował ciążący na nim na mocy prawa francuskiego

317 ETPC, *Michaud przeciwko Francji*, nr 12323/11, 6 grudnia 2012 r.; zob. też 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.

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, 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, stwierdzając, że nie doszło do naruszenia art. 8.

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[318]. W zaleceniu tym sprecyzowano zakres zgodnego z prawem gromadzenia i wykorzystywania danych w kontekście płatności, zwłaszcza z użyciem kart płatniczych. Dodatkowo zasugerowano ustawodawcom krajowym szczegółowe regulacje dotyczące ograniczeń przekazywania danych o płatnościach stronom trzecim, terminów przechowywania danych, przejrzystości, bezpieczeństwa danych i transgranicznego przepływu danych, jak też nadzoru oraz środków prawnych. Proponowane rozwiązania są zgodne z późniejszymi ogólnymi ramami ochrony danych UE zawartymi w dyrektywie o ochronie danych.

Uchwalono akty prawne dotyczące regulacji rynków instrumentów finansowych oraz działalności instytucji kredytowych i firm inwestycyjnych[319]. Inne akty prawne pomagają w zwalczaniu wykorzystywania informacji wewnętrznych i manipulacji

318 RE, Komitet Ministrów (1990), Recommendation No. R(90)19 on the protection of personal data used for payment and other related operations [„Zalecenie Rec(90)19 w sprawie ochrony danych osobowych wykorzystywanych do płatności i innych powiązanych czynności"], 13 września 1990 r.

319 Komisja Europejska (2011), *Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych uchylającej dyrektywę 2004/39/WE Parlamentu Europejskiego i Rady*, COM(2011) 656 final, Bruksela, 20 października 2011 r.; Komisja Europejska (2011), *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie rynków instrumentów finansowych oraz zmieniającego rozporządzenie [EMIR] w sprawie instrumentów pochodnych będących przedmiotem obrotu poza rynkiem regulowanym, partnerów centralnych i repozytoriów transakcji*, COM(2011) 652 final, Bruksela, 20 października 2011 r.; Komisja Europejska (2011), *Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie warunków podejmowania i prowadzenia działalności przez instytucje kredytowe oraz nadzoru ostrożnościowego nad instytucjami kredytowymi i firmami inwestycyjnymi i zmieniającej dyrektywę 2002/87/WE Parlamentu Europejskiego i Rady w sprawie dodatkowego nadzoru nad instytucjami kredytowymi, zakładami ubezpieczeń oraz przedsiębiorstwami inwestycyjnymi konglomeratu finansowego*, COM(2011) 453 final, Bruksela, 20 lipca 2011 r.

na rynku[320]. Najważniejszymi zagadnieniami w tych obszarach, które wywierają wpływ na ochronę danych, są:

- zatrzymywanie zapisów dotyczących transakcji finansowych;
- przekazywanie danych osobowych do państw trzecich;
- nagrywanie 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).

W tej dziedzinie występują także inne konkretnie wskazane zagadnienia, w tym gromadzenie danych na temat sytuacji finansowej osób, których dane dotyczą[321], bądź płatności transgraniczne przy wykorzystaniu przelewów bankowych, które muszą ze swojej natury prowadzić do przepływu danych osobowych[322].

320 Komisja Europejska (2011), *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie wykorzystywania informacji poufnych i manipulacji na rynku* (nadużyć na rynku), COM(2011) 651 final, Bruksela, 20 października 2011 r.; Komisja Europejska (2011), Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie sankcji karnych za wykorzystywanie informacji poufnych i manipulacje na rynku, COM(2011) 654 final, Bruksela, 20 października 2011 r.

321 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; Komisja Europejska, *Wniosek dotyczący rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie (WE) nr 1060/2009 w sprawie agencji ratingowych*, COM(2010) 289 final, Bruksela, 2 czerwca 2010 r.

322 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.

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*, Wien, Manzsche Verlags- und Universitätsbuchhandlung.

EDRi, *An introduction to data protection* [„Wprowadzenie do ochrony danych"], Brussels, dokument dostępny pod adresem: www.edri.org/files/paper06_datap.pdf.

Frowein, J. i Peukert, W. (2009), *Europäische Menschenrechtskonvention*, Berlin, N. P. Engel Verlag.

Grabenwarter, C. i Pabel, K. (2012), *Europäische Menschenrechtskonvention*, München, C. H. Beck.

