OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH

USTAWA O OCHRONIE DANYCH OSOBOWYCH

Komentarz

Paweł Fajgielski

KOMENTARZE

WYDANIE 2

Wolters Kluwer

OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH

USTAWA O OCHRONIE DANYCH OSOBOWYCH

Komentarz

Paweł Fajgielski

KOMENTARZE

WYDANIE 2

Wolters Kluwer

WARSZAWA 2022

Stan prawny na 30 września 2021 r.

Wydawca
Monika Pawłowska

Redaktor prowadzący
Joanna Tchorek

Opracowanie redakcyjne
Michał Dymiński

Projekt okładek serii
Wojtek Kwiecień-Janikowski, Przemek Dębowski

ISBN 978-83-8246-564-8 *ISBN PDF-a: 978-83-8246-967-7*
2. wydanie

Wolters Kluwer Polska Sp. z o.o.
Dział Praw Autorskich
01-208 Warszawa, ul. Przyokopowa 33
tel. 22 535 82 19
e-mail: PL-ksiazki@wolterskluwer.com

księgarnia internetowa www.profinfo.pl

Spis treści

CZĘŚĆ II
KOMENTARZ DO USTAWY Z DNIA 10 MAJA 2018 R. O OCHRONIE DANYCH OSOBOWYCH

Wykaz skrótów

1. Akty prawne

dyrektywa 95/46/WE – dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24.10.1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz swobodnego przepływu tych danych (Dz.Urz. WE L 281, s. 31 ze zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 15, s. 355, ze zm.); określana też jako dyrektywa o ochronie danych osobowych (uchylona)

dyrektywa 2000/31/WE – dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. WE L 178, s. 1; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 25, s. 399); określana też jako dyrektywa o handlu elektronicznym

dyrektywa 2002/58/WE – dyrektywa 2002/58/WE Parlamentu Europejskiego i Rady z 12.07.2002 r. dotycząca przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej) (Dz.Urz. WE L 201, s. 37 ze zm.; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 29, s. 514, ze zm.)

dyrektywa 2016/680 – dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW (Dz.Urz. UE L 119, s. 89 ze zm.), określana też jako dyrektywa policyjna

Karta Praw Podstawowych UE	– Karta Praw Podstawowych Unii Europejskiej (Dz.Urz. UE C 202 z 2016 r., s. 389)
k.c.	– ustawa z 23.04.1964 r. – Kodeks cywilny (Dz.U. z 2020 r. poz. 1740 ze zm.)
k.k.	– ustawa z 6.06.1997 r. – Kodeks karny (Dz.U. z 2020 r. poz. 1444 ze zm.)
Konstytucja RP	– Konstytucja Rzeczypospolitej Polskiej z 2.04.1997 r. (Dz.U. poz. 483 ze zm.)
Konwencja 108	– Konwencja Nr 108 Rady Europy sporządzona w Strasburgu 28.01.1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (Dz.U. z 2003 r. Nr 3, poz. 25) uzupełniona protokołem dodatkowym, sporządzonym w Strasburgu dnia 8.11.2001 r. (Dz.U. z 2006 r. Nr 3, poz. 15)
k.p.a.	– ustawa z 14.06.1960 r. – Kodeks postępowania administracyjnego (Dz.U. z 2021 r. poz. 735 ze zm.)
k.p.c.	– ustawa z 17.11.1964 – Kodeks postępowania cywilnego (Dz.U. z 2021 r. poz. 1805 ze zm.)
o.p.	– ustawa z 29.08.1997 r. – Ordynacja podatkowa (Dz.U. z 2021 r. poz. 1540 ze zm.)
p.p.s.a.	– ustawa z 30.08.2002 r. – Prawo o postępowaniu przed sądami administracyjnymi (Dz.U. z 2019 r. poz. 2325 ze zm.)
preambuła	– preambuła do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE
pr.pras.	– ustawa z 26.01.1984 r. – Prawo prasowe (Dz.U. z 2018 r. poz. 1914)
pr.przeds.	– ustawa z 6.03.2018 r. – Prawo przedsiębiorców (Dz.U. z 2021 r. poz. 162)
pr.szkoln.wyż.	– ustawa z 20.07.2018 r. – Prawo o szkolnictwie wyższym i nauce (Dz.U. z 2021 r. poz. 478 ze zm.)
pr.telekom.	– ustawa z 16.07.2004 r. – Prawo telekomunikacyjne (Dz.U. z 2021 r. poz. 576 ze zm.)
rozporządzenie 2016/679	– rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1 ze zm.), określane też jako rozporządzenie ogólne

rozporządzenie 2018/1725	– rozporządzenie Parlamentu Europejskiego i Rady 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.Urz. UE L 295 z 21.11.2018 r., s. 39 i n.)
sprostowanie rozporządzenia	– Sprostowanie do rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 127 z 2018 r., s. 2)
TFUE	– Traktat o funkcjonowaniu Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 47)
TUE	– Traktat o Unii Europejskiej (wersja skonsolidowana Dz.Urz. UE C 202 z 2016 r., s. 13)
u.CEIDG	– ustawa z 6.03.2018 r. o Centralnej Ewidencji i Informacji o Działalności Gospodarczej i Punkcie Informacji dla Przedsiębiorcy (Dz.U. z 2020 r. poz. 2296 ze zm.)
u.d.i.p.	– ustawa z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176 ze zm.)
u.f.p.	– ustawa z 27.08.2009 r. o finansach publicznych (Dz.U. z 2021 r. poz. 305 ze zm.)
u.inf.	– ustawa z 17.02.2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. z 2021 r. poz. 670 ze zm.)
u.o.d.o.1997	– ustawa z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.) – uchylona
u.o.d.o.2018	– ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781)
u.o.d.o.p.	– ustawa z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125)
u.o.i.n.	– ustawa z 5.08.2010 r. o ochronie informacji niejawnych (Dz.U. z 2019 r. poz. 742)
u.p.e.a.	– ustawa z 17.06.1966 r. o postępowaniu egzekucyjnym w administracji (Dz.U. z 2020 r. poz. 1427 ze zm.)
u.s.g.	– ustawa z 8.03.1990 r. o samorządzie gminnym (Dz.U. z 2021 r. poz. 1372 ze zm.)

ustawa o IPN – ustawa z 18.12.1998 r. o Instytucie Pamięci Narodowej – Komisji Ścigania Zbrodni przeciwko Narodowi Polskiemu (Dz.U. z 2021 r. poz. 177 ze zm.)

ustawa o NIK – ustawa z 23.12.1994 r. o Najwyższej Izbie Kontroli (Dz.U. z 2020 r. poz. 1200 ze zm.)

ustawa o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia 2016/679 – ustawa z 21.02.2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.U. z 2019 r. poz. 730)

u.ś.u.d.e. – ustawa z 18.07.2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2020 r. poz. 344 ze zm.)

u.u.i.ś. – ustawa z 3.10.2008 r. o udostępnianiu informacji o środowisku i jego ochronie, udziale społeczeństwa w ochronie środowiska oraz o ocenach oddziaływania na środowisko (Dz.U. z 2021 r. poz. 247 ze zm.)

2. Inne

ABI – administrator bezpieczeństwa informacji

BCR – wiążące reguły korporacyjne (ang. *binding corporate rules*)

BIP – Biuletyn Informacji Publicznej

CEIDG – Centralna Ewidencja i Informacja o Działalności Gospodarczej

CEPiK – Centralna Ewidencja Pojazdów i Kierowców

CURIA – strona internetowa z orzecznictwem Trybunału Sprawiedliwości UE, https://curia.europa.eu/

EOG – Europejski Obszar Gospodarczy

EPS – Europejski Przegląd Sądowy

EROD – Europejska Rada Ochrony Danych

ETPCz – Europejski Trybunał Praw Człowieka

GIODO – Generalny Inspektor Ochrony Danych Osobowych

HUDOC – strona internetowa z orzecznictwem Europejskiego Trybunału Praw Człowieka, https://hudoc.echr.coe.int/eng

IOD – inspektor ochrony danych

KRK – Krajowy Rejestr Karny

M.P. – Monitor Polski

M. Praw. – Monitor Prawniczy

NSA	– Naczelny Sąd Administracyjny
ODO	– ochrona(-y) danych osobowych
PbD	– uwzględnienie ochrony danych w fazie projektowania (ang. *Privacy by Design*)
PCA	– Polskie Centrum Akredytacji
PiP	– Państwo i Prawo
PPH	– Przegląd Prawa Handlowego
Prezes Urzędu	– Prezes Urzędu Ochrony Danych Osobowych
procesor	– podmiot przetwarzający dane na zlecenie administratora (ang. *processor*)
PS	– Przegląd Sądowy
PUG	– Przegląd Ustawodawstwa Gospodarczego
RDK	– Rejestr Danych Kontaktowych
SN	– Sąd Najwyższy
TS	– Trybunał Sprawiedliwości
TSUE	– Trybunał Sprawiedliwości Unii Europejskiej
UDT	– Urząd Dozoru Technicznego
UK	– Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej
UOKiK	– Urząd Ochrony Konkurencji i Konsumentów
WP	– Grupa Robocza (ang. *Working Party*), także oznaczenie dokumentów przygotowywanych przez Grupę Roboczą

Wstęp

W okresie ostatnich kilku lat w Unii Europejskiej przeprowadzona została reforma ochrony danych osobowych. Dnia 24.05.2016 r. weszło w życie ogólne rozporządzenie o ochronie danych (Dz.Urz. UE L 119, s. 1 ze zm.), które powinno być stosowane od 25.05.2018 r. Rozporządzenie zastąpiło dyrektywę 95/46/WE i krajowe ustawy o ochronie danych. Jednym z założeń reformy było ujednolicenie prawnej regulacji ochrony danych we wszystkich państwach członkowskich. Realizacji tego celu służyć ma zmiana formy prawnej regulacji – dyrektywa, która wymagała implementacji do prawa krajowego, została zastąpiona rozporządzeniem niewymagającym implementacji, a stosowanym bezpośrednio. Oznacza to, że w całej Unii Europejskiej w zakresie ochrony danych osobowych obowiązuje zasadniczo jeden akt normatywny – ogólne rozporządzenie o ochronie danych (rozporządzenie 2016/679). Brak konieczności implementacji nie oznacza jednak braku krajowej regulacji prawnej, ponieważ unijne rozporządzenie wymaga uzupełnienia i uszczegółowienia niektórych zagadnień (m.in. kwestii ustrojowych i proceduralnych). Uzupełnieniem unijnego rozporządzenia w prawie polskim jest ustawa z 10.05.2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781), która zastąpiła ustawę o tym samym tytule z 1997 r.

Częścią unijnej reformy ochrony danych osobowych jest również regulacja odnosząca się do ochrony danych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar. Zagadnienia te zostały uregulowane w dyrektywie unijnej 2016/680 (Dz.Urz. UE L 119, s. 89), która została implementowana do prawa polskiego ustawą z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125). Jednak ze względu na specyficzny charakter tej problematyki, zagadnienia te nie zostaną poddane szczegółowym analizom w niniejszym komentarzu, gdyż wymagają odrębnego opracowania, które jest przedmiotem odrębnych komentarzy do u.o.d.o.p.

Niniejsza publikacja stanowi komentarz do przepisów o ochronie danych osobowych. Nie została ona jednak ograniczona – jak wszystkie wydane wcześniej w naszym kraju komentarze – do przepisów unijnych, ale obejmuje również przepisy krajowe.

W pierwszej części zawarty został komentarz do unijnego ogólnego rozporządzenia o ochronie danych, uwzględniający dwa sprostowania do tego aktu normatywnego (Dz.Urz. UE L 127 z 2018 r., s. 2; Dz.Urz. UE L 74 z 2021 r., s. 35), natomiast druga część zawiera komentarz do nowej polskiej ustawy o ochronie danych osobowych. Obie części są ze sobą powiązane poprzez system odesłań, co ma zapewnić spójność, pozwolić na uniknięcie zbędnych powtórzeń, a zarazem umożliwić łatwe poruszanie się po tekstach komentowanych przepisów.

Układ komentarzy do poszczególnych artykułów unijnego rozporządzenia ma budowę jednorodną. Komentarz do każdego z artykułów rozpoczyna krótkie wskazanie przedmiotu regulacji zawartej w danym przepisie, następnie sygnalizowane są regulacje unijne i krajowe, które stanowiły odpowiedniki komentowanego przepisu w poprzednich regulacjach prawnych, w dalszej – zasadniczej części przedstawiona jest analiza treści przepisu i omówienie konstrukcji prawnych tam zawartych, z odwołaniem się do literatury przedmiotu i orzecznictwa, a w końcowej części przedstawione są relacje z innymi przepisami lub inne kwestie szczególne.

W zamierzeniu autora komentarz ma łączyć w sobie walory praktyczne i naukowe. Wymiar praktyczny przejawia się przede wszystkim w tym, że omawiane konstrukcje prawne są ilustrowane przykładami, podawane są informacje, które mogą ułatwić interpretację i stosowanie komentowanych przepisów, sygnalizowane są wątpliwości i problemy oraz podejmowane są próby rozstrzygania nasuwających się wątpliwości. Walor naukowy przejawia się m.in. w tym, że przy dokonywaniu wykładni przepisów omawiane są zagadnienia teoretyczne i konstrukcyjne, prezentowane analizy prowadzone są z wykorzystaniem metod przyjętych i stosowanych w naukach prawnych (stosowane są metody: dogmatyczna, historyczna, prawnoporównawcza), opierają się nie tylko na tekstach aktów normatywnych, ale również na orzecznictwie i piśmiennictwie przedmiotu, a wykorzystane źródła wskazywane są w tekście zasadniczym (w nawiasach), jak również w zamieszczonym na końcu komentarza wykazie źródeł.

Od czasu opublikowania pierwszego wydania niniejszego komentarza minęły 3 lata. W okresie tym uchwalone zostały przepisy szczególne dotyczące ochrony danych osobowych, dokonano zmian obowiązujących przepisów, wydane zostały orzeczenia sądowe i decyzje oraz stanowiska organu nadzorczego mające istotne znaczenie dla interpretacji przepisów, a także ukazały się liczne publikacje dotyczące ochrony danych osobowych i dokumenty Europejskiej Rady Ochrony Danych, co pociągnęło za sobą potrzebę uaktualnienia komentarza. W drugim wydaniu komentarza uwzględnione zostały nowe bądź zmienione przepisy prawa (m.in. omówiona została nowelizacja Kodeksu postępowania administracyjnego w zakresie ochrony danych osobowych), nowe decyzje wykonawcze dotyczące standardowych klauzul umownych, wskazane zostały najistotniejsze orzeczenia sądów i decyzje Prezesa UODO (m.in. dotyczące nałożenia administracyjnych kar pieniężnych) oraz przedstawione zostały poglądy prezentowane

w najnowszym piśmiennictwie przedmiotu (m.in. komentarzach do u.o.d.o.2018 i publikacjach naukowych). Ponadto publikacja została uzupełniona o indeks rzeczowy, zawarty na końcu książki, który ma ułatwić odnalezienie komentarzy odnoszących się do wybranych zagadnień.

W drugim wydaniu komentarza uwzględniony został stan prawny na dzień 30.09.2021 r.

Paweł Fajgielski

CZĘŚĆ I

KOMENTARZ DO OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679

z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

(Tekst mający znaczenie dla EOG)

(Dz.Urz. UE L 119, s. 1 z 4.05.2016 r.; sprost.: Dz.Urz. UE L 127, s. 2 z 23.05.2018 r.; Dz.Urz. UE L 74, s. 35 z 3.04.2021 r.)

PARLAMENT EUROPEJSKI I RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej, w szczególności jego art. 16,

uwzględniając wniosek Komisji Europejskiej,

po przekazaniu projektu aktu ustawodawczego parlamentom narodowym,

uwzględniając opinię Europejskiego Komitetu Ekonomiczno-Społecznego[1],

uwzględniając opinię Komitetu Regionów[2],

stanowiąc zgodnie ze zwykłą procedurą ustawodawczą[3],

a także mając na uwadze, co następuje:

(1) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej (zwanej dalej „Kartą praw podstawowych") oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej (TFUE) stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

(2) Zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych nie mogą – niezależnie od obywatelstwa czy miejsca zamieszkania takich osób – naruszać ich podstawowych praw i wolności, w szczególności prawa do ochrony danych osobowych. Niniejsze rozporządzenie ma na celu przyczyniać się do tworzenia przestrzeni wolności, bezpieczeństwa i sprawiedliwości oraz unii gospodarczej, do postępu społeczno-gospodarczego, do wzmacniania i konwergencji gospodarek na rynku wewnętrznym, a także do pomyślności ludzi.

(3) Celem dyrektywy Parlamentu Europejskiego i Rady 95/46/WE[4] jest zharmonizowanie ochrony podstawowych praw i wolności osób fizycznych w związku z czynnościami przetwarzania oraz zapewnienie swobodnego przepływu danych osobowych między państwami członkowskimi.

[1] Dz.U. C 229 z 31.7.2012, s. 90.

[2] Dz.U. C 391 z 18.12.2012, s. 127.

[3] Stanowisko Parlamentu Europejskiego z dnia 12 marca 2014 r. (dotychczas nieopublikowane w Dzienniku Urzędowym) oraz stanowisko Rady w pierwszym czytaniu z dnia 8 kwietnia 2016 r. (dotychczas nieopublikowane w Dzienniku Urzędowym). Stanowisko Parlamentu Europejskiego z dnia 14 kwietnia 2016 r.

[4] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, s. 31).

(4) Przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości. Prawo do ochrony danych osobowych nie jest prawem bezwzględnym; należy je postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności. Niniejsze rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w Traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.

(5) Integracja społeczno-gospodarcza wynikająca z funkcjonowania rynku wewnętrznego doprowadziła do znacznego zwiększenia transgranicznych przepływów danych osobowych. Wzrosła wymiana danych osobowych między podmiotami publicznymi i prywatnymi, w tym między osobami fizycznymi, zrzeszeniami i przedsiębiorstwami w Unii. Od organów krajowych państw członkowskich prawo Unii coraz częściej wymaga, by w celu wykonania swoich obowiązków lub w celu realizacji zadań w imieniu organu innego państwa członkowskiego współpracowały ze sobą i wymieniały się danymi osobowymi.

(6) Szybki postęp techniczny i globalizacja przyniosły nowe wyzwania w dziedzinie ochrony danych osobowych. Skala zbierania i wymiany danych osobowych znacząco wzrosła. Dzięki technologii zarówno przedsiębiorstwa prywatne, jak i organy publiczne mogą na niespotykaną dotąd skalę wykorzystywać dane osobowe w swojej działalności. Osoby fizyczne coraz częściej udostępniają informacje osobowe publicznie i globalnie. Technologia zmieniła gospodarkę i życie społeczne i powinna nadal ułatwiać swobodny przepływ danych osobowych w Unii oraz ich przekazywanie do państw trzecich i organizacji międzynarodowych, równocześnie zaś powinna zapewniać wysoki stopień ochrony danych osobowych.

(7) Przemiany te wymagają stabilnych, spójniejszych ram ochrony danych w Unii oraz zdecydowanego ich egzekwowania, gdyż ważna jest budowa zaufania, które pozwoli na rozwój gospodarki cyfrowej na rynku wewnętrznym. Osoby fizyczne powinny mieć kontrolę nad własnymi danymi osobowymi. Osoby fizyczne, podmioty gospodarcze i organy publiczne powinny zyskać większe poczucie pewności prawa i jego stosowania w praktyce.

(8) W zakresie, w jakim niniejsze rozporządzenie dopuszcza doprecyzowanie lub zawężenie jego przepisów przez prawo państw członkowskich, mogą one – o ile jest to niezbędne, by krajowe przepisy były spójne i zrozumiałe dla osób, do których mają zastosowanie – włączyć elementy niniejszego rozporządzenia do swego prawa krajowego.

(9) Cele i zasady dyrektywy 95/46/WE pozostają aktualne, jednak wdrażając ochronę danych w Unii, nie uniknięto fragmentaryzacji, niepewności prawnej oraz upowszechnienia się poglądu, że ochrona osób fizycznych jest znacznie zagrożona, w szczególności w związku z działaniami w internecie. Różnice w stopniu ochrony praw i wolności osób fizycznych w państwach członkowskich – w szczególności prawa do ochrony danych osobowych – w związku z przetwarzaniem danych osobowych mogą utrudniać swobodny przepływ danych osobowych w Unii. Mogą zatem stanowić przeszkodę w prowadzeniu działalności gospodarczej na szczeblu Unii, zakłócać konkurencję oraz utrudniać organom wykonywanie obowiązków nałożonych na nie prawem Unii. Różnice w stopniu ochrony wynikają z różnic we wdrażaniu i stosowaniu dyrektywy 95/46/WE.

(10) Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych. Jeżeli chodzi o przetwarzanie danych osobowych w celu wypełnienia obowiązku prawnego, w celu wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, państwa członkowskie powinny móc zachować lub wprowadzić krajowe przepisy doprecyzowujące stosowanie przepisów niniejszego rozporządzenia. Obok ogólnego, horyzontalnego prawa o ochronie danych wdrażającego dyrektywę 95/46/WE państwa członkowskie przyjęły uregulowania sektorowe w dziedzinach wymagających przepisów bardziej szczegółowych. Niniejsze rozporządzenie umożliwia też państwom członkowskim doprecyzowanie jego przepisów, w tym w odniesieniu do przetwarzania szczególnych kategorii danych osobowych (zwanych dalej „danymi wrażliwymi"). W tym względzie niniejsze rozporządzenie nie wyklucza możliwości określenia w prawie państwa członkowskiego okoliczności dotyczących konkretnych sytuacji związanych z przetwarzaniem danych, w tym dookreślenia warunków, które decydują o zgodności przetwarzania z prawem.

(11) Aby ochrona danych osobowych w Unii była skuteczna, należy wzmocnić i doprecyzować prawa osób, których dane dotyczą, oraz obowiązki podmiotów przetwarzających dane osobowe i decydujących o przetwarzaniu, jak również zapewnić równorzędne uprawnienia w zakresie monitorowania i egzekwowania przepisów o ochronie danych osobowych oraz równorzędne kary za naruszenia tych przepisów w państwach członkowskich.

(12) Art. 16 ust. 2 TFUE powierza Parlamentowi Europejskiemu i Radzie określenie zasad ochrony osób fizycznych w zakresie przetwarzania danych osobowych oraz zasad swobodnego przepływu takich danych.

(13) Aby zapewnić spójny stopień ochrony osób fizycznych w Unii oraz zapobiegać rozbieżnościom hamującym swobodny przepływ danych osobowych na rynku wewnętrznym, należy przyjąć rozporządzenie, które zagwarantuje podmiotom gospodarczym – w tym mikroprzedsiębiorstwom oraz małym i średnim przedsiębiorstwom – pewność prawa i przejrzystość, a osobom fizycznym we wszystkich państwach członkowskich ten sam poziom prawnie egzekwowalnych praw oraz obowiązków i zadań administratorów i podmiotów przetwarzających, które pozwoli spójnie monitorować przetwarzanie danych osobowych, a także które zapewni równoważne kary we wszystkich państwach członkowskich oraz skuteczną współpracę organów nadzorczych z różnych państw członkowskich. Aby rynek wewnętrzny mógł właściwie funkcjonować, swobodny przepływ danych osobowych w Unii nie jest ograniczany ani zakazany z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Z uwagi na szczególną sytuację mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw niniejsze rozporządzenie przewiduje wyjątek dotyczący rejestrowania czynności przetwarzania dla podmiotów zatrudniających mniej niż 250 pracowników. Ponadto zachęca się instytucje i organy Unii, państwa członkowskie i ich organy nadzorcze, by stosując niniejsze rozporządzenie, uwzględniały szczególne potrzeby mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. Rozumienie pojęcia mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw powinno opierać się na art. 2 załącznika do zalecenia Komisji 2003/361/WE[5].

(14) Ochrona zapewniana niniejszym rozporządzeniem powinna mieć zastosowanie do osób fizycznych – niezależnie od ich obywatelstwa czy miejsca zamieszkania – w związku z przetwarzaniem ich danych osobowych. Niniejsze rozporządzenie nie dotyczy przetwarzania danych osobowych dotyczących osób prawnych, w szczególności przedsiębiorstw będących osobami prawnymi, w tym danych o firmie i formie prawnej oraz danych kontaktowych osoby prawnej.

(15) Aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. Ochrona osób fizycznych powinna mieć zastosowanie do zautomatyzowanego przetwarzania danych osobowych oraz do przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych. Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia.

[5] Zalecenie Komisji z dnia 6 maja 2003 r. dotyczące definicji mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (C(2003) 1422) (Dz.U. L 124 z 20.5.2003, s. 36).

(16) Niniejsze rozporządzenie nie ma zastosowania do kwestii ochrony podstawowych praw i wolności ani do swobodnego przepływu danych osobowych w związku z działalnością nieobjętą zakresem prawa Unii, taką jak działalność dotycząca bezpieczeństwa narodowego. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez państwa członkowskie w związku z działaniami związanymi ze wspólną polityką zagraniczną i bezpieczeństwa Unii.

(17) Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii ma zastosowanie rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 45/2001[6]. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych należy dostosować do zasad i przepisów ustanowionych w niniejszym rozporządzeniu oraz stosować w świetle niniejszego rozporządzenia. Aby zapewnić solidne i spójne ramy ochrony danych w Unii, należy po przyjęciu niniejszego rozporządzenia dokonać koniecznych modyfikacji rozporządzenia (WE) nr 45/2001, tak by umożliwić jego stosowanie równocześnie z niniejszym rozporządzeniem.

(18) Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez osobę fizyczną w ramach działalności czysto osobistej lub domowej, czyli bez związku z działalnością zawodową lub handlową. Działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Niniejsze rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej.

(19) Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy w ramach zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych, lub wykonywania kar, w tym w celu ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom, oraz swobodny przepływ takich danych podlegają szczególnemu aktowi prawnemu Unii. Niniejsze rozporządzenie nie powinno zatem mieć zastosowania do czynności przetwarzania w tych celach. Jeżeli jednak dane osobowe przetwarzane przez organy publiczne na mocy niniejszego rozporządzenia są wykorzystywane do tych celów, dane te powinny podlegać szczególnemu aktowi prawnemu Unii, mianowicie dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680[7]. Państwa członkowskie mogą powierzyć właściwym organom w ro-

[6] 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, s. 1).

[7] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestęp-

zumieniu dyrektywy (UE) 2016/680 zadania – które niekoniecznie służą zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu lub ściganiu czynów zabronionych, lub też wykonywaniu kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom – tak by przetwarzanie danych osobowych do tych innych celów, o ile objęte jest zakresem prawa Unii, wchodziło w zakres zastosowania niniejszego rozporządzenia.

Jeżeli chodzi o przetwarzanie danych osobowych przez te właściwe organy do celów wchodzących w zakres niniejszego rozporządzenia, państwa członkowskie powinny mieć możliwość zachowania lub wprowadzenia przepisów szczególnych dostosowujących stosowanie przepisów niniejszego rozporządzenia. W takich przepisach możliwe jest doprecyzowanie szczególnych wymogów przetwarzania danych przez te właściwe organy do tych innych celów, z uwzględnieniem konstytucyjnych, organizacyjnych i administracyjnych struktur danego państwa członkowskiego. Jeżeli przetwarzanie danych osobowych przez podmioty prywatne objęte jest zakresem stosowania niniejszego rozporządzenia, niniejsze rozporządzenie powinno na określonych warunkach umożliwiać państwom członkowskim ograniczenie w swoich przepisach niektórych obowiązków i praw, o ile takie ograniczenie stanowi w demokratycznym społeczeństwie niezbędny i proporcjonalny środek chroniący określone, ważne interesy, w tym bezpieczeństwo publiczne oraz zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, wykrywanie lub ściganie czynów zabronionych, lub też wykonywanie kar, w tym ochronę przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom. Jest to istotne na przykład w związku z przeciwdziałaniem praniu pieniędzy lub w działalności laboratoriów kryminalistycznych.

(20) Niniejsze rozporządzenie ma zastosowanie między innymi do działań sądów i innych organów wymiaru sprawiedliwości, niemniej prawo Unii lub prawo państwa członkowskiego może doprecyzować operacje i procedury przetwarzania danych osobowych przez sądy i inne organy wymiaru sprawiedliwości. Właściwość organów nadzorczych nie powinna dotyczyć przetwarzania danych osobowych przez sądy w ramach sprawowania wymiaru sprawiedliwości – tak by chronić niezawisłość sprawowania wymiaru sprawiedliwości. Powinna istnieć możliwość powierzenia nadzoru nad takimi operacjami przetwarzania danych specjalnym organom w systemie wymiaru sprawiedliwości państwa członkowskiego, organy te powinny w szczególności zapewnić przestrzeganie przepisów niniejszego rozporządzenia, zwiększać w wymiarze sprawiedliwości wiedzę o jego obowiązkach wynikających z niniejszego rozporządzenia oraz rozpatrywać skargi związane z takim operacjami przetwarzania danych.

czości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, swobodnego przepływu tych danych i oraz uchylenia decyzji ramowej Rady 2008/977/WSiSW (zob. s. 89 niniejszego Dziennika Urzędowego).

(21) Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy Parlamentu Europejskiego i Rady 2000/31/WE[8], w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy. Dyrektywa ta ma przyczyniać się do właściwego funkcjonowania rynku wewnętrznego przez zapewnienie swobodnego przepływu usług społeczeństwa informacyjnego między państwami członkowskimi.

(22) Przetwarzanie danych osobowych w kontekście działalności prowadzonej przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii powinno odbywać się zgodnie z niniejszym rozporządzeniem, niezależnie od tego, czy samo przetwarzanie ma miejsce w Unii. Pojęcie „jednostka organizacyjna" zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury. Forma prawna takich struktur, niezależnie od tego, czy chodzi o oddział czy spółkę zależną posiadającą osobowość prawną, nie jest w tym względzie czynnikiem decydującym.

(23) Aby osoby fizyczne nie zostały pozbawione ochrony przysługującej im na mocy niniejszego rozporządzenia, przetwarzanie danych osobowych osób, których dane dotyczą, znajdujących się w Unii, przez administratora lub podmiot przetwarzający, którzy nie posiadają jednostki organizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu, jeżeli czynności przetwarzania wiążą się z oferowaniem takim osobom towarów lub usług, niezależnie od tego, czy pociąga to za sobą płatność. Aby stwierdzić, czy administrator lub podmiot przetwarzający oferują towary lub usługi znajdującym się w Unii osobom, których dane dotyczą, należy ustalić, czy jest oczywiste, że administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim Unii. O ile do ustalenia takiego zamiaru nie wystarczy sama dostępność w Unii strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator, o tyle potwierdzeniem oczywistości faktu, że administrator planuje oferować w Unii towary lub usługi osobom, których dane dotyczą, mogą być czynniki takie, jak posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w Unii.

(24) Przetwarzanie danych osobowych znajdujących się w Unii osób, których dane dotyczą, przez administratora lub podmiot przetwarzający, którzy nie mają jednostki or-

[8] Dyrektywa 2000/31/WE Parlamentu Europejskiego i Rady z dnia 8 czerwca 2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.U. L 178 z 17.7.2000, s. 1).

ganizacyjnej w Unii, powinno podlegać niniejszemu rozporządzeniu także w przypadkach, gdy wiąże się z monitorowaniem zachowania takich osób, których dane dotyczą, o ile zachowanie to ma miejsce w Unii. Aby stwierdzić, czy czynność przetwarzania można uznać za „monitorowanie zachowania" osób, których dane dotyczą, należy ustalić, czy osoby fizyczne są obserwowane w internecie, w tym także czy później potencjalnie stosowane są techniki przetwarzania danych polegające na profilowaniu osoby fizycznej, w szczególności w celu podjęcia decyzji jej dotyczącej lub przeanalizowania lub prognozowania jej osobistych preferencji, zachowań i postaw.

(25) Niniejsze rozporządzenie powinno mieć zastosowanie do administratora niemającego jednostki organizacyjnej w Unii także w przypadkach, gdy na mocy prawa międzynarodowego publicznego stosuje się prawo państwa członkowskiego, na przykład na terenie misji dyplomatycznej lub placówki konsularnej państwa członkowskiego.

(26) Zasady ochrony danych powinny mieć zastosowanie do wszelkich informacji o zidentyfikowanych lub możliwych do zidentyfikowania osobach fizycznych. Spseudonimizowane dane osobowe, które przy użyciu dodatkowych informacji można przypisać osobie fizycznej, należy uznać za informacje o możliwej do zidentyfikowania osobie fizycznej. Aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie rozsądnie prawdopodobne sposoby (w tym wyodrębnienie wpisów dotyczących tej samej osoby), w stosunku do których istnieje uzasadnione prawdopodobieństwo, iż zostaną wykorzystane przez administratora lub inną osobę w celu bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej. Aby stwierdzić, czy dany sposób może być z uzasadnionym prawdopodobieństwem wykorzystany do zidentyfikowania danej osoby, należy wziąć pod uwagę wszelkie obiektywne czynniki, takie jak koszt i czas potrzebne do jej zidentyfikowania, oraz uwzględnić technologię dostępną w momencie przetwarzania danych, jak i postęp technologiczny. Zasady ochrony danych nie powinny więc mieć zastosowania do informacji anonimowych, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.