Harris, D., O'Boyle, M., Warbrick, C. i Bates, E. (2009), *Law of the European Convention on Human Rights* [„Prawo europejskiej konwencji praw człowieka"], Oxford, Oxford University Press.

Jarass, H. (2010), *Charta der Grundrechte der Europäischen Union*, München, C. H. Beck.

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* [„Przypadki, materiały i komentarze dotyczące europejskiej konwencji praw człowieka"], Oxford, Oxford University Press.

Nowak, M., Januszewski, K. i Hofstätter, T. (2012), *All Human Rights for All – Vienna Manual on Human Rights* [„Wszystkie prawa człowieka dla wszystkich – wiedeński podręcznik praw człowieka"], Antwerp, 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*, Brussels, 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" [„Prawo do prywatności"], *Harvard Law Review,* t. 4, nr 5, s. 193–220, dokument dostępny pod adresem: www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf.

White, R. i Ovey, C. (2010), *The European Convention on Human Rights* [„Europejska konwencja praw człowieka"], Oxford, Oxford University Press.

Rozdział 2

Carey, P. (2009), *Data protection: A practical guide to UK and EU law* [„Ochrona danych: praktyczny przewodnik po prawie Zjednoczonego Królestwa i UE"], Oxford, Oxford University Press.

Delgado, L. (2008), *Vida privada y protección de datos en la Unión Europea*, Madrid, Dykinson S. L.

Desgens-Pasanau, G. (2012), *La protection des données à caractère personnel*, Paris, LexisNexis.

Di Martino, A. (2005), *Datenschutz im europäischen Recht*, Baden-Baden, Nomos.

Morgan, R. i Boardman, R. (2012), *Data protection strategy: Implementing data protection compliance* [„Strategia ochrony danych: jak zapewnić przestrzeganie przepisów"], London, Sweet & Maxwell.

Ohm, P. (2010), „Broken promises of privacy: Responding to the surprising failure of anonymization" [„Złamane obietnice prywatności: jak reagować na zaskakujące niepowodzenie anonimizacji"], *UCLA Law Review*, t. 57, nr 6, s. 1701–1777.

Tinnefeld, M., Buchner, B. i Petri, T. (2012), *Einführung in das Datenschutzrecht: Datenschutz und Informationsfreiheit in europäischer Sicht*, München, Oldenbourg Wissenschaftsverlag.

United Kingdom Information Commissioner's Office (2012), *Anonymisation: managing data protection risk. Code of practice* [„Anonimizacja: zarządzanie ryzykiem ochrony danych. Kodeks postępowania"], dokument dostępny pod adresem: www.ico.org.uk/for_organisations/data_protection/topic_guides/anonymisation.

Rozdziały 3–5

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*, t. IV, rozdz. 30, München, C. H. Beck.

Conde Ortiz, C. (2008), *La protección de datos personales*, Cadiz, Dykinson.

Coudray, L. (2010), *La protection des données personnelles dans l'Union européenne*, Saarbrücken, Éditions universitaires européennes.

Dammann, U. i Simitis, S. (1997), *EG-Datenschutzrichtlinie*, Baden-Baden, Nomos.

FRA (Agencja Praw Podstawowych Unii Europejskiej) (2010), *Data Protection in the European Union: the role of National Data Protection Authorities (Strengthening the fundamental rights architecture in the EU II)* [„Ochrona danych w Unii Europejskiej: rola krajowych urzędów ochrony danych (wzmacnianie architektury praw podstawowych w UE II)"], Luxembourg, Publications Office of the European Union (Publications Office).

FRA (2010), *Developing indicators for the protection, respect and promotion of the rights of the child in the European Union* [„Opracowanie wskaźników ochrony, poszanowania i promowania praw dziecka w Unii Europejskiej"] (Conference edition), Wien, FRA.

FRA (2011), *Access to justice in Europe: an overview of challenges and opportunities* [„Dostęp do wymiaru sprawiedliwości w Europie: wyzwania i możliwości"], Luxembourg, Publications Office.

Simitis, S. (2011), *Bundesdatenschutzgesetz*, Baden-Baden, Nomos.

United Kingdom Information Commissioner's Office, *Privacy Impact Assessment* [„Ocena skutków w zakresie prywatności"], dokument dostępny pod adresem: www.ico.org.uk/for_organisations/data_protection/topic_guides/privacy_impact_assessment.

Rozdział 6

Gutwirth, S., Poullet, Y., De Hert, P., De Terwangne, C. i Nouwt, S. (2009), *Reinventing data protection?* [„Ochrona danych na nowo?"], Berlin, Springer.