(27) Niniejsze rozporządzenie nie ma zastosowania do danych osobowych osób zmarłych. Państwa członkowskie mogą przyjąć przepisy o przetwarzaniu danych osobowych osób zmarłych.

(28) Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wy-

wiązać się z obowiązku ochrony danych. Tym samym bezpośrednie wprowadzenie pojęcia „pseudonimizacja" w niniejszym rozporządzeniu nie służy wykluczeniu innych środków ochrony danych.

(29) Aby zachęcić do stosowania pseudonimizacji podczas przetwarzania danych osobowych, należy umożliwić stosowanie u tego samego administratora środków pseudonimizacyjnych niewykluczających ogólnej analizy, o ile administrator ten zastosował środki techniczne i organizacyjne niezbędne do tego, by niniejsze rozporządzenie zostało wdrożone w zakresie danego przetwarzania i by dodatkowe informacje pozwalające przypisać dane osobowe konkretnej osobie, której dane dotyczą, były przechowywane osobno. Administrator przetwarzający dane osobowe powinien wskazać osoby uprawnione.

(30) Osobom fizycznym mogą zostać przypisane identyfikatory internetowe – takie jak adresy IP, identyfikatory plików cookie – generowane przez ich urządzenia, aplikacje, narzędzia i protokoły, czy też inne identyfikatory, generowane na przykład przez etykiety RFID. Może to skutkować zostawianiem śladów, które w szczególności w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskiwanymi przez serwery mogą być wykorzystywane do tworzenia profili i do identyfikowania tych osób.

(31) Organy publiczne, którym ujawnia się dane osobowe w związku z ich prawnym obowiązkiem sprawowania funkcji publicznej (takich jak organy podatkowe, organy celne, finansowe jednostki analityki finansowej, niezależne organy administracyjne czy organy rynków finansowych regulujące i nadzorujące rynki papierów wartościowych), nie powinny być traktowane jako odbiorcy, jeżeli otrzymane przez nie dane osobowe są im niezbędne do przeprowadzenia określonego postępowania w interesie ogólnym zgodnie z prawem Unii lub prawem państwa członkowskiego. Żądanie ujawnienia danych osobowych, z którym występują takie organy publiczne, powinno zawsze mieć formę pisemną, być uzasadnione, mieć charakter wyjątkowy, nie powinno dotyczyć całego zbioru danych ani prowadzić do połączenia zbiorów danych. Przetwarzając otrzymane dane osobowe, takie organy powinny przestrzegać mających zastosowanie przepisów o ochronie danych, zgodnie z celami przetwarzania.

(32) Zgoda powinna być wyrażona w drodze jednoznacznej, potwierdzającej czynności, która wyraża odnoszące się do określonej sytuacji dobrowolne, świadome i jednoznaczne przyzwolenie osoby, których dane dotyczą, na przetwarzanie dotyczących jej danych osobowych i która ma na przykład formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Może to polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego lub też na in-

nym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba, której dane dotyczą, zaakceptowała proponowane przetwarzanie jej danych osobowych. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie powinny zatem oznaczać zgody. Zgoda powinna dotyczyć wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie te cele. Jeżeli osoba, której dane dotyczą, ma wyrazić zgodę w odpowiedzi na elektroniczne zapytanie, zapytanie takie musi być jasne, zwięzłe i nie zakłócać niepotrzebnie korzystania z usługi, której dotyczy.

(33) W momencie zbierania danych często nie da się w pełni zidentyfikować celu przetwarzania danych osobowych na potrzeby badań naukowych. Dlatego osoby, których dane dotyczą, powinny móc wyrazić zgodę na niektóre obszary badań naukowych, o ile badania te są zgodne z uznanymi normami etycznymi w zakresie badań naukowych. Osoby, których dane dotyczą, powinny móc wyrazić zgodę tylko na niektóre obszary badań lub elementy projektów badawczych, o ile umożliwia to zamierzony cel.

(34) Dane genetyczne należy zdefiniować jako dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, uzyskane z analizy próbki biologicznej danej osoby fizycznej, w szczególności z analizy chromosomów, kwasu dezoksyrybonukleinowego (DNA) lub kwasu rybonukleinowego (RNA) lub z analizy innych elementów umożliwiających pozyskanie równoważnych informacji.

(35) Do danych osobowych dotyczących zdrowia należy zaliczyć wszystkie dane o stanie zdrowia osoby, której dane dotyczą, ujawniające informacje o przeszłym, obecnym lub przyszłym stanie fizycznego lub psychicznego zdrowia osoby, której dane dotyczą. Do danych takich należą informacje o danej osobie fizycznej zbierane podczas jej rejestracji do usług opieki zdrowotnej lub podczas świadczenia jej usług opieki zdrowotnej, jak to określa dyrektywa Parlamentu Europejskiego i Rady 2011/24/UE[9]; numer, symbol lub oznaczenie przypisane danej osobie fizycznej w celu jednoznacznego zidentyfikowania tej osoby fizycznej do celów zdrowotnych; informacje pochodzące z badań laboratoryjnych lub lekarskich części ciała lub płynów ustrojowych, w tym danych genetycznych i próbek biologicznych; oraz wszelkie informacje, na przykład o chorobie, niepełnosprawności, ryzyku choroby, historii medycznej, leczeniu klinicznym lub stanie fizjologicznym lub biomedycznym osoby, której dane dotyczą, niezależnie od ich źródła, którym może być na przykład lekarz lub inny pracownik służby zdrowia, szpital, urządzenie medyczne lub badanie diagnostyczne in vitro.

[9] 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, s. 45).

(36) Główną jednostką organizacyjną administratora w Unii powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, chyba że decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej administratora w Unii, w którym to przypadku za główną jednostkę organizacyjną należy uznać tą drugą jednostkę organizacyjną. Główną jednostkę organizacyjną administratora w Unii należy określać na podstawie obiektywnych kryteriów; powinna ona oznaczać skuteczne i faktycznie zarządzanie za pośrednictwem stabilnych struktur polegające na podejmowaniu najważniejszych decyzji co do celów i sposobów przetwarzania. Kryterium to nie powinno zależeć od faktu, czy przetwarzanie danych osobowych odbywa się w tej lokalizacji. Obecność i wykorzystywanie środków technicznych i technologii do przetwarzania danych osobowych lub do czynności przetwarzania nie stanowią same w sobie o głównej jednostce organizacyjnej, nie są więc kryteriami decydującymi o jej określeniu. Główną jednostką organizacyjną podmiotu przetwarzającego powinno być miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli nie ma on centralnej administracji w Unii – miejsce, w którym odbywają się główne czynności przetwarzania w Unii. Jeżeli sprawa dotyczy zarówno administratora, jak i podmiotu przetwarzającego, właściwym wiodącym organem nadzorczym powinien pozostać organ nadzorczy państwa członkowskiego, w którym administrator ma główną jednostkę organizacyjną, ale organ nadzorczy podmiotu przetwarzającego powinien być uznawany za organ nadzorczy, którego sprawa dotyczy, i powinien uczestniczyć w procedurze współpracy przewidzianej w niniejszym rozporządzeniu. Organy nadzorcze państwa członkowskiego lub państw członkowskich, w których podmiot przetwarzający ma co najmniej jedną jednostkę organizacyjną, nie powinny być w żadnym przypadku uznawane za organy nadzorcze, których sprawa dotyczy, jeżeli projekt decyzji dotyczy wyłącznie administratora. Jeżeli przetwarzania dokonuje grupa przedsiębiorstw, za jej główną jednostkę organizacyjną należy uznać główną jednostkę organizacyjną przedsiębiorstwa sprawującego kontrolę, chyba że cel i sposoby przetwarzania określa inne przedsiębiorstwo.

(37) Grupa przedsiębiorstw powinna obejmować przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa kontrolowane, przy czym przedsiębiorstwo sprawujące kontrolę powinno być przedsiębiorstwem, które może wywierać dominujący wpływ na pozostałe przedsiębiorstwa ze względu na przykład na strukturę właścicielską, udział finansowy lub przepisy regulujące jego działalność, lub też uprawnienia do nakazywania wdrożenia przepisów o ochronie danych osobowych. Za grupę przedsiębiorstw należy uznać przedsiębiorstwo kontrolujące przetwarzanie danych osobowych w przedsiębiorstwach powiązanych z nim, wraz z tymi przedsiębiorstwami.

(38) Szczególnej ochrony danych osobowych wymagają dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im

w związku z przetwarzaniem danych osobowych. Taka szczególna ochrona powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich. Zgoda osoby sprawującej władzę rodzicielską lub opiekę nie powinna być konieczna w przypadku usług profilaktycznych lub doradczych oferowanych bezpośrednio dziecku.

(39) Wszelkie przetwarzanie danych osobowych powinno być zgodne z prawem i rzetelne. Dla osób fizycznych powinno być przejrzyste, że dotyczące ich dane osobowe są zbierane, wykorzystywane, przeglądane lub w inny sposób przetwarzane oraz w jakim stopniu te dane osobowe są lub będą przetwarzane. Zasada przejrzystości wymaga, by wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych były łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem. Zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o tożsamości administratora i celach przetwarzania oraz innych informacji mających zapewnić rzetelność i przejrzystość przetwarzania w stosunku do osób, których sprawa dotyczy, a także prawa takich osób do uzyskania potwierdzenia i informacji o przetwarzanych danych osobowych ich dotyczących. Osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem. W szczególności konkretne cele przetwarzania danych osobowych powinny być wyraźne, uzasadnione i określone w momencie ich zbierania. Dane osobowe powinny być adekwatne, stosowne i ograniczone do tego, co niezbędne do celów, dla których są one przetwarzane. Wymaga to w szczególności zapewnienia ograniczenia okresu przechowywania danych do ścisłego minimum. Dane osobowe powinny być przetwarzane tylko w przypadkach, gdy celu przetwarzania nie można w rozsądny sposób osiągnąć innymi sposobami. Aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu. Należy podjąć wszelkie rozsądne działania zapewniające sprostowanie lub usunięcie danych osobowych, które są nieprawidłowe. Dane osobowe powinny być przetwarzane w sposób zapewniający im odpowiednie bezpieczeństwo i odpowiednią poufność, w tym ochronę przed nieuprawnionym dostępem do nich i do sprzętu służącego ich przetwarzaniu oraz przed nieuprawnionym korzystaniem z tych danych i z tego sprzętu.

(40) Aby przetwarzanie danych było zgodne z prawem, powinno się odbywać na podstawie zgody osoby, której dane dotyczą, lub na innej uzasadnionej podstawie przewidzianej prawem: albo w niniejszym rozporządzeniu, albo w innym akcie prawnym Unii lub w prawie państwa członkowskiego, o których mowa w niniejszym rozporządzeniu, w tym musi się ono odbywać z poszanowaniem obowiązku

prawnego, któremu podlega administrator, lub z poszanowaniem umowy, której stroną jest osoba, której dane dotyczą, lub w celu podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy.

(41) W przypadku gdy w niniejszym rozporządzeniu jest mowa o podstawie prawnej lub akcie prawnym, niekoniecznie wymaga to przyjęcia aktu prawnego przez parlament, z zastrzeżeniem wymogów wynikających z porządku konstytucyjnego danego państwa członkowskiego. Taka podstawa prawna lub taki akt prawny powinny być jasne i precyzyjne, a ich zastosowanie przewidywalne dla osób im podlegających – jak wymaga tego orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej (zwanego dalej „Trybunałem Sprawiedliwości") i Europejskiego Trybunału Praw Człowieka.

(42) Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania. W szczególności w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu. Zgodnie z dyrektywą Rady 93/13/EWG[10] oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków. Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych. Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.

(43) Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem, w szczególności gdy administrator jest organem publicznym i dlatego jest mało prawdopodobne, by w tej konkretnej sytuacji zgodę wyrażono dobrowolnie we wszystkich przypadkach. Zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych osobowych, mimo że w danym przypadku byłoby to stosowne, lub jeżeli od zgody uzależnione jest wykonanie umowy – w tym świadczenie usługi – mimo że do jej wykonania zgoda nie jest niezbędna.

(44) Przetwarzanie powinno być zgodne z prawem, jeżeli jest ono niezbędne w związku z zawarciem umowy lub zamiarem zawarcia umowy.

[10] Dyrektywa Rady 93/13/EWG z dnia 5 kwietnia 1993 r. w sprawie nieuczciwych warunków w umowach konsumenckich (Dz.U. L 95, 21.4.1993, s. 29).

(45) Jeżeli przetwarzanie odbywa się w celu wypełnienia obowiązku prawnego, któremu podlega administrator, lub jeżeli jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, podstawę przetwarzania powinno stanowić prawo Unii lub prawo państwa członkowskiego. Niniejsze rozporządzenie nie nakłada wymogu, aby dla każdego indywidualnego przetwarzania istniało szczegółowe uregulowanie prawne. Wystarczyć może to, że dane uregulowanie prawne stanowi podstawę różnych operacji przetwarzania wynikających z obowiązku prawnego, któremu podlega administrator, lub że przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej. Prawo Unii lub prawo państwa członkowskiego powinno określać także cel przetwarzania. Ponadto prawo to może doprecyzowywać ogólne warunki określone w niniejszym rozporządzeniu dotyczące zgodności przetwarzania z prawem, określać sposoby wskazywania administratora, rodzaj danych osobowych podlegających przetwarzaniu, osoby, których dane dotyczą, podmioty, którym można ujawniać dane osobowe, ograniczenia celu, okres przechowywania oraz inne środki zapewniające zgodność z prawem i rzetelność przetwarzania. Prawo Unii lub prawo państwa członkowskiego powinno określać także, czy administratorem wykonującym zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powinien być organ publiczny czy inna osoba fizyczna lub prawna podlegająca prawu publicznemu lub prawu prywatnemu, na przykład zrzeszenie zawodowe, jeżeli uzasadnia to interes publiczny, w tym cele zdrowotne, takie jak zdrowie publiczne, ochrona socjalna oraz zarządzanie usługami opieki zdrowotnej.

(46) Przetwarzanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne do ochrony interesu, który ma istotne znaczenie dla życia osoby, której dane dotyczą, lub innej osoby fizycznej. Żywotny interes innej osoby fizycznej powinien zasadniczo być podstawą przetwarzania danych osobowych wyłącznie w przypadkach, gdy ewidentnie przetwarzania tego nie da się oprzeć na innej podstawie prawnej. Niektóre rodzaje przetwarzania mogą służyć zarówno ważnemu interesowi publicznemu, jak i żywotnym interesom osoby, której dane dotyczą, na przykład gdy przetwarzanie jest niezbędne do celów humanitarnych, w tym monitorowania epidemii i ich rozprzestrzeniania się lub w nadzwyczajnych sytuacjach humanitarnych, w szczególności w przypadku klęsk żywiołowych i katastrof spowodowanych przez człowieka.

(47) Podstawą prawną przetwarzania mogą być prawnie uzasadnione interesy administratora, w tym administratora, któremu mogą zostać ujawnione dane osobowe, lub strony trzeciej, o ile w świetle rozsądnych oczekiwań osób, których dane dotyczą, opartych na ich powiązaniach z administratorem nadrzędne nie są interesy lub podstawowe prawa i wolności osoby, której dane dotyczą. Taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i od-

powiedni rodzaj powiązania między osobą, której dane dotyczą, a administratorem, na przykład gdy osoba, której dane dotyczą, jest klientem administratora lub działa na jego rzecz. Aby stwierdzić istnienie prawnie uzasadnionego interesu, należałoby w każdym przypadku przeprowadzić dokładną ocenę, w tym ocenę tego, czy w czasie i w kontekście, w którym zbierane są dane osobowe, osoba, której dane dotyczą, ma rozsądne przesłanki by spodziewać się, że może nastąpić przetwarzanie danych w tym celu. Interesy i prawa podstawowe osoby, której dane dotyczą, mogą być nadrzędne wobec interesu administratora danych w szczególności w przypadkach, gdy dane osobowe są przetwarzane w sytuacji, w której osoby, których dane dotyczą, nie mają rozsądnych przesłanek, by spodziewać się dalszego przetwarzania. Ponieważ dla organów publicznych podstawę prawną przetwarzania danych osobowych powinien określić ustawodawca, prawnie uzasadniony interes administratora nie powinien mieć zastosowania jako podstawa prawna do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań. Prawnie uzasadnionym interesem administratora, którego sprawa dotyczy, jest również przetwarzanie danych osobowych bezwzględnie niezbędne do zapobiegania oszustwom. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego.

(48) Administratorzy, którzy są częścią grupy przedsiębiorstw lub instytucji powiązanych z podmiotem centralnym, mogą mieć prawnie uzasadniony interes w przesyłaniu danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych osobowych klientów lub pracowników. Pozostaje to bez wpływu na ogólne zasady przekazywania danych osobowych w ramach grupy przedsiębiorstw przedsiębiorstwu mieszczącemu się w państwie trzecim.