Kuner, C. (2007), *European data protection law* [„Europejskie prawo ochrony danych"], Oxford, Oxford University Press.

Kuner, C. (2013), *Transborder data flow regulation and data privacy law* [„Regulacja transgranicznego przepływu danych i prawo o prywatności danych"], Oxford, Oxford University Press.

Rozdział 7

Europol (2012), *Data Protection at Europol* [„Ochrona danych w Europolu"], Luxembourg, Publications Office, dokument dostępny pod adresem: www.europol.europa.eu/sites/default/files/publications/europol_dpo_booklet_0.pdf.

Eurojust, *Data protection at Eurojust: A robust, effective and tailor-made regime* [„Ochrona danych w Eurojuście: solidny, skuteczny i dostosowany do potrzeb system"], Den Haag, Eurojust.

Drewer, D., Ellermann, J. (2012), *Europol's data protection framework as an asset in the fight against cybercrime* [„Ramy ochrony danych Europolu jako atut w walce z cyberprzestępczością"], ERA Forum, t. 13, nr 3, s. 381–395.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world* [„Ochrona danych w sprofilowanym świecie"], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* [„Komputery, prywatność i ochrona danych: element wyboru"], Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem" [„Niszczenie demokracji czy jej obrona? Dyrektywa o zatrzymywaniu danych, wszechobecny nadzór państwowy i nasz ekosystem konstytucyjny"], *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* [„Rola Parlamentu Europejskiego w zawarciu transatlantyckich umów o przekazywaniu danych osobowych po traktacie lizbońskim"], Centre for the Law of External Relations, CLEER Working Papers 2013/2, dokument dostępny pod adresem: www.asser.nl/upload/documents/20130226T013310-cleer_13-2_web.pdf.

Rozdział 8

Büllesbach, A., Gijrath, S., Poullet, Y. i Hacon, R. (2010), *Concise European IT law* [„Europejskie prawo informatyczne w skrócie"], Amsterdam, Kluwer Law International.

Gutwirth, S., Leenes, R., De Hert, P. i Poullet, Y. (2012), *European data protection: In good health?* [„Europejska ochrona danych: w dobrej kondycji?"], Dordrecht, Springer.

Gutwirth, S., Poullet, Y. i De Hert, P. (2010), *Data protection in a profiled world* [„Ochrona danych w sprofilowanym świecie"], Dordrecht, Springer.

Gutwirth, S., Poullet, Y., De Hert, P. i Leenes, R. (2011), *Computers, privacy and data protection: An element of choice* [„Komputery, prywatność i ochrona danych: element wyboru"], Dordrecht, Springer.

Konstadinides, T. (2011), „Destroying democracy on the ground of defending it? The Data Retention Directive, the surveillance state and our constitutional ecosystem" [„Niszczenie demokracji czy jej obrona? Dyrektywa o zatrzymywaniu danych, wszechobecny nadzór państwowy i nasz ekosystem konstytucyjny"], *European Law Review*, t. 36, nr 5, s. 722–776.

Rosemary, J. i Hamilton, A. (2012), *Data protection law and practice* [„Prawo i praktyka ochrony danych"], London, Sweet & Maxwell.

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 inni przeciwko Słowacji, nr 32881/04, 28 kwietnia 2009 r.
Leander przeciwko Szwecji, nr 9248/81, 26 marca 1987 r.
Odièvre przeciwko Francji [Wielka Izba], nr 42326/98, 13 lutego 2003 r.

Wyważenie ochrony danych z wolnością wypowiedzi

Axel Springer AG przeciwko Niemcom [Wielka Izba], nr 39954/08, 7 lutego 2012 r.
Von Hannover przeciwko Niemcom, nr 59320/00, 24 czerwca 2004 r.
Von Hannover przeciwko Niemcom (nr 2) [Wielka Izba], nr 40660/08 i 60641/08, 7 lutego 2012 r.

Wyzwania związane z ochroną danych w internecie

K.U. przeciwko Finlandii, nr 2872/02, 2 grudnia 2008 r.

Korespondencja

Amann przeciwko Szwajcarii [Wielka Izba], nr 27798/95, 16 lutego 2000 r.
Bernh Larsen Holding AS i inni 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.
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.
McMichael przeciwko Zjednoczonemu Królestwu, nr 16424/90, 24 lutego 1995 r.
M.G. przeciwko Zjednoczonemu Królestwu, nr 39393/98, 24 września 2002 r.
Rotaru przeciwko Rumunii [Wielka Izba], nr 28341/95, 4 maja 2000 r.
S. i Marper przeciwko Zjednoczonemu Królestwu, nr 30562/04 i 30566/04, 4 grudnia 2008 r.
Shimovolos przeciwko Rosji, nr 30194/09, 21 czerwca 2011 r.
Turek przeciwko Słowacji, nr 57986/00, 14 lutego 2006 r.