(49) Przetwarzanie danych osobowych w zakresie bezwzględnie niezbędnym i proporcjonalnym do zapewnienia bezpieczeństwa sieci i informacji – tj. zapewnienia odporności sieci lub systemu informacyjnego na danym poziomie poufności na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych – oraz bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych poprzez te sieci i systemy przez organy publiczne, zespoły reagowania na zagrożenia komputerowe, zespoły reagowania na komputerowe incydenty naruszające bezpieczeństwo, dostawców sieci i usług łączności elektronicznej oraz dostawców technologii i usług w zakresie bezpieczeństwa jest prawnie uzasadnionym interesem administratora, którego sprawa dotyczy. Może to obejmować na przykład zapobieganie nieuprawnionemu dostępowi do sieci łączności elektronicznej i rozprowadzaniu złośliwych kodów, przerywanie ataków typu „odmowa usługi", a także przeciwdziałanie uszkodzeniu systemów komputerowych i systemów łączności elektronicznej.

(50) Przetwarzanie danych osobowych do celów innych niż cele, w których dane te zostały pierwotnie zebrane, powinno być dozwolone wyłącznie w przypadkach, gdy jest zgodne z celami, w których dane osobowe zostały pierwotnie zebrane. W takim przypadku nie jest wymagana odrębna podstawa prawna inna niż podstawa prawna, która umożliwiła zbieranie danych osobowych. Jeżeli przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi, prawo Unii lub prawo państwa członkowskiego mogą określać i precyzować zadania i cele, w których dalsze przetwarzanie powinno być uznawane za zgodne z prawem i z pierwotnymi celami. Dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinny być uznawane za operacje przetwarzania zgodne z prawem i z pierwotnymi celami. Podstawa prawna przetwarzania danych osobowych przewidziana prawem Unii lub prawem państwa członkowskiego może być również podstawą prawną dalszego przetwarzania. Aby ustalić, czy cel dalszego przetwarzania danych osobowych jest zgodny z celem, w którym dane te zostały pierwotnie zebrane, administrator – po spełnieniu wszystkich wymogów warunkujących zgodność pierwotnego przetwarzania z prawem – powinien uwzględnić między innymi: wszelkie powiązania pomiędzy tymi celami a celami zamierzonego dalszego przetwarzania; kontekst, w którym dane osobowe zostały zebrane, w szczególności rozsądne przesłanki pozwalające osobom, których dane dotyczą, oczekiwać dalszego wykorzystania danych oparte na rodzaju ich powiązania z administratorem; charakter danych osobowych; konsekwencje zamierzonego dalszego przetwarzania dla osób, których dane dotyczą; oraz istnienie odpowiednich zabezpieczeń zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania.

Jeżeli osoba, której dane dotyczą, wyraziła zgodę lub jeżeli przetwarzanie ma za podstawę prawo Unii lub prawo państwa członkowskiego stanowiące w demokratycznym społeczeństwie niezbędny i proporcjonalny środek, który zapewnia w szczególności realizację ważnych celów leżących w ogólnym interesie publicznym, administrator powinien móc dokonać dalszego przetwarzania danych osobowych, bez względu na jego zgodność z pierwotnymi celami. W każdym przypadku należy zapewnić stosowanie zasad przewidzianych w niniejszym rozporządzeniu, w szczególności stosowanie zasady informowania osoby, której dane dotyczą, o tych innych celach oraz o jej prawach, w tym prawie do sprzeciwu. Wskazanie przez administratora ewentualnych czynów zabronionych czy zagrożeń dla bezpieczeństwa publicznego oraz przesłanie w indywidualnym przypadku – lub w różnych przypadkach związanych z tym samym czynem zabronionym lub zagrożeniem dla bezpieczeństwa publicznego – odpowiednich danych osobowych właściwemu organowi należy uznać za zrealizowanie przez administratora prawnie uzasadnionego interesu. Jednak takie przesłanie w prawnie uzasadnionym interesie administratora lub dalsze przetwarzanie danych osobowych powinno być zabronione, jeżeli jest niezgodne z prawnym, zawodowym lub innym wiążącym obowiązkiem zachowania tajemnicy.

(51) Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe w świetle podstawowych praw i wolności, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować poważne ryzyko dla podstawowych praw i wolności. Do takich danych osobowych powinny zaliczać się dane osobowe ujawniające pochodzenie rasowe lub etniczne, przy czym użycie w niniejszym rozporządzeniu terminu „pochodzenie rasowe" nie oznacza, że Unia akceptuje teorie sugerujące istnienie osobnych ras ludzkich. Przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w przypadkach, gdy są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości. Takich danych osobowych nie należy przetwarzać, chyba że niniejsze rozporządzenie dopuszcza ich przetwarzanie w szczególnych przypadkach, przy czym należy uwzględnić, że prawo państw członkowskich może obejmować przepisy szczegółowe o ochronie danych dostosowujące zastosowanie przepisów niniejszego rozporządzenia tak, by można było wypełnić obowiązki prawne lub wykonać zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Oprócz wymogów szczegółowych mających zastosowanie do takiego przetwarzania, zastosowanie powinny mieć zasady ogólne i inne przepisy niniejszego rozporządzenia, w szczególności jeżeli chodzi o warunki zgodności przetwarzania z prawem. Należy wyraźnie przewidzieć wyjątki od ogólnego zakazu przetwarzania takich szczególnych kategorii danych osobowych, m.in. w razie wyraźnej zgody osoby, której dane dotyczą, lub ze względu na szczególne potrzeby, w szczególności gdy przetwarzanie danych odbywa się w ramach uzasadnionych działań niektórych zrzeszeń lub fundacji, których celem jest umożliwienie korzystania z podstawowych wolności.

(52) Należy również zezwolić na wyjątki od zakazu przetwarzania szczególnych kategorii danych osobowych – o ile przewiduje to prawo Unii lub prawo państwa członkowskiego i podlega to odpowiednim zabezpieczeniom chroniącym dane osobowe i inne prawa podstawowe – jeżeli uzasadnia to interes publiczny, w szczególności polegający na przetwarzaniu danych osobowych w dziedzinie prawa pracy, prawa zabezpieczenia społecznego, w tym emerytur, oraz do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego, zapobiegania chorobom zakaźnym i innym poważnym zagrożeniom zdrowotnym. Taki wyjątek może być przewidziany ze względu na cele zdrowotne, w tym związane ze zdrowiem publicznym oraz zarządzaniem usługami opieki zdrowotnej, w szczególności zapewnianiem jakości i ekonomiczności procedur stosowanych do rozstrzygania roszczeń w sprawie świadczeń i usług w ramach systemu ubezpieczeń zdrowotnych, lub ze względu na cele archiwalne w interesie publicznym, cele badań naukowych lub historycznych lub cele statystyczne. Należy także przewidzieć wyjątek pozwalający przetwarzać takie dane osobowe, jeżeli jest to niezbędne do ustalenia, dochodzenia lub obrony roszczeń w postępowaniu sądowym, administracyjnym lub też innym postępowaniu pozasądowym.

(53) Szczególne kategorie danych osobowych zasługujące na większą ochronę powinny być przetwarzane do celów zdrowotnych wyłącznie w przypadkach, gdy jest to niezbędne do realizacji tych celów z korzyścią dla osób fizycznych i ogółu społeczeństwa, w szczególności w kontekście zarządzania usługami i systemami opieki zdrowotnej i zabezpieczenia społecznego, w tym przetwarzania takich danych przez organy zarządcze i centralne krajowe organy ds. zdrowia do celów kontroli jakości, pozyskiwania informacji zarządczych oraz ogólnego krajowego i lokalnego nadzoru nad systemem opieki zdrowotnej i zabezpieczenia społecznego oraz zapewniania ciągłości opieki zdrowotnej lub zabezpieczenia społecznego oraz transgranicznej opieki zdrowotnej lub do celów bezpieczeństwa, monitorowania i ostrzegania zdrowotnego lub do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, które mają podstawę w prawie Unii lub prawie państwa członkowskiego i służą interesowi publicznemu, a także na potrzeby analiz prowadzonych w interesie publicznym w dziedzinie zdrowia publicznego. Niniejsze rozporządzenie powinno zatem przewidywać zharmonizowane warunki przetwarzania szczególnych kategorii danych osobowych dotyczących zdrowia, ze względu na szczególne potrzeby, w szczególności gdy dane takie są przetwarzane w określonych celach zdrowotnych przez osoby podlegające prawnemu obowiązkowi zachowania tajemnicy zawodowej. Prawo Unii lub prawo państwa członkowskiego powinny przewidywać konkretne, odpowiednie środki chroniące prawa podstawowe i dane osobowe osób fizycznych. Państwa członkowskie powinny móc zachować lub wprowadzić dalsze warunki, w tym ograniczenia, przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. Warunki te nie powinny jednak utrudniać swobodnego przepływu danych osobowych w Unii, jeżeli odnoszą się do transgranicznego przetwarzania takich danych.

(54) Niezbędne z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego może być przetwarzanie szczególnych kategorii danych osobowych bez zgody osoby, której dane dotyczą. Przetwarzanie takie powinno podlegać konkretnym, odpowiednim środkom chroniącym prawa i wolności osób fizycznych. W tym kontekście „zdrowie publiczne" należy interpretować zgodnie z definicją z rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 1338/2008[11], czyli jako wszystkie elementy związane ze zdrowiem, mianowicie stan zdrowia, w tym zachorowalność i niepełnosprawność, czynniki warunkujące stan zdrowia, potrzeby w zakresie opieki zdrowotnej, zasoby opieki zdrowotnej, oferowane usługi opieki zdrowotnej i powszechny dostęp do nich, wydatki na opiekę zdrowotną i sposób jej finansowania oraz przyczyny zgonów. Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego nie powinno skutkować przetwarzaniem danych osobowych do innych celów przez strony trzecie, takie jak pracodawcy, czy zakłady ubezpieczeń i banki.

[11] Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1338/2008 z dnia 16 grudnia 2008 r. w sprawie statystyk Wspólnoty w zakresie zdrowia publicznego oraz zdrowia i bezpieczeństwa w pracy (Dz.U. L 354 z 31.12.2008, s. 70).

(55) Przetwarzanie danych osobowych przez organy publiczne do celów – określonych w prawie konstytucyjnym lub prawie międzynarodowym publicznym – oficjalnie uznanych związków wyznaniowych odbywa się w interesie publicznym.

(56) Jeżeli w ramach działań związanych z wyborami funkcjonowanie systemu demokratycznego w państwie członkowskim wymaga zbierania przez partie polityczne danych osobowych dotyczących poglądów politycznych obywateli, można zezwolić na przetwarzanie tych danych z uwagi na względy interesu publicznego pod warunkiem ustanowienia odpowiednich zabezpieczeń.

(57) Jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby fizycznej, nie powinien on mieć obowiązku uzyskania dodatkowych informacji w celu zidentyfikowania osoby, której dane dotyczą, wyłącznie po to, by zastosować się do przepisów niniejszego rozporządzenia. Administrator nie powinien jednak odmawiać przyjęcia dodatkowych informacji od osoby, której dane dotyczą, by ułatwić jej wykonywanie jej praw. Weryfikacja tożsamości powinna obejmować cyfrową identyfikację osoby, której dane dotyczą, na przykład poprzez mechanizm uwierzytelniania, taki jak te same dane uwierzytelniające, których osoba, której dane dotyczą, używa, by zalogować się do usług internetowych oferowanych przez administratora.

(58) Zasada przejrzystości wymaga, by wszelkie informacje kierowane do ogółu społeczeństwa lub osoby, której dane dotyczą, były zwięzłe, łatwo dostępne i zrozumiałe, by były formułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane. Informacje te mogą być przekazywane w formie elektronicznej, na przykład za pomocą strony internetowej, gdy są kierowane do ogółu społeczeństwa. Dotyczy to w szczególności sytuacji, gdy duża liczba podmiotów i złożoność technologiczna działań sprawiają, że osobie, której dane dotyczą, trudno jest dowiedzieć się i zrozumieć, czy dotyczące jej dane osobowe są zbierane, przez kogo oraz w jakim celu, na przykład w przypadku reklamy w internecie. Zważywszy że dzieci zasługują na szczególną ochronę, wszelkie informacje i komunikaty – gdy przetwarzanie dotyczy dziecka – powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć.

(59) Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia, w tym mechanizmy żądania – i gdy ma to zastosowanie bezpłatnego uzyskiwania – w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu. Administrator powinien zapewnić możliwość wnoszenia odnośnych żądań także drogą elektroniczną, w szczególności gdy dane osobowe są przetwarzane drogą elektroniczną. Administrator powinien być zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej

zwłoki – najpóźniej w terminie miesiąca, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny.

(60) Zasady rzetelnego i przejrzystego przetwarzania wymagają, by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach. Administrator powinien podać osobie, której dane dotyczą, wszelkie inne informacje niezbędne do zapewnienia rzetelności i przejrzystości przetwarzania, uwzględniając konkretne okoliczności i konkretny kontekst przetwarzania danych osobowych. Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania. Jeżeli gromadzi się dane osobowe od osoby, której dane dotyczą, należy ją też poinformować, czy ma ona obowiązek je podać, oraz o konsekwencjach ich niepodania. Informacje te można przekazać w połączeniu ze standardowymi znakami graficznymi, które w widoczny, zrozumiały i czytelny sposób przedstawią sens zamierzonego przetwarzania. Jeżeli znaki te są przedstawione elektronicznie, powinny nadawać się do odczytu maszynowego.

(61) Informacje o przetwarzaniu danych osobowych dotyczących osoby, której dane dotyczą, należy przekazać tej osobie w momencie zbierania danych, a jeżeli danych nie uzyskuje się od osoby, której dane dotyczą, lecz z innego źródła – w rozsądnym terminie, zależnie od okoliczności. Jeżeli dane osobowe można zgodnie z prawem ujawnić innemu odbiorcy, należy poinformować o tym osobę, której dane dotyczą, w momencie pierwszorazowego ujawnienia danych temu odbiorcy. Jeżeli administrator planuje przetwarzać dane osobowe w celu innym niż cel, w których dane osobowe zostały zebrane, powinien on przed takim dalszym przetwarzaniem poinformować osobę, której dane dotyczą, o tym innym celu oraz dostarczyć jej innych niezbędnych informacji. Jeżeli osobie, której dane dotyczą, nie można podać pochodzenia danych osobowych, ponieważ korzystano z różnych źródeł, informacje należy przedstawić w sposób ogólny.

(62) Nałożenie obowiązku udzielenia informacji nie jest jednak konieczne, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami, jeżeli utrwalenie lub ujawnienie danych są wyraźnie przewidziane prawem, lub jeżeli poinformowanie osoby, której dane dotyczą, okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Sytuacja braku możliwości lub niewspółmiernie dużego wysiłku może zachodzić w szczególności przypadku, gdy przetwarzanie służy celom archiwalnym w interesie publicznym, celom badań naukowych lub historycznych lub celom statystycznym. Uwzględnić przy tym należy liczbę osób, których dane dotyczą, okres przechowywania danych oraz wszelkie przyjęte odpowiednie zabezpieczenia.

(63) Każda osoba fizyczna powinna mieć prawo dostępu do zebranych danych jej dotyczących oraz powinna mieć możliwość łatwego wykonywania tego prawa w rozsądnych odstępach czasu, by mieć świadomość przetwarzania i móc zweryfikować zgodność przetwarzania z prawem. Obejmuje to prawo dostępu osób, których dane

dotyczą, do danych dotyczących ich zdrowia, na przykład do danych w dokumentacji medycznej zawierającej takie informacje, jak diagnoza, wyniki badań, oceny dokonywane przez lekarzy prowadzących, stosowane terapie czy przeprowadzone zabiegi. Dlatego też każda osoba, której dane dotyczą, powinna mieć prawo do wiedzy i informacji, w szczególności w zakresie celów, w jakich dane osobowe są przetwarzane, w miarę możliwości okresu, przez jaki dane osobowe są przetwarzane, odbiorców danych osobowych, założeń ewentualnego zautomatyzowanego przetwarzania danych osobowych oraz, przynajmniej w przypadku profilowania, konsekwencji takiego przetwarzania. W miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji. Jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie.

(64) Administrator powinien skorzystać z wszelkich rozsądnych środków w celu zweryfikowania tożsamości żądającej dostępu osoby, której dane dotyczą, w szczególności w kontekście usług internetowych i identyfikatorów internetowych. Administrator nie powinien zatrzymywać danych osobowych wyłącznie w celu reagowania na ewentualne żądania.