Bazy danych rejestrów karnych

B.B. przeciwko Francji, nr 5335/06, 17 grudnia 2009 r.
M.M. przeciwko Zjednoczonemu Królestwu, nr 24029/07, 13 listopada 2012 r.

Bazy danych DNA

S. i Marper przeciwko Zjednoczonemu Królestwu, 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

Biriuk przeciwko Litwie, nr 23373/03, 25 listopada 2008 r.
I. przeciwko Finlandii, nr 20511/03, 17 lipca 2008 r.
L.L. przeciwko Francji, nr 7508/02, 10 października 2006 r.
M.S. przeciwko Szwecji, nr 34209/96, 27 sierpnia 1997 r.
Szuluk przeciwko Zjednoczonemu Królestwu, nr 36936/05, 2 czerwca 2009 r.
Z. przeciwko Finlandii, nr 22009/93, 25 lutego 1997 r.

Tożsamość

Ciubotaru przeciwko Mołdawii, nr 27138/04, 27 kwietnia 2010 r.

Godelli przeciwko Włochom, nr 33783/09, 25 września 2012 r.
Odièvre przeciwko Francji [Wielka Izba], nr 42326/98, 13 lutego 2003 r.

Informacje o działalności zawodowej

Michaud przeciwko Francji, nr 12323/11, 6 grudnia 2012 r.
Niemietz przeciwko Niemcom, nr 13710/88, 16 grudnia 1992 r.

Przechwytywanie łączności

Amann przeciwko Szwajcarii [Wielka Izba], nr 27798/95, 16 lutego 2000 r.
Copland przeciwko Zjednoczonemu Królestwu, nr 62617/00, 3 kwietnia 2007 r.
Cotlet przeciwko Rumunii, nr 38565/97, 3 czerwca 2003 r.
Kruslin przeciwko Francji, nr 11801/85, 24 kwietnia 1990 r.
Lambert przeciwko Francji, nr 23618/94, 24 sierpnia 1998 r.
Liberty i inni przeciwko Zjednoczonemu Królestwu, nr 58243/00, 1 lipca 2008 r.
Malone przeciwko Zjednoczonemu Królestwu, nr 8691/79, 2 sierpnia 1984 r.
Halford przeciwko Zjednoczonemu Królestwu, nr 20605/92, 25 czerwca 1997 r.
Szuluk przeciwko Zjednoczonemu Królestwu, nr 36936/05, 2 czerwca 2009 r.

Obowiązki spoczywające na stosownych podmiotach

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.

Zdjęcia

Sciacca przeciwko Włochom, nr 50774/99, 11 stycznia 2005 r.
Von Hannover przeciwko Niemcom, nr 59320/00, 24 czerwca 2004 r.

Prawo do zapomnienia

Segerstedt-Wiberg i inni przeciwko Szwecji, nr 62332/00, 6 czerwca 2006 r.

Prawo sprzeciwu

Leander przeciwko Szwecji, nr 9248/81, 26 marca 1987 r.
Mosley przeciwko Zjednoczonemu Królestwu, nr 48009/08, 10 maja 2011 r.
M.S. przeciwko Szwecji, nr 34209/96, 27 sierpnia 1997 r.
Rotaru przeciwko Rumunii [Wielka Izba], nr 28341/95, 4 maja 2000 r.

Szczególnie chronione kategorie danych

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, nr 30562/04 i 30566/04, 4 grudnia 2008 r.

Nadzór i egzekwowanie (rola poszczególnych podmiotów, w tym urzędów ochrony danych)

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) [Wielka Izba], nr 40660/08 i 60641/08, 7 lutego 2012 r.

Metody nadzoru

Allan przeciwko Zjednoczonemu Królestwu, nr 48539/99, 5 listopada 2002 r.
Association „21 Décembre 1989" i inni przeciwko Rumunii, nr 33810/07 i 18817/08, 24 maja 2011 r.
Bykov przeciwko Rosji [Wielka Izba], nr 4378/02, 10 marca 2009 r.
Kennedy przeciwko Zjednoczonemu Królestwu, nr 26839/05, 18 maja 2010 r.
Klass i inni przeciwko Niemcom, nr 5029/71, 6 września 1978 r.
Rotaru przeciwko Rumunii [Wielka Izba], nr 28341/95, 4 maja 2000 r.
Taylor-Sabori przeciwko Zjednoczonemu Królestwu, nr 47114/99, 22 października 2002 r.
Uzun przeciwko Niemcom, nr 35623/05, 2 września 2010 r.
Vetter przeciwko Francji, nr 59842/00, 31 maja 2005 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

C-73/07, *Tietosuojavaltuutettu przeciwko Satakunnan Markkinapörssi Oy i Satamedia Oy*, 16 grudnia 2008 r.
[Pojęcie „działalności dziennikarskiej" w rozumieniu art. 9 dyrektywy o ochronie danych]

Sprawy połączone C-92/09 i C-93/09, *Volker und Markus Schecke GbR oraz Hartmut Eifert przeciwko Land Hessen*, 9 listopada 2010 r.
[Proporcjonalność prawnego obowiązku publikowania danych osobowych beneficjentów niektórych funduszy rolnych UE]

C-101/01, *Bodil Lindqvist*, 6 listopada 2003 r.
[Zgodność z prawem publikowania przez osobę prywatną danych o życiu prywatnym innych osób w internecie]

C-131/12, *Google Spain, S.L., Google Inc. przeciwko Agencia Española de Protección de Datos, Mario Costeja González*, wniosek o wydanie orzeczenia w trybie prejudycjalnym skierowany przez Audiencia Nacional (Hiszpania) złożony w dniu 9 marca 2012, 25 maja 2012 r., w toku.
[Obowiązek zaprzestania przez podmioty świadczące usługi wyszukiwarek wyświetlania danych osobowych w wynikach wyszukiwania na wniosek osoby, której dane dotyczą]

C-270/11, *Komisja Europejska przeciwko Królestwu Szwecji*, 30 maja 2013 r.
[Kara za niewdrożenie dyrektywy]

C-275/06, *Productores de Música de España (Promusicae) przeciwko Telefónica de España SAU*, 29 stycznia 2008 r.
[Obowiązek ujawnienia przez usługodawców internetowych tożsamości użytkowników programów wymiany plików KaZaA stowarzyszeniu na rzecz ochrony własności intelektualnej]

C-288/12, *Komisja Europejska przeciwko Węgrom*, 8 kwietnia 2014 r.
[Zgodność z prawem likwidacji urzędu krajowego inspektora ochrony danych]

C-291/12, *Michael Schwarz przeciwko Stadt Bochum*, opinia rzecznika generalnego, 13 czerwca 2013 r.
[Naruszenie prawa pierwotnego UE przez rozporządzenie (WE) 2252/2004, w którym nakazano przechowywanie odcisków palców w paszportach]

Sprawy połączone C-293/12 i C-549/12, *Digital Rights Ireland i Seitlinger i inni,* 8 kwietnia 2014 r. [Naruszenie prawa pierwotnego UE przez dyrektywę o zatrzymywaniu danych].
[Naruszenie prawa pierwotnego UE przez dyrektywę o zatrzymywaniu danych]

C-360/10, *SABAM przeciwko Netlog NV*, 16 lutego 2012 r.
[Obowiązek zapobiegania przez usługodawców świadczących usługi sieci społecznościowych niezgodnemu z prawem korzystaniu z utworów muzycznych i audiowizualnych przez użytkowników sieci]

Sprawy połączone C-465/00, C-138/01 i C-139/01*, Rechnungshof przeciwko Österreichischer Rundfunk i innym oraz Neukomm i Lauermann przeciwko Österreichischer Rundfunk*, 20 maja 2003 r.
[Proporcjonalność prawnego obowiązku publikowania danych osobowych dotyczących wynagrodzeń niektórych kategorii pracowników instytucji związanych z sektorem publicznym]

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-518/07, *Komisja Europejska przeciwko Republice Federalnej Niemiec*, 9 marca 2010 r.
[Niezależność krajowego organu nadzoru]

C-524/06, *Huber przeciwko Bundesrepublik Deutschland*, 16 grudnia 2008 r.
[Zasadność przechowywania danych na temat cudzoziemców w rejestrze statystycznym]

C-543/09, *Deutsche Telekom AG przeciwko Republice Federalnej Niemiec*, 5 maja 2011 r.
[Konieczność ponownej zgody]

C-553/07, *College van burgemeester en wethouders van Rotterdam przeciwko M.E.E. Rijkeboer*, 7 maja 2009 r.
[Prawo dostępu osoby, której dane dotyczą]