(65) Każda osoba fizyczna powinna mieć prawo do sprostowania danych osobowych jej dotyczących oraz prawo do „bycia zapomnianym", jeżeli zatrzymywanie takich danych narusza niniejsze rozporządzenie, prawo Unii lub prawo państwa członkowskiego, któremu podlega administrator. Osoba, której dane dotyczą, powinna w szczególności mieć prawo do tego, by jej dane osobowe zostały usunięte i przestały być przetwarzane, jeżeli dane te nie są już niezbędne do celów, w których były zbierane lub w inny sposób przetwarzane, jeżeli osoba, której dane dotyczą, cofnęła zgodę lub jeżeli wniosła sprzeciw wobec przetwarzania danych osobowych jej dotyczących, lub jeżeli przetwarzanie jej danych osobowych nie jest z innego powodu zgodne z niniejszym rozporządzeniem. Prawo to ma znaczenie w przypadkach, gdy osoba, której dane dotyczą, wyraziła zgodę jako dziecko, gdy nie była w pełni świadoma ryzyka związanego z przetwarzaniem, a w późniejszym czasie chce usunąć takie dane osobowe, w szczególności z internetu. Osoba, której dane dotyczą, powinna móc wykonywać to prawo, mimo że już nie jest dzieckiem. Niemniej dalsze zatrzymywanie danych osobowych powinno być uznane za zgodne z prawem, jeżeli jest niezbędne do korzystania z wolności wypowiedzi i informacji, do wywiązania się z obowiązku prawnego, do wykonania zadania realizowanego w interesie publicznym lub w ra-

mach sprawowania władzy publicznej powierzonej administratorowi, z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego, do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.

(66) Aby wzmocnić prawo do „bycia zapomnianym" w internecie, należy rozszerzyć prawo do usunięcia danych poprzez zobowiązanie administratora, który upublicznił te dane osobowe, do poinformowania administratorów, którzy przetwarzają takie dane osobowe o usunięciu wszelkich łączy do tych danych, kopii tych danych osobowych lub ich replikacji. Spełniając ten obowiązek administrator powinien podjąć racjonalne działania z uwzględnieniem dostępnych technologii i dostępnych mu środków, w tym dostępnych środków technicznych, w celu poinformowania administratorów, którzy przetwarzają dane osobowe, o żądaniu osoby, której dane dotyczą.

(67) Wśród metod pozwalających ograniczyć przetwarzanie danych osobowych mogą się znaleźć między innymi: czasowe przeniesienie wybranych danych osobowych do innego systemu przetwarzania, uniemożliwienie użytkownikom dostępu do wybranych danych, lub czasowe usunięcie opublikowanych danych ze strony internetowej. W zautomatyzowanych zbiorach danych przetwarzanie należy zasadniczo ograniczyć środkami technicznymi w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane. Fakt ograniczenia przetwarzania danych osobowych należy wyraźnie zaznaczyć w systemie.

(68) Aby zyskać większą kontrolę nad swoimi danymi w ramach zautomatyzowanego przetwarzania danych osobowych, osoba, której dane dotyczą, powinna także mieć możliwość otrzymywania dotyczących jej danych osobowych, których dostarczyła administratorowi, w ustrukturyzowanym, powszechnie używanym, nadającym się do odczytu maszynowego i interoperacyjnym formacie oraz przesyłania ich innemu administratorowi. Administratorów danych należy zachęcać do opracowywania interoperacyjnych formatów, które umożliwiają przenoszenie danych. Prawo to powinno mieć zastosowanie w przypadkach, gdy osoba, której dane dotyczą, dostarczyła danych osobowych za własną zgodą lub gdy przetwarzanie jest niezbędne do wykonania umowy. Nie powinno mieć zastosowania, jeżeli przetwarzanie opiera się na innej podstawie prawnej niż zgoda lub umowa. Prawa tego – z uwagi na jego charakter – nie powinno się wykonywać w stosunku do administratorów przetwarzających dane osobowe w ramach wykonywania obowiązków publicznych. Dlatego nie powinno ono mieć zastosowania w przypadkach, gdy przetwarzanie danych osobowych jest niezbędne do wywiązania się z obowiązku prawnego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przysługujące osobie, której dane dotyczą, prawo do przesłania lub otrzymania swoich danych osobowych nie powinno nakładać na administratorów obowiązku prowadzenia lub wprowadzenia kompatybilnych tech-

nicznie systemów przetwarzania. Jeżeli określony zestaw danych osobowych odnosi się do więcej niż jednej osoby, której dane dotyczą, prawo do otrzymania danych osobowych nie powinno powodować uszczerbku dla praw i wolności innych osób, których dane dotyczą, na podstawie niniejszego rozporządzenia. Prawo to powinno ponadto pozostawać bez uszczerbku dla prawa osoby, której dane dotyczą, do spowodowania, by dane osobowe zostały usunięte, oraz bez uszczerbku dla ograniczeń tego prawa określonych w niniejszym rozporządzeniu i nie powinno w szczególności skutkować usunięciem danych osobowych dotyczących osoby, której dane dotyczą, których osoba ta dostarczyła do wykonania umowy, o ile i w takim zakresie, w jakim te dane osobowe są niezbędne do wykonania tej umowy. O ile jest to technicznie możliwe, osoba, której dane dotyczą, powinna mieć prawo do spowodowania, by dane osobowe zostały przesłane przez jednego administratora bezpośrednio innemu administratorowi.

(69) Nawet jeżeli dane osobowe mogą być przetwarzane zgodnie z prawem, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub ze względu na prawnie uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, powinno przysługiwać prawo sprzeciwu wobec przetwarzania danych osobowych dotyczących jej szczególnej sytuacji. Za wykazanie, że ważne prawnie uzasadnione interesy administratora mają nadrzędny charakter wobec interesów lub podstawowych praw i wolności osoby, której dane dotyczą, powinien odpowiadać administrator.

(70) Jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, powinna mieć prawo wnieść w dowolnym momencie, bezpłatnie sprzeciw wobec tego przetwarzania, pierwotnego lub dalszego – w tym profilowania, o ile jest ono powiązane z marketingiem bezpośrednim. Prawo to powinno zostać wyraźnie podane do wiadomości osobie, której dane dotyczą, oraz powinno być przedstawione jasno i oddzielnie od wszelkich innych informacji.

(71) Osoba, której dane dotyczą, powinna mieć prawo do tego, by nie podlegać decyzji – mogącej obejmować określone środki – która ocenia jej czynniki osobowe, opiera się wyłącznie na przetwarzaniu zautomatyzowanym i wywołuje wobec osoby, której dane dotyczą, skutki prawne lub w podobny sposób znacząco na nią wpływa, jak na przykład automatyczne odrzucenie elektronicznego wniosku kredytowego czy elektroniczne metody rekrutacji bez interwencji ludzkiej. Do takiego przetwarzania zalicza się „profilowanie" – które polega na dowolnym zautomatyzowanym przetwarzaniu danych osobowych pozwalającym ocenić czynniki osobowe osoby fizycznej, a w szczególności analizować lub prognozować aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się osoby, której dane dotyczą – o ile wywołuje skutki prawne względem tej osoby lub w podobny sposób znacząco na nią wpływa. Niemniej

podejmowanie decyzji na podstawie takiego przetwarzania, w tym profilowania, powinno być dozwolone, w przypadku gdy jest to wyraźnie dopuszczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator, w tym do celów monitorowania i zapobiegania – zgodnie z uregulowaniami, standardami i zaleceniami instytucji Unii lub krajowych podmiotów nadzorujących – oszustwom i uchylaniu się od podatków oraz do zapewniania bezpieczeństwa i niezawodności usług świadczonych przez administratora, lub gdy jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem, lub gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę. Przetwarzanie takie powinno zawsze podlegać odpowiednim zabezpieczeniom, obejmującym informowanie osoby, której dane dotyczą, prawo do uzyskania interwencji człowieka, prawo do wyrażenia własnego stanowiska, prawo do uzyskania wyjaśnienia co do decyzji wynikłej z takiej oceny oraz prawo do zakwestionowania takiej decyzji. Takie przetwarzanie nie powinno dotyczyć dzieci.

Aby zapewnić rzetelność i przejrzystość przetwarzania wobec osoby, której dane dotyczą, mając na uwadze konkretne okoliczności i kontekst przetwarzania danych osobowych, administrator powinien stosować odpowiednie matematyczne lub statystyczne procedury profilowania, wdrożyć środki techniczne i organizacyjne zapewniające w szczególności korektę czynników powodujących nieprawidłowości w danych osobowych i maksymalne zmniejszenie ryzyka błędów, zabezpieczyć dane osobowe w sposób uwzględniający potencjalne ryzyko dla interesów i praw osoby, której dane dotyczą, oraz zapobiec m.in. skutkom w postaci dyskryminacji osób fizycznych z uwagi na pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania, przynależność do związków zawodowych, stan genetyczny lub zdrowotny lub orientację seksualną, lub przetwarzaniu skutkującemu środkami mającymi taki efekt.

(72) Profilowanie podlega przepisom niniejszego rozporządzenia dotyczącym przetwarzania danych osobowych, takim jak przepisy określające podstawy prawne przetwarzania lub zasady ochrony danych. Europejska Rada Ochrony Danych ustanowiona niniejszym rozporządzeniem powinna mieć możliwość wydawania wskazówek w tym względzie.

(73) W prawie Unii lub w prawie państwa członkowskiego można przewidzieć ograniczenia dotyczące określonych zasad oraz prawa do informacji, dostępu do danych osobowych i ich sprostowania lub usuwania, prawa do przenoszenia danych, prawa do sprzeciwu, decyzji opartych na profilowaniu, zawiadamiania osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych oraz określonych powiązanych obowiązków administratorów, o ile jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym, by zapewnić bezpieczeństwo publiczne, w tym ochronę życia ludzkiego – w szczególności w ramach reakcji na klęski żywiołowe lub katastrofy spowodowane przez człowieka – zapobieganie przestępczości, prowadzenie postępowań przygotowawczych, ściganie czynów zabronionych, lub wykonywanie kar, w tym ochronę przed

zagrożeniami dla bezpieczeństwa publicznego i zapobieganie takim zagrożeniom lub zapobieganie naruszeniom zasad etyki w zawodach regulowanych, ochronę innych ważnych celów leżących w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnego interesu gospodarczego lub finansowego Unii lub państwa członkowskiego, prowadzenie rejestrów publicznych z uwagi na względy ogólnego interesu publicznego, dalsze przetwarzanie zarchiwizowanych danych osobowych w celu dostarczenia konkretnych informacji o postawie politycznej w ramach dawnych systemów państw totalitarnych lub ochronę osoby, której dane dotyczą, lub praw i wolności innych osób, w tym cele w dziedzinie ochrony socjalnej, zdrowia publicznego i cele humanitarne. Ograniczenia te powinny być zgodne z wymogami Karty praw podstawowych oraz Europejskiej konwencji o ochronie praw człowieka i podstawowych wolności.

(74) Należy nałożyć na administratora obowiązki i ustanowić odpowiedzialność prawną administratora za przetwarzanie danych osobowych przez niego samego lub w jego imieniu. W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych.

(75) Ryzyko naruszenia praw lub wolności osób, o różnym prawdopodobieństwie i wadze, może wynikać z przetwarzania danych osobowych mogącego prowadzić do uszczerbku fizycznego lub szkód majątkowych lub niemajątkowych, w szczególności: jeżeli osoby, których dane dotyczą, mogą zostać pozbawione przysługujących im praw i wolności lub możliwości sprawowania kontroli nad swoimi danymi osobowymi; jeżeli przetwarzane są dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, wyznanie lub przekonania światopoglądowe, lub przynależność do związków zawodowych oraz jeżeli przetwarzane są dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyroków skazujących i czynów zabronionych lub związanych z tym środków bezpieczeństwa; jeżeli oceniane są czynniki osobowe, w szczególności analizowane lub prognozowane aspekty dotyczące efektów pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji lub zainteresowań, wiarygodności lub zachowania, lokalizacji lub przemieszczania się – w celu tworzenia lub wykorzystywania profili osobistych; lub jeżeli przetwarzane są dane osobowe osób wymagających szczególnej opieki, w szczególności dzieci; jeżeli przetwarzanie dotyczy dużej ilości danych osobowych i wpływa na dużą liczbę osób, których dane dotyczą.

(76) Prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, należy określić poprzez odniesienie się do charakteru, zakresu, kontekstu i celów przetwarzania danych. Ryzyko należy oszacować na podstawie obiektywnej oceny, w ramach której stwierdza się, czy z operacjami przetwarzania danych wiąże się ryzyko lub wysokie ryzyko.

(77) Wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności jeżeli chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę pod kątem źródła, charakteru, prawdopodobieństwa i wagi oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko – mogą być przekazane w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub poprzez sugestie inspektora ochrony danych. Europejska Rada Ochrony Danych może wydawać wytyczne także w sprawie operacji przetwarzania, których nie uznaje się za mogące powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, i wskazywać, jakie środki mogą wystarczyć w takich przypadkach dla zaradzenia takiemu ryzyku.

(78) Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. Aby móc wykazać przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych. Takie środki mogą polegać m.in. na minimalizacji przetwarzania danych osobowych, jak najszybszej pseudonimizacji danych osobowych, przejrzystości co do funkcji i przetwarzania danych osobowych, umożliwieniu osobie, której dane dotyczą, monitorowania przetwarzania danych, umożliwieniu administratorowi tworzenia i doskonalenia zabezpieczeń. Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych albo przetwarzają dane osobowe w celu realizacji swojego zadania, należy zachęcać wytwórców tych produktów, usług i aplikacji, by podczas opracowywania i projektowania takich produktów, usług i aplikacji wzięli pod uwagę prawo do ochrony danych osobowych i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych. Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych.

(79) Ochrona praw i wolności osób, których dane dotyczą, oraz obowiązki i odpowiedzialność prawna, administratorów i podmiotów przetwarzających – także w odniesieniu do monitorowania ze strony organów nadzorczych i do środków przez nie stosowanych – wymagają dokonania w ramach niniejszego rozporządzenia jasnego podziału obowiązków, także w sytuacji, gdy administrator określa cele i sposoby przetwarzania wspólnie z innymi administratorami lub gdy operacji przetwarzania dokonuje się w imieniu administratora.

(80) Gdy administrator lub podmiot przetwarzający niemający jednostki organizacyjnej w Unii przetwarza dane osobowe osób, których dane dotyczą, znajdujących się w Unii, a jego czynności przetwarzania wiążą się z oferowaniem towarów lub usług tym osobom w Unii (niezależnie od tego, czy wymaga od tych osób płatności) lub z monitorowaniem ich zachowania (o ile ma ono miejsce w Unii), to taki administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela, chyba że przetwarzanie ma charakter sporadyczny, nie obejmuje – na dużą skalę – przetwarzania szczególnych kategorii danych osobowych, ani przetwarzania danych osobowych dotyczących wyroków skazujących i czynów zabronionych, i jest mało prawdopodobne, by ze względu na swój charakter, kontekst, zakres i cele powodowało ryzyko naruszenia praw lub wolności osób fizycznych, lub jeżeli administrator jest organem lub podmiotem publicznym. Przedstawiciel powinien działać w imieniu administratora lub podmiotu przetwarzającego i może być adresatem ewentualnych działań organu nadzorczego. Administrator lub podmiot przetwarzający powinien wyznaczyć przedstawiciela w wyraźny sposób za pomocą pisemnego upoważnienia do podejmowania działań w jego imieniu w odniesieniu do obowiązków administratora lub podmiotu przetwarzającego wynikających z niniejszego rozporządzenia. Wyznaczenie przedstawiciela nie wpływa na obowiązki lub odpowiedzialność prawną administratora lub podmiotu przetwarzającego wynikającą z niniejszego rozporządzenia. Przedstawiciel powinien wykonywać swoje zadania zgodnie z upoważnieniem otrzymanym od administratora lub podmiotu przetwarzającego, w tym współpracować z właściwymi organami nadzorczymi w odniesieniu do wszelkich działań służących zapewnieniu przestrzegania niniejszego rozporządzenia. W razie jego nieprzestrzegania przez administratora lub podmiot przetwarzający wyznaczony przedstawiciel powinien zostać poddany działaniom egzekucyjnym.

(81) Aby zapewnić przestrzeganie wymogów niniejszego rozporządzenia w przypadku przetwarzania, którego w imieniu administratora ma dokonać podmiot przetwarzający, administrator powinien, powierzając podmiotowi przetwarzającemu czynności przetwarzania, korzystać z usług wyłącznie podmiotów przetwarzających, które zapewniają wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom niniejszego rozporządzenia, w tym wymogom bezpieczeństwa przetwarzania. Stosowanie przez podmiot przetwarzający zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji może posłużyć za element wykazujący wywiązywanie się z obowiązków administratora. Przetwarzanie przez podmiot przetwarzający powinno być regulowane umową lub innym instrumentem prawnym, które podlegają prawu Unii lub prawu państwa członkowskiego, wiążą podmiot przetwarzający z administratorem, określają przedmiot i czas trwania przetwarzania, charakter i cele przetwarzania, rodzaj danych osobowych i kategorie osób, których dane dotyczą, oraz które powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osoby,

której dane dotyczą. Administrator i podmiot przetwarzający mogą postanowić skorzystać z umowy indywidualnej lub ze standardowych klauzul umownych, które zostały przyjęte bezpośrednio przez Komisję albo które zostały przyjęte przez organ nadzorczy zgodnie z mechanizmem spójności, a następnie przyjęte przez Komisję. Po zakończeniu przetwarzania w imieniu administratora podmiot przetwarzający powinien – zgodnie z decyzją administratora – zwrócić lub usunąć dane osobowe, chyba że prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający, nakładają obowiązek przechowywania danych osobowych.

(82) Dla zachowania zgodności z niniejszym rozporządzeniem, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania.

(83) W celu zachowania bezpieczeństwa i zapobiegania przetwarzaniu niezgodnemu z niniejszym rozporządzeniem administrator lub podmiot przetwarzający powinni oszacować ryzyko właściwe dla przetwarzania oraz wdrożyć środki – takie jak szyfrowanie – minimalizujące to ryzyko. Środki takie powinny zapewnić odpowiedni poziom bezpieczeństwa, w tym poufność, oraz uwzględniać stan wiedzy technicznej oraz koszty ich wdrożenia w stosunku do ryzyka i charakteru danych osobowych podlegających ochronie. Oceniając ryzyko w zakresie bezpieczeństwa danych, należy wziąć pod uwagę ryzyko związane z przetwarzaniem danych osobowych – takie jak przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych – i mogące w szczególności prowadzić do uszczerbku fizycznego, szkód majątkowych lub niemajątkowych.

(84) Aby poprawić przestrzeganie niniejszego rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać administratora do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem należy skonsultować się z organem nadzorczym.

(85) Przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych

lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

(86) Administrator powinien bez zbędnej zwłoki poinformować osobę, której dane dotyczą, o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia dla danej osoby fizycznej co do minimalizacji potencjalnych niekorzystnych skutków. Informacje należy przekazywać osobom, których dane dotyczą, tak szybko, jak jest to rozsądnie możliwe, w ścisłej współpracy z organem nadzorczym, z poszanowaniem wskazówek przekazanych przez ten organ lub inne odpowiednie organy, takie jak organy ścigania. Na przykład potrzeba zminimalizowania bezpośredniego ryzyka wystąpienia szkody będzie wymagać niezwłocznego poinformowania osób, których dane dotyczą, natomiast wdrożenie odpowiednich środków przeciwko takim samym lub podobnym naruszeniom ochrony danych może uzasadniać późniejsze poinformowanie.

(87) Należy się upewnić, czy wdrożono wszelkie odpowiednie techniczne środki ochrony i wszelkie odpowiednie środki organizacyjne, by od razu stwierdzić naruszenie ochrony danych osobowych i szybko poinformować organ nadzorczy i osobę, której dane dotyczą. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą. Takie zawiadomienie może skutkować interwencją organu nadzorczego, zgodnie z jego zadaniami i uprawnieniami określonymi w niniejszym rozporządzeniu.

(88) Przy określaniu szczegółowych przepisów o formie i procedurach mających zastosowanie do zawiadamiania o naruszeniu ochrony danych osobowych należy wziąć pod uwagę okoliczności naruszenia, w tym fakt, czy dane osobowe były zabezpieczone odpowiednimi technicznymi środkami ochrony skutecznie ograniczającymi prawdopodobieństwo oszustwa dotyczącego tożsamości lub innych form nadużycia.

W przepisach tych i procedurach należy ponadto uwzględnić prawnie uzasadnione interesy organów ścigania, jeżeli przedwczesne ujawnienie mogłoby niepotrzebnie utrudnić badanie okoliczności naruszenia ochrony danych osobowych.

(89) Dyrektywa 95/46/WE przewidywała ogólny obowiązek zawiadamiania organów nadzorczych o przetwarzaniu danych osobowych. Obowiązek ten powodując jednak obciążenia administracyjne i finansowe i nie zawsze przyczyniał się do poprawy ochrony danych osobowych. Dlatego należy znieść te powszechne, ogólne obowiązki zawiadamiania i zastąpić je skutecznymi procedurami i mechanizmami koncentrującymi się w zamian na tych rodzajach operacji przetwarzania, które ze względu na swój charakter, zakres, kontekst i cele mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych. Takie rodzaje operacji przetwarzania obejmują w szczególności operacje, które wiążą się w szczególności z użyciem nowych technologii lub które są nowe i nie zostały jeszcze poddane przez administratora ocenie skutków dla ochrony danych lub stały się niezbędne z uwagi na upływ czasu od pierwotnego przetwarzania.

(90) W takim przypadku administrator powinien przed przetwarzaniem dokonać oceny skutków dla ochrony danych, aby ocenić konkretne prawdopodobieństwo i powagę tego wysokiego ryzyka, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz źródła ryzyka. Ocena skutków powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające minimalizować to ryzyko, zapewniać ochronę danych osobowych oraz wykazać przestrzeganie niniejszego rozporządzenia.

(91) Powinno to mieć zastosowanie w szczególności do operacji przetwarzania o dużej skali – które służą przetwarzaniu znacznej ilości danych osobowych na szczeblu regionalnym, krajowym lub ponadnarodowym i które mogą wpłynąć na dużą liczbę osób, których dane dotyczą, oraz które mogą powodować wysokie ryzyko, na przykład (ze względu na swój szczególny charakter) gdy zgodnie ze stanem wiedzy technicznej stosowana jest na dużą skalę nowa technologia – oraz do innych operacji przetwarzania powodujących wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności gdy operacje te utrudniają osobom, których dane dotyczą, wykonywanie przysługujących im praw. Oceny skutków dla ochrony danych należy także dokonywać w przypadkach, w których dane osobowe przetwarza się w celu podjęcia decyzji wobec konkretnej osoby fizycznej po dokonaniu systematycznej, kompleksowej oceny czynników osobowych osób fizycznych na podstawie profilowania tych danych lub po przetworzeniu szczególnych kategorii danych osobowych, danych biometrycznych lub danych osobowych dotyczących wyroków skazujących, czynów zabronionych lub odnośnych środków bezpieczeństwa. Ocena skutków dla ochrony danych jest niezbędna również w przypadku monitorowania na dużą skalę miejsc publicznie dostępnych – w szczególności za pomocą urządzeń optyczno-elektronicznych – lub wszelkich innych operacji,

względem których właściwy organ nadzorczy uznaje, że przetwarzanie może powodować wysokie ryzyko naruszenia praw lub wolności osób, których dane dotyczą, w szczególności dlatego, że operacje te uniemożliwiają osobom, których dane dotyczą, wykonywanie prawa lub korzystania z usługi lub umowy lub mają systematyczny charakter i dużą skalę. Przetwarzanie danych osobowych nie powinno być uznawane za przetwarzanie na dużą skalę, jeżeli dotyczy danych osobowych pacjentów lub klientów i jest dokonywane przez pojedynczego lekarza, innego pracownika służby zdrowia lub prawnika. W takich przypadkach ocena skutków dla ochrony danych nie powinna być obowiązkowa.

(92) W niektórych okolicznościach rozsądnie i korzystnie byłoby nie ograniczać oceny skutków dla ochrony danych do pojedynczego projektu, na przykład w przypadkach gdy organy lub podmioty publiczne zamierzają ustanowić wspólną aplikację lub platformę przetwarzania lub gdy kilku administratorów planuje wprowadzić wspólną aplikację lub środowisko przetwarzania obejmujące sektor lub segment gospodarki lub szeroko rozpowszechnioną działalność horyzontalną.

(93) Przyjmując prawo, które ma być dla organu lub podmiotu publicznego podstawą do wykonywania zadań i ma regulować konkretną operację przetwarzania lub konkretny zestaw operacji, państwa członkowskie mogą uznać, że przed takimi czynnościami przetwarzania należy koniecznie przeprowadzić taką ocenę.

(94) Jeżeli ocena skutków dla ochrony danych wykaże, że przy braku zabezpieczeń, środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, a administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia, wtedy przed rozpoczęciem czynności przetwarzania należy skonsultować się z organem nadzorczym. Takie wysokie ryzyko mogą powodować pewne rodzaje przetwarzania oraz zakres i częstotliwość przetwarzania, które mogą skutkować także szkodą lub ingerencją w prawa i wolności osoby fizycznej. Na wniosek o konsultacje organ nadzorczy powinien odpowiedzieć w określonym terminie. Jednak brak reakcji ze strony organu nadzorczego w tym terminie nie powinien wykluczać interwencji tego organu zgodnie z jego zadaniami i uprawnieniami ustanowionymi w niniejszym rozporządzeniu, w tym uprawnieniami do zakazania operacji przetwarzania. W ramach konsultacji można przedłożyć organowi nadzorczemu wyniki oceny skutków dla ochrony danych dokonanej w odniesieniu do danego przetwarzania, a w szczególności środki planowane w celu zminimalizowania ryzyka naruszenia praw lub wolności osób fizycznych.

(95) W razie potrzeby i na żądanie podmiot przetwarzający powinien pomagać administratorowi w zapewnieniu przestrzegania obowiązków wynikających z dokonania oceny skutków dla ochrony danych oraz z uprzednich konsultacji z organem nadzorczym.

(96) Konsultacji z organem nadzorczym należy dokonać również w trakcie przygotowywania aktu ustawodawczego lub wykonawczego przewidującego przetwarzanie danych osobowych, aby zapewnić zgodność zamierzonego przetwarzania z niniejszym rozporządzeniem, a w szczególności zminimalizować ewentualne ryzyko dla osoby, której dane dotyczą.

(97) Jeżeli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości lub jeżeli w sektorze prywatnym przetwarzania dokonuje administrator, którego główna działalność polega na operacjach przetwarzania wymagających regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę lub jeżeli główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych oraz danych osobowych dotyczących wyroków skazujących i czynów zabronionych, to w monitorowaniu wewnętrznego przestrzegania niniejszego rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. W sektorze prywatnym przetwarzanie danych osobowych jest główną działalnością administratora, jeżeli oznacza jego zasadnicze, a nie poboczne czynności. Niezbędny poziom wiedzy fachowej należy ustalić w szczególności w świetle prowadzonych operacji przetwarzania danych oraz ochrony, której wymagają dane osobowe przetwarzane przez administratora lub podmiot przetwarzający. Tacy inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

(98) Należy zachęcać zrzeszenia lub inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających do sporządzania kodeksów postępowania, w granicach niniejszego rozporządzenia, by ułatwiać skuteczne stosowanie niniejszego rozporządzenia, z uwzględnieniem szczególnych cech przetwarzania prowadzonego w niektórych sektorach i szczególnych potrzeb mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw. W takich kodeksach można w szczególności dopasować obowiązki administratorów i podmiotów przetwarzających do ryzyka naruszenia praw lub wolności osób fizycznych, jakie może powodować przetwarzanie.

(99) Sporządzając kodeks postępowania bądź zmieniając go lub rozszerzając jego zakres, zrzeszenia i inne organy reprezentujące kategorie administratorów lub podmiotów przetwarzających powinny konsultować się z odpowiednimi stronami, których sprawa dotyczy, w tym jeżeli jest to wykonalne, z osobami, których dane dotyczą, oraz mieć na względzie uwagi i opinie otrzymane w ramach takich konsultacji.

(100) Aby zwiększyć przejrzystość i poprawić przestrzeganie niniejszego rozporządzenia, należy zachęcać do ustanowienia mechanizmów certyfikacji oraz do

wprowadzenia znaków jakości i oznaczeń w dziedzinie ochrony danych, pozwalając w ten sposób osobom, których dane dotyczą, szybko ocenić stopień ochrony danych, której podlegają stosowne produkty i usługi.

(101) Przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest niezbędnym warunkiem rozwoju handlu międzynarodowego i współpracy międzynarodowej. Wzrost takiego przepływu spowodował nowe wyzwania i problemy w dziedzinie ochrony danych osobowych. Przekazując dane osobowe z Unii administratorom, podmiotom przetwarzającym lub innym odbiorcom w państwach trzecich lub organizacjom międzynarodowym, nie należy jednak obniżać stopnia ochrony osób fizycznych zapewnianego w Unii niniejszym rozporządzeniem, także w przypadkach dalszego przekazywania danych osobowych: z państwa trzeciego lub organizacji międzynarodowej administratorom lub pomiotom przetwarzającym w tym samym lub w innym państwie trzecim lub tej samej lub innej organizacji międzynarodowej. W każdym przypadku przekazywanie danych do państw trzecich i organizacji międzynarodowych może się odbywać wyłącznie w pełnej zgodzie z niniejszym rozporządzeniem. Przekazywanie może mieć miejsce wyłącznie w przypadkach, gdy administrator lub podmiot przetwarzający przestrzegają warunków określonych w przepisach niniejszego rozporządzenia dotyczących przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym – z zastrzeżeniem pozostałych przepisów niniejszego rozporządzenia.

(102) Niniejsze rozporządzenie pozostaje bez uszczerbku dla umów międzynarodowych między Unią a państwami trzecimi regulujących przekazywanie danych osobowych, w tym zawierających odpowiednie zabezpieczania dla osób, których dane dotyczą. Państwa członkowskie mogą zawierać umowy międzynarodowe przewidujące m.in. przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych, o ile umowy takie nie wpływają na niniejsze rozporządzenie ani na inne przepisy prawa Unii i o ile przewidują odpowiedni stopień ochrony podstawowych praw osób, których dane dotyczą.

(103) Komisja może stwierdzić ze skutkiem dla całej Unii, że państwo trzecie – lub terytorium lub określony sektor w państwie trzecim – lub organizacja międzynarodowa zapewniają odpowiedni stopień ochrony danych, gwarantując tym samym pewność i jednolitość prawną w całej Unii w odniesieniu do państw trzecich lub organizacji międzynarodowych, które zostały uznane za zapewniające taki stopień ochrony. W takich przypadkach przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej może się odbywać bez potrzeby uzyskania dodatkowego zezwolenia. Komisja może także zdecydować, wcześniej informując o tym państwo trzecie lub organizację międzynarodową i przedstawiając im uzasadnienie, o cofnięciu takiej decyzji.

(104) Zgodnie z podstawowymi wartościami, na których opiera się Unia, w szczególności z ochroną praw człowieka, Komisja powinna w swojej ocenie państwa trzeciego lub terytorium lub określonego sektora w państwie trzecim wziąć pod uwagę sposób, w jaki dane państwo trzecie przestrzega praworządności, dostępu do wymiaru sprawiedliwości oraz międzynarodowych norm i standardów ochrony praw człowieka, jego prawo ogólne i sektorowe, w tym ustawodawstwo dotyczące bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i porządku publicznego, a także prawo karne. Przy przyjmowaniu decyzji stwierdzających odpowiedni stopień ochrony w odniesieniu do terytorium lub w określonego sektora w państwie trzecim, należy wziąć pod uwagę jasne i obiektywne kryteria, takie jak konkretne czynności przetwarzania, zakres mających zastosowanie standardów prawnych i ustawodawstwo obowiązujące w danym państwie trzecim. Państwo trzecie powinno dawać gwarancje zapewniające odpowiedni stopień ochrony, zasadniczo odpowiadający stopniowi ochrony zapewnianemu w Unii, w szczególności w przypadkach, gdy dane osobowe są przetwarzane w jednym szczególnym sektorze lub większej ich liczbie. Państwo trzecie powinno w szczególności zapewnić skuteczny niezależny nadzór nad ochroną danych oraz powinno przewidzieć mechanizmy współpracy z organami ochrony danych państw członkowskich, a osoby, których dane dotyczą, powinny uzyskać skuteczne i egzekwowalne prawa oraz skuteczne administracyjne i sądowe środki zaskarżenia.

(105) Pozazobowiązaniami międzynarodowymipaństwa trzeciego lub organizacji międzynarodowej, Komisja powinna brać pod uwagę obowiązki wynikające z udziału państwa trzeciego lub organizacji międzynarodowej w systemach wielostronnych lub regionalnych, w szczególności w odniesieniu do ochrony danych osobowych, a także realizację takich obowiązków. W szczególności powinna wziąć pod uwagę przystąpienie państwa trzeciego do konwencji Rady Europy z dnia 28 stycznia 1981 r. o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych. Oceniając stopień ochrony w państwach trzecich lub organizacjach międzynarodowych, Komisja powinna konsultować się z Europejską Radą Ochrony Danych.