C-614/10, *Komisja Europejska przeciwko Republice Austrii*, 16 października 2012 r.
[Niezależność krajowego organu nadzorczego]

Orzecznictwo związane z rozporządzeniem o ochronie danych przez instytucje UE

C-28/08 P, *Komisja Europejska przeciwko The Bavarian Lager Co. Ltd*, 29 czerwca 2010 r.
[Dostęp do dokumentów]

C-41/00 P, *Interporc Im- und Export GmbH przeciwko Komisji Wspólnot Europejskich*, 6 marca 2003 r.
[Dostęp do dokumentów]

F-35/08, *Dimitrios Pachtitis przeciwko Komisji Europejska*, 15 czerwca 2010 r.
[Wykorzystanie danych osobowych w kontekście zatrudnienia w instytucjach UE]

F-46/09, *V przeciwko Parlamentowi Europejskiemu*, 5 lipca 2011 r.
[Wykorzystanie danych osobowych w kontekście zatrudnienia w instytucjach UE]

Wykaz spraw

Orzecznictwo Europejskiego Trybunału Sprawiedliwości

Orzecznictwo Europejskiego Trybunału Praw Człowieka

Orzecznictwo sądów krajowych

Agencja Praw Podstawowych Unii Europejskiej
Rada Europy – Europejski Trybunał Praw Człowieka

Podręcznik europejskiego prawa o ochronie danych

2014 — 214 s. — 14,8 × 21 cm

ISBN 978-92-871-9940-9 (RE)
ISBN 978-92-9239-338-0 (FRA)
doi:10.2811/5514
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 Rady Europy jest dostępne w Internecie na stronie hub.coe.int.

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 francuskim, tłumaczeń na inne języki, comiesięcznych biuletynów informacyjnych dotyczących orzecznictwa, komunikatów prasowych oraz innych informacji na temat pracy Trybunału.

JAK OTRZYMAĆ PUBLIKACJE UE

Publikacje bezpłatne:
- jeden egzemplarz:
  w księgarni UE (http://bookshop.europa.eu);
- większa liczba egzemplarzy lub plakaty/mapy:
  w przedstawicielstwach Unii Europejskiej (http://ec.europa.eu/represent_en.htm);
  w delegaturach w krajach spoza UE (http://eeas.europa.eu/delegations/index_en.htm);
  kontaktujac się z serwisem Europe Direct (http://europa.eu/europedirect/index_en.htm)
  lub dzwoniac na numer 00 800 6 7 8 9 10 11 (bezpłatny numer infolinii w całej UE) (*).

Publikacje odpłatne:
- w księgarnii UE (http://bookshop.europa.eu);

Subskrypcje odpłatne:
- u dystrybutorów Urzędu Publikacji Unii Europejskiej
  (http://publications.europa.eu/others/agents/index_en.htm).

(*) Informacje udzielane są nieodpłatnie, większość połączeń również jest bezpłatna (jednak niektórzy operatorzy, hotele lub aparaty w budkach telefonicznych mogą naliczać opłaty).

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/.

10.2811/5514
TK-01-13-772-PL-C

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

Szybki rozwój technologii informacyjnych i komunikacyjnych 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 dla prawa do ochrony danych. Niniejszy podręcznik ma stanowić wprowadzenie do tej 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 zarówno Europejskiego Trybunału Praw Człowieka (ETPC), jak i Trybunału Sprawiedliwości Unii Europejskiej (TSUE). W przypadku braku stosownego orzecznictwa przedstawiono praktyczne przykłady z hipotetycznymi scenariuszami. Krótko mówiąc, niniejszy podręcznik ma pomagać w energicznej i stanowczej obronie prawa do ochrony danych.

AGENCJA PRAW PODSTAWOWYCH UNII EUROPEJSKIEJ
Schwarzenbergplatz 11 – 1040 Wiedeń – Austria
Tel. +43 (1) 580 30-60 - Fax +43 (1) 580 30-693
fra.europa.eu – info@fra.europa.eu

RADA EUROPY
EUROPEJSKI TRYBUNAŁ PRAW CZŁOWIEKA
67075 Strasbourg - Francja
Tel. +33 (0) 3 88 41 20 00 - Fax +33 (0) 3 88 41 27 30
echr.coe.int – publishing@echr.coe.int

Urząd Publikacji
ISBN 978-92-871-9940-9 (RE)
ISBN 978-92-9239-338-0 (FRA)