(106) Komisja powinna monitorować obowiązywanie decyzji o stopniu ochrony w państwie trzecim, na terytorium lub w określonym sektorze w państwie trzecim lub w organizacji międzynarodowej, oraz monitorować funkcjonowanie decyzji przyjętych na podstawie art. 25 ust. 6 lub art. 26 ust. 4 dyrektywy 95/46/WE. W swoich decyzjach stwierdzających odpowiedni stopień ochrony Komisja powinna przewidzieć mechanizm okresowego przeglądu ich funkcjonowania. Taki okresowy przegląd powinna ona przeprowadzać w konsultacji z danym państwem trzecim lub daną organizacją międzynarodową i powinna w nim uwzględniać wszelkie mające znaczenie zmiany w tym państwie trzecim lub tej organizacji międzynarodowej. Prowadząc monitorowanie i dokonując okresowych przeglądów, Komisja powinna uwzględnić stanowisko i wnioski Parlamentu Europejskiego i Rady, a także innych odpowiednich organów i źródeł. Komisja powinna w rozsądnym

terminie ocenić funkcjonowanie decyzji wspomnianego drugiego typu i przekazać wszelkie odpowiednie wnioski komitetowi w rozumieniu rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 182/2011[12] ustanowionemu na mocy niniejszego rozporządzenia, Parlamentowi Europejskiemu i Radzie.

(107) Komisja może uznać, że państwo trzecie, terytorium lub określony sektor w państwie trzecim, lub organizacja międzynarodowa przestały zapewniać odpowiedni stopień ochrony danych. W związku z tym przekazywanie danych osobowych do tego państwa trzeciego lub tej organizacji międzynarodowej powinno zostać zakazane, chyba że spełnione są wymogi niniejszego rozporządzenia dotyczące przekazywania z zastrzeżeniem odpowiednich zabezpieczeń, w tym wiążących reguł korporacyjnych oraz wyjątków w odniesieniu do szczególnych sytuacji. W takim przypadku należy przewidzieć konsultacje między Komisją a takimi państwami trzecimi lub organizacjami międzynarodowymi. Komisja powinna niezwłocznie poinformować to państwo trzecie lub tę organizację międzynarodową o powodach oraz podjąć z nimi konsultacje w celu rozwiązania sytuacji.

(108) W razie braku stwierdzenia odpowiedniego stopnia ochrony danych administrator lub podmiot przetwarzający powinni zastosować środki rekompensujące brak ochrony danych w państwie trzecim, zapewniając osobie, której dane dotyczą, odpowiednie zabezpieczenia. Takie odpowiednie zabezpieczenia mogą polegać na skorzystaniu z wiążących reguł korporacyjnych, standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy lub klauzul umownych dopuszczonych przez organ nadzorczy. Zabezpieczenia te powinny zapewniać, by przestrzegane były wymogi ochrony danych oraz prawa osób, których dane dotyczą, takie same jak w przypadku przetwarzania wewnątrzunijnego, w tym zapewniać dostępność egzekwowalnych praw osoby, której dane dotyczą, i skutecznych środków ochrony prawnej – w tym prawa do skutecznych administracyjnych lub sądowych środków zaskarżenia i do żądania odszkodowania – w Unii lub w państwie trzecim. Powinny one dotyczyć w szczególności przestrzegania ogólnych zasad związanych z przetwarzaniem danych osobowych oraz zasad uwzględniania ochrony danych w fazie projektowania i domyślnej ochrony danych. Również organy lub podmioty publiczne mogą przekazywać dane organom lub podmiotom publicznym w państwach trzecich lub organizacjom międzynarodowym o analogicznych obowiązkach lub funkcjach, w tym na podstawie przepisów, które powinny znaleźć się w uzgodnieniach administracyjnych, takich jak protokoły ustaleń, i które powinny przewidywać egzekwowalne i skuteczne prawa osób, których dane dotyczą. Jeżeli zabezpieczenia zawarte są w niewiążących prawnie uzgodnieniach administracyjnych, należy uzyskać zezwolenie właściwego organu nadzorczego.

[12] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z dnia 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję (Dz.U. L 55 z 28.2.2011, s. 13).

(109) Możliwość korzystania przez administratora lub podmiot przetwarzający ze standardowych klauzul ochrony danych przyjętych przez Komisję lub organ nadzorczy nie powinna stanowić dla administratora lub podmiotu przetwarzającego przeszkody, by standardowe klauzule ochrony danych włączyć do szerszej umowy, takiej jak umowa między wspomnianym podmiotem przetwarzającym a innym podmiotem przetwarzającym, ani by dodać inne klauzule lub dodatkowe zabezpieczenia, pod warunkiem że nie są one bezpośrednio lub pośrednio sprzeczne ze standardowymi klauzulami umownymi przyjętymi przez Komisję lub organ nadzorczy ani nie naruszają podstawowych praw lub wolności osób, których dane dotyczą. Należy zachęcać administratorów i podmioty przetwarzające, by w drodze zobowiązań umownych przewidywały dodatkowe zabezpieczenia, stanowiące uzupełnienie dla standardowych klauzul ochrony.

(110) Grupa przedsiębiorstw lub grupa przedsiębiorców prowadzących wspólną działalność gospodarczą powinna móc korzystać z zatwierdzonych wiążących reguł korporacyjnych przy międzynarodowym przekazywaniu danych z Unii do organizacji w tej samej grupie przedsiębiorstw lub w grupie przedsiębiorców prowadzących wspólną działalność gospodarczą, pod warunkiem, że w takich regułach korporacyjnych są ujęte wszystkie podstawowe zasady i egzekwowalne prawa zapewniające odpowiednie zabezpieczenia na potrzeby przekazywania danych osobowych lub na potrzeby określonych kategorii przekazań danych osobowych.

(111) Należy wprowadzić możliwość przekazywania danych w niektórych okolicznościach, jeżeli osoba, której dane dotyczą, wyraziła na to wyraźną zgodę, jeżeli przekazywanie jest sporadyczne i niezbędne w związku z umową lub roszczeniem – niezależnie od rodzaju postępowania: sądowego lub administracyjnego lub jakiegokolwiek innego postępowania pozasądowego, w tym postępowania przed organami regulacyjnymi. Należy także przewidzieć możliwość przekazywania danych, jeżeli wymaga tego ważny interes publiczny określony w prawie Unii lub prawie państwa członkowskiego lub jeżeli przekazanie następuje z rejestru utworzonego na mocy prawa i przeznaczonego do wglądu dla ogółu obywateli lub osób mających prawnie uzasadniony interes. W drugim z tych przypadków przekazanie nie powinno obejmować całości danych osobowych lub całych kategorii danych z rejestru, a jeżeli rejestr jest przeznaczony do wglądu dla osób mających prawnie uzasadniony interes, przekazanie danych powinno nastąpić wyłącznie na żądanie tych osób lub osoby te mają być odbiorcami, przy pełnym uwzględnieniu interesów i praw podstawowych osoby, której dane dotyczą.

(112) Wyjątki te powinny mieć w szczególności zastosowanie do przekazywania danych wymaganego i niezbędnego z uwagi na ważne względy interesu publicznego, na przykład do międzynarodowej wymiany danych między organami ds. konkurencji, organami podatkowymi lub celnymi, organami nadzoru finansowego, służbami odpowiedzialnymi za sprawy zabezpieczenia społecznego lub za zdrowie

publiczne, na przykład w przypadku ustalania kontaktów zakaźnych w razie chorób zakaźnych lub w celu zmniejszenia lub wyeliminowania dopingu w sporcie. Przekazywanie danych osobowych należy uznać za zgodne z prawem również w przypadkach, gdy jest niezbędne w celu ochrony interesu, który ma istotne znaczenie dla żywotnych interesów osoby, której dane dotyczą, lub innej osoby, w tym integralności fizycznej lub życia, a osoba, której dane dotyczą, nie jest w stanie wyrazić zgody. W razie braku stwierdzenia odpowiedniego stopnia ochrony prawo Unii lub prawo państwa członkowskiego może z uwagi na ważne względy interesu publicznego wyraźnie nakładać ograniczenia na przekazywanie konkretnych kategorii danych do państwa trzeciego lub organizacji międzynarodowej. O takich przepisach państwa członkowskie powinny powiadomić Komisję. Każde przekazanie danych osobowych osoby, której dane dotyczą, będącej fizycznie lub prawnie niezdolną do wyrażenia zgody, do międzynarodowej organizacji humanitarnej, aby mogła wykonać zadanie nałożone na nią konwencjami genewskimi lub by mogła spełnić wymogi międzynarodowego prawa humanitarnego mającego zastosowanie w konfliktach zbrojnych, można uznać za niezbędne z uwagi na ważny wzgląd interesu publicznego lub za leżące w żywotnym interesie osoby, której dane dotyczą.

(113) Przekazanie, które można uznać za niepowtarzające się i dotyczące tylko ograniczonej liczby osób, których dane dotyczą, może być także dopuszczalne ze względu na ważne prawnie uzasadnione interesy realizowane przez administratora, o ile charakteru nadrzędnego nie mają interesy lub prawa i wolności osoby, której dane dotyczą, i administrator ocenił wszelkie okoliczności związane z przekazaniem danych. Administrator powinien zwrócić szczególną uwagę na charakter danych osobowych, cel i czas trwania proponowanej operacji przetwarzania lub proponowanych operacji przetwarzania oraz na sytuację w państwie pochodzenia, państwie trzecim i państwie ostatecznego przeznaczenia, a także powinien zapewnić odpowiednie zabezpieczenia poszanowania podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych. Takie przekazanie powinno być dopuszczalne w nielicznych przypadkach – gdy nie ma zastosowania żadna z pozostałych podstaw umożliwiających przekazanie. Gdy chodzi o cele badań naukowych lub historycznych lub cele statystyczne, należy wziąć pod uwagę uzasadnione oczekiwania społeczne co do rozwoju wiedzy. Administrator powinien informować o przekazaniu organ nadzorczy oraz osobę, której dane dotyczą.

(114) W każdym przypadku, jeżeli Komisja nie podjęła decyzji stwierdzającej odpowiedni stopień ochrony danych w państwie trzecim, administrator lub podmiot przetwarzający powinni zastosować rozwiązania, które pozwolą osobom, których dane dotyczą, dysponować – gdy przekazanie już dojdzie do skutku – egzekwowalnymi i skutecznymi prawami względem przetwarzania ich danych w Unii, tak że osoby te nadal będą mogły korzystać z podstawowych praw i zabezpieczeń.

(115) Niektóre państwa trzecie przyjmują ustawy, rozporządzenia i inne akty prawne mające bezpośrednio regulować czynności przetwarzania podejmowane przez osoby fizyczne i prawne podlegające jurysdykcji państw członkowskich. Może to obejmować wyroki sądów lub trybunałów czy decyzje organów administracyjnych państwa trzeciego nakazujące administratorowi lub podmiotowi przetwarzającemu przekazać lub ujawnić dane osobowe, które niemają za podstawę umowy międzynarodowej – na przykład umowy o wzajemnej pomocy prawnej – obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim. Transgraniczne stosowanie tych ustaw, rozporządzeń i innych aktów prawnych może naruszać prawo międzynarodowe i uniemożliwiać zapewnienie osobom fizycznym ochrony zapewnianej niniejszym rozporządzeniem przez Unię. Przekazywanie danych powinno być dopuszczalne wyłącznie w przypadkach, gdy spełnione są warunki przekazywania do państw trzecich ustanowione w niniejszym rozporządzeniu. Tak może być m.in. w przypadkach, gdy ujawnienie jest niezbędne ze względu na ważny interes publiczny uznany w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator.

(116) Transgraniczne przekazywanie danych osobowych poza Unią może spowodować wzrost ryzyka, że osoby fizyczne nie będą mogły wykonywać prawa do ochrony danych osobowych, w szczególności w celu ochrony przed niezgodnym z prawem wykorzystaniem lub ujawnieniem tych informacji. Jednocześnie organy nadzorcze mogą uznać, że nie są w stanie rozpatrzyć skargi lub przeprowadzić postępowania w sprawie działalności, która ma miejsce poza granicami ich państwa. Ich starania na rzecz współpracy w kontekście transgranicznym mogą także zostać zakłócone przez niewystarczające uprawnienia prewencyjne lub zaradcze, niespójne systemy prawne oraz przeszkody praktyczne, takie jak ograniczone środki. Należy więc upowszechniać ściślejszą współpracę między organami nadzorującymi ochronę danych, by pomóc im wymieniać informacje i prowadzić postępowania z ich międzynarodowymi odpowiednikami. Aby stworzyć mechanizmy współpracy międzynarodowej, ułatwiające i przewidujące wzajemną międzynarodową pomoc w egzekwowaniu ustawodawstwa z zakresu ochrony danych osobowych, Komisja i organy nadzorcze powinny w ramach działań związanych z wykonywaniem swoich uprawnień wymieniać się informacjami i współpracować z właściwymi organami państw trzecich na zasadzie wzajemności i zgodnie z niniejszym rozporządzeniem.

(117) Zasadniczym elementem ochrony osób fizycznych w związku z przetwarzaniem danych osobowych jest utworzenie w państwach członkowskich organów nadzorczych, uprawnionych do wypełniania zadań i wykonywania uprawnień w sposób całkowicie niezależny. Aby uwzględnić swoją strukturę konstytucyjną, organizacyjną i administracyjną, państwa członkowskie powinny mieć możliwość utworzenia więcej niż jednego organu nadzorczego.

(118) Niezależność organów nadzorczych nie powinna oznaczać, że organy te nie mogą podlegać mechanizmom kontroli lub monitorowania pod kątem wydatków ani kontroli sądowej.

(119) Jeżeli państwo członkowskie utworzy kilka organów nadzorczych, powinno przewidzieć przepisy określające mechanizmy zapewniające skuteczny udział tych organów w stosowaniu mechanizmu spójności. Takie państwo członkowskie powinno w szczególności wyznaczyć organ nadzorczy, który pełnił będzie funkcję pojedynczego punktu kontaktowego do celów skutecznego udziału tych organów w stosowaniu mechanizmu, aby zapewnić sprawną i płynną współpracę z innymi organami nadzorczymi, Europejską Radą Ochrony Danych oraz Komisją.

(120) Każdy organ nadzorczy powinien zostać wyposażony w zasoby finansowe i kadrowe, pomieszczenia i infrastrukturę niezbędne do skutecznego wykonywania zadań, w tym zadań związanych z wzajemną pomocą i współpracą z innymi organami nadzorczymi z całej Unii. Każdy organ nadzorczy powinien dysponować odrębnym, publicznym budżetem rocznym, który może być częścią ogólnego budżetu krajowego lub państwowego.

(121) Ogólne warunki pełnienia funkcji członka organu nadzorczego powinny zostać określone w prawie każdego państwa członkowskiego i powinny w szczególności zapewniać, by członków tego organu powoływał przy zastosowaniu procedury zapewniającej przejrzystość parlament, rząd lub głowa danego państwa członkowskiego – na wniosek rządu, członka rządu, parlamentu lub izby parlamentu – lub niezależny organ, któremu zadanie to powierzono w prawie państwa członkowskiego. Aby zapewnić niezależność organu nadzorczego, jego członek lub członkowie powinni działać uczciwie, powstrzymać się od wszelkich czynności niezgodnych ze swoimi obowiązkami i nie powinni podczas swojej kadencji podejmować żadnego zajęcia zarobkowego ani niezarobkowego niezgodnego z tymi obowiązkami. Organ nadzorczy powinien dysponować własnym personelem, który jest dobierany przez ten organ nadzorczy lub niezależny organ utworzony na mocy prawa państwa członkowskiego i powinien działać pod wyłącznym kierownictwem członka lub członków tego organu nadzorczego.

(122) Każdy organ nadzorczy powinien być właściwy na terytorium swojego państwa członkowskiego do wykonywania uprawnień i wypełniania zadań powierzonych mu w myśl niniejszego rozporządzenia. Powinno to dotyczyć w szczególności przetwarzania w ramach działalności jednostki organizacyjnej administratora lub podmiotu przetwarzającego na terytorium tego państwa członkowskiego, przetwarzania danych osobowych przez organy publiczne lub podmioty prywatne działające w interesie publicznym, przetwarzania mającego wpływ na osoby, których dane dotyczą, na tym terytorium lub przetwarzania dokonywanego przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli

zwracają się oni do osób, których dane dotyczą, mających miejsce zamieszkania na tym terytorium. Powinno to dotyczyć rozpatrywania skarg wnoszonych przez osoby, których dane dotyczą, prowadzenia postępowań w sprawie stosowania niniejszego rozporządzenia oraz uświadamiania ryzyka, zasad, zabezpieczeń i praw związanych z przetwarzaniem danych osobowych.

(123) Organy nadzorcze powinny monitorować stosowanie przepisów niniejszego rozporządzenia oraz przyczyniać się do jego spójnego stosowania w całej Unii, aby chronić osoby fizyczne w związku z przetwarzaniem ich danych osobowych oraz ułatwiać swobodny przepływ danych osobowych na rynku wewnętrznym. W tym celu organy nadzorcze powinny współpracować ze sobą oraz z Komisją bez konieczności zawierania przez państwa członkowskie umów o wzajemnej pomocy lub współpracy.

(124) Jeżeli przetwarzanie danych osobowych odbywa się w ramach działalności jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, a administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim lub jeżeli przetwarzanie, które odbywa się w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, organem wiodącym powinien być organ nadzorczy głównej jednostki organizacyjnej administratora lub podmiotu przetwarzającego lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego. Powinien on współpracować z innymi organami, których sprawa dotyczy, z uwagi na to, że administrator lub podmiot przetwarzający mają jednostkę organizacyjną na terytorium ich państwa członkowskiego, że odnotowuje się znaczny wpływ na osoby, których dane dotyczą, mające miejsce zamieszkania na tym terytorium lub że wniesiono do tych organów skargę. Także w przypadkach, gdy skargę wniosła osoba, której dane dotyczą, niemająca miejsca zamieszkania w tym państwie członkowskim, organ nadzorczy, do którego wniesiono skargę, powinien być uznawany za organ nadzorczy, którego sprawa dotyczy. W ramach zadania, którym jest wydawanie wytycznych co do stosowania niniejszego rozporządzenia, Europejska Rada Ochrony Danych powinna mieć możliwość wydawania wytycznych w szczególności w sprawie kryteriów, które należy uwzględnić, by stwierdzić, czy dane przetwarzanie znacznie wpływa na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim, oraz w sprawie tego, czym jest mający znaczenie dla sprawy i uzasadniony sprzeciw.

(125) Wiodący organ nadzorczy powinien być właściwy do przyjmowania wiążących decyzji co do środków wdrażających uprawnienia powierzone mu zgodnie z niniejszym rozporządzeniem. Organ nadzorczy sprawujący funkcję organu wiodącego powinien ściśle angażować w proces decyzyjny organy nadzorcze, których sprawa dotyczy, i powinien go z nimi koordynować. Jeżeli na mocy decyzji skarga

osoby, której dane dotyczą, ma zostać w całości lub w części odrzucona, decyzję tę powinien przyjmować organ nadzorczy, do którego wniesiono skargę.

(126) Decyzja powinna być uzgadniana wspólnie przez wiodący organ nadzorczy i organy nadzorcze, których sprawa dotyczy, powinna być skierowana do głównej lub pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego i powinna być wiążąca dla administratora i podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinien zastosować wszelkie niezbędne środki, by zapewnić zgodność z niniejszym rozporządzeniem i zastosować się do decyzji doręczonej przez wiodący organ nadzorczy głównej jednstce organizacyjnej administratora lub podmiotu przetwarzającego w odniesieniu do czynności przetwarzania w Unii.

(127) Każdy organ nadzorczy niepełniący funkcji wiodącego organu nadzorczego powinien być właściwy w sprawach lokalnych, gdy administrator lub podmiot przetwarzający posiadają jednostki organizacyjne w więcej niż jednym państwie członkowskim, ale przedmiot danego przetwarzania dotyczy wyłącznie przetwarzania prowadzonego w pojedynczym państwie członkowskim i wyłącznie osób, których dane dotyczą, w tym pojedynczym państwie członkowskim, na przykład gdy chodzi o przetwarzanie danych osobowych pracowników w szczególowym kontekście zatrudnienia w państwie członkowskim. W takim przypadku organ nadzorczy powinien niezwłocznie poinformować o sprawie wiodący organ nadzorczy. Po otrzymaniu informacji wiodący organ nadzorczy powinien postanowić, czy zajmie się daną sprawą zgodnie z przepisami niniejszego rozporządzenia dotyczącymi współpracy między wiodącym organem nadzorczym a innymi organami nadzorczymi, których sprawa dotyczy („mechanizm kompleksowej współpracy"), czy też powinien się nią zająć na szczeblu lokalnym organ nadzorczy, który o niej poinformował. Podejmując decyzję, czy zająć się sprawą, wiodący organ nadzorczy powinien uwzględnić, czy w państwie członkowskim, którego organ nadzorczy przekazał mu informacje, znajduje się jednostka organizacyjna administratora lub podmiotu przetwarzającego – aby zapewnić skuteczne wykonanie decyzji względem administratora lub podmiotu przetwarzającego. Jeżeli wiodący organ nadzorczy postanowi zająć się daną sprawą, organ nadzorczy, który przekazał mu informacje, powinien mieć możliwość przedłożenia projektu decyzji, którą wiodący organ nadzorczy powinien w jak największym stopniu uwzględnić, przygotowując projekt swojej decyzji w ramach mechanizmu kompleksowej współpracy.

(128) Przepisy dotyczące wiodącego organu nadzorczego i mechanizmu kompleksowej współpracy nie powinny mieć zastosowania, gdy organy publiczne lub podmioty prywatne dokonują przetwarzania w interesie publicznym. W takich przypadkach jedynym organem nadzorczym właściwym do wykonywania uprawnień przyznanych zgodnie z niniejszym rozporządzeniem powinien być organ nadzorczy państwa członkowskiego, w którym organ publiczny lub podmiot prywatny posiadają jednostkę organizacyjną.

(129) Aby zapewnić spójne monitorowanie i egzekwowanie niniejszego rozporządzenia w całej Unii, organy nadzorcze powinny mieć w każdym państwie członkowskim te same zadania i faktyczne uprawnienia, w tym uprawnienia do prowadzenia postępowań wyjaśniających, naprawcze, uprawnienia do nakładania kar oraz do udzielania zezwoleń i doradcze, w szczególności w przypadku skarg osób fizycznych, i – bez uszczerbku dla uprawnień organów prokuratorskich na mocy prawa państwa członkowskiego – uprawnienia do zgłaszania naruszeń niniejszego rozporządzenia organom wymiaru sprawiedliwości oraz do udziału w postępowaniu sądowym. Wśród tych uprawnień powinno być także uprawnienie do wprowadzania czasowego lub definitywnego ograniczenia przetwarzania, w tym zakazania przetwarzania. Państwa członkowskie mogą określić także inne zadania związane z ochroną danych osobowych na mocy niniejszego rozporządzenia. Swoje uprawnienia organy nadzorcze powinny wykonywać zgodnie z odpowiednimi zabezpieczeniami proceduralnymi przewidzianymi w prawie Unii i prawie państwa członkowskiego, bezstronnie, sprawiedliwie i w rozsądnym terminie. W szczególności każdy środek powinien być odpowiedni, niezbędny i proporcjonalny, aby zapewnić przestrzeganie niniejszego rozporządzenia – z uwzględnieniem okoliczności danej sprawy, z poszanowaniem prawa do wysłuchania danej osoby przed zastosowaniem indywidualnego środka, który miałby niekorzystnie na nią wpłynąć, i bez nadmiernych kosztów i niedogodności dla danej osoby. Uprawnienia do prowadzenia postępowań wyjaśniających, jeżeli chodzi o dostęp do pomieszczeń, należy wykonywać zgodnie ze szczegółowymi wymogami przepisów państwa członkowskiego dotyczących postępowania, takimi jak wymóg uzyskania uprzedniego zezwolenia sądu. Każdy prawnie wiążący środek organu nadzorczego powinien być sporządzony na piśmie, mieć jasny i jednoznaczny charakter, wskazywać organ nadzorczy, który wydał środek, i datę wydania środka, nosić podpis szefa lub członka organu nadzorczego przez niego upoważnionego, podawać powody zastosowania środka oraz informować o prawie do skutecznego środka ochrony prawnej. Nie powinno to wykluczać dodatkowych wymogów na mocy przepisów państwa członkowskiego dotyczących postępowania. Wydanie prawnie wiążącej decyzji oznacza, że może ona być przedmiotem kontroli sądowej w państwie członkowskim organu nadzorczego, który ją wydał.

(130) Jeżeli organ nadzorczy, do którego wniesiono skargę, nie jest wiodącym organem nadzorczym, wiodący organ nadzorczy powinien ściśle współpracować z organem nadzorczym, do którego wniesiono skargę, zgodnie z przepisami o współpracy i spójności ustanowionymi w niniejszym rozporządzeniu. W takim przypadku wiodący organ nadzorczy powinien, w przypadkach gdy stosuje środki mające wywołać skutki prawne, w tym nakłada administracyjne kary pieniężne, w jak największym stopniu brać pod uwagę opinię organu nadzorczego, do którego wniesiono skargę, ten zaś powinien pozostać właściwy do przeprowadzenia postępowania wyjaśniającego na terytorium własnego państwa członkowskiego będąc w kontakcie z wiodącym organem nadzorczym.

(131) Jeżeli funkcję wiodącego organu nadzorczego wobec czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający powinien pełnić inny organ nadzorczy, ale konkretny przedmiot skargi lub ewentualnego naruszenia dotyczy wyłącznie czynności przetwarzania prowadzonych przez administratora lub podmiot przetwarzający w państwie członkowskim, w którym wniesiono skargę lub wykryto ewentualne naruszenie, a sprawa nie wpływa znacznie lub najprawdopodobniej nie wpłynie znacznie na osoby, których dane dotyczą, w innych państwach członkowskich, wtedy organ nadzorczy, do którego wniesiono skargę lub który wykrył lub w inny sposób dowiedział się o sytuacjach mogących skutkować ewentualnymi naruszeniami niniejszego rozporządzenia, powinien dążyć do polubownego rozwiązania z administratorem, a jeżeli okaże się ono niemożliwe, skorzystać z pełni przysługujących mu uprawnień. Powinno to dotyczyć także: konkretnego przetwarzania, które odbywa się na terytorium państwa członkowskiego organu nadzorczego lub odnosi się do osób, których dane dotyczą, na terytorium tego państwa członkowskiego; przetwarzania, które odbywa się w ramach oferowania towarów lub usług konkretnie osobom, których dane dotyczą, na terytorium państwa członkowskiego organu nadzorczego; lub przetwarzania wymagającego oceny z uwagi na stosowne obowiązki prawne wynikające z prawa państwa członkowskiego.

(132) Na uświadamiające działania organów nadzorczych skierowane do opinii publicznej powinny się składać m.in. konkretne środki adresowane do administratorów i podmiotów przetwarzających, w tym do mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw, a także do osób fizycznych, w szczególności w ramach edukacji.

(133) Organy nadzorcze powinny się wzajemnie wspierać w wykonywaniu swoich zadań oraz świadczyć sobie wzajemną pomoc, by zapewnić spójne stosowanie i egzekwowanie niniejszego rozporządzenia na rynku wewnętrznym. Organ nadzorczy, który występuje z wnioskiem o wzajemną pomoc, może przyjąć środek tymczasowy, jeżeli nie uzyska odpowiedzi w terminie miesiąca od otrzymania wniosku o udzielenie wzajemnej pomocy przez wezwany organ nadzorczy.

(134) Każdy organ nadzorczy powinien w stosownych przypadkach uczestniczyć we wspólnych operacjach organów nadzorczych. Wezwany organ nadzorczy powinien mieć obowiązek udzielenia odpowiedzi w określonym terminie.

(135) Aby zapewnić spójne stosowanie niniejszego rozporządzenia w całej Unii, należy ustanowić mechanizm spójności na potrzeby współpracy między organami nadzorczymi. Mechanizm ten powinien mieć zastosowanie w szczególności w przypadkach, gdy organ nadzorczy zamierza przyjąć środek mający wywoływać skutki prawne w odniesieniu do operacji przetwarzania, które znacznie wpływają na istotną liczbę osób, których dane dotyczą, w kilku państwach członkowskich. Powinien mieć zastosowanie także w przypadkach, gdy organ nadzorczy, którego sprawa dotyczy, lub Komisja zwracają się z wnioskiem o rozwiązanie danej kwe-

stii w ramach mechanizmu spójności. Mechanizm ten powinien pozostawać bez uszczerbku dla środków, które Komisja może zastosować w ramach wykonywania uprawnień przysługujących jej na mocy traktatów.

(136) W ramach stosowania mechanizmu spójności Europejska Rada Ochrony Danych powinna w określonym terminie wydawać opinie, jeżeli tak postanowią większością głosów jej członkowie lub jeżeli zwróci się do niej z takim wnioskiem organ nadzorczy, którego sprawa dotyczy, lub Komisja. Europejska Rada Ochrony Danych powinna być także umocowana do przyjmowania prawnie wiążących decyzji w razie sporów między organami nadzorczymi. W tym celu powinna wydawać, zasadniczo większością dwóch trzecich głosów swoich członków, prawnie wiążące decyzje w jasno określonych przypadkach, gdy wśród organów nadzorczych panują sprzeczne opinie – w szczególności w ramach mechanizmu współpracy między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy – co do meritum sprawy, w szczególności tego, czy doszło do naruszenia niniejszego rozporządzenia.

(137) Może wystąpić pilna potrzeba podjęcia działań w celu ochrony praw i wolności osób, których dane dotyczą, w szczególności gdy istnieje ryzyko, że wyegzekwowanie prawa przysługującego osobie, której dane dotyczą, może być znacznie utrudnione. Organ nadzorczy powinien w związku z tym mieć możliwość przyjmowania na swoim terytorium należycie uzasadnionych środków tymczasowych o określonym okresie obowiązywania, który nie powinien przekraczać trzech miesięcy.

(138) Jeżeli zastosowanie takiego mechanizmu jest obowiązkowe, to od jego zastosowania powinna zależeć zgodność z prawem środka, którym organ nadzorczy chce wywołać skutki prawne. W innych przypadkach o znaczeniu transgranicznym należy stosować mechanizm współpracy między wiodącym organem nadzorczym a organami nadzorczymi, których sprawa dotyczy, oraz można świadczyć wzajemną pomoc i prowadzić wspólne operacje między organami nadzorczymi, których sprawa dotyczy, na zasadzie dwustronnej lub wielostronnej bez uruchamiania mechanizmu spójności.

(139) Aby wspierać spójne stosowanie niniejszego rozporządzenia, należy utworzyć – jako niezależny organ Unii – Europejską Radę Ochrony Danych. Rada ta, by móc realizować swoje cele, powinna mieć osobowość prawną. Europejską Radę Ochrony Danych powinien reprezentować jej przewodniczący. Powinna ona zastąpić Grupę Roboczą ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych, powołaną na mocy dyrektywy 95/46/WE. W jej skład powinni wchodzić szefowie organów nadzorczych wszystkich państw członkowskich oraz Europejski Inspektor Ochrony Danych lub ich przedstawiciele. Komisja powinna uczestniczyć bez prawa głosu w działaniach Europejskiej Rady Ochrony Danych, a Europejski Inspektor Ochrony Danych – bez prawa głosu w niektórych sprawach. Europejska Rada Ochrony Danych powinna przyczyniać się do spójnego stosowania niniejszego rozporządzenia w całej Unii, m.in. po-

przez doradzanie Komisji – w szczególności w sprawie stopnia ochrony w państwach trzecich lub organizacjach międzynarodowych – i propagowanie współpracy organów nadzorczych w całej Unii. Wypełniając swoje zadania, Europejska Rada Ochrony Danych powinna działać w sposób niezależny.

(140) Europejską Radę Ochrony Danych powinien wspierać sekretariat, zapewniany przez Europejskiego Inspektora Ochrony Danych. Personel Europejskiego Inspektora Ochrony Danych wykonujący zadania, które niniejsze rozporządzenie powierza Europejskiej Radzie Ochrony Danych, powinien wykonywać swoje zadania wyłącznie pod kierunkiem przewodniczącego Europejskiej Rady Ochrony Danych i jemu podlegać.

(141) Każda osoba, której dane dotyczą, powinna mieć prawo wniesienia skargi do jednego organu nadzorczego oraz prawo do skutecznego środka ochrony prawnej przed sądem, zgodnie z art. 47 Karty praw podstawowych, w szczególności w państwie członkowskim, w którym ma miejsce zwykłego pobytu, a jeżeli uzna, że jej prawa wynikające z niniejszego rozporządzenia są naruszane, lub jeżeli organ nadzorczy nie reaguje na skargę, częściowo lub w całości ją odrzuca lub oddala, lub nie podejmuje działania, choć jest to niezbędne do ochrony praw tej osoby. Postępowanie wyjaśniające na podstawie skargi powinno być prowadzone – z zastrzeżeniem kontroli sądowej – w zakresie odpowiadającym konkretnej sprawie. Organ nadzorczy powinien w rozsądnym terminie poinformować osobę, której dane dotyczą, o postępach i wynikach rozpatrywania skargi. Jeżeli dana sprawa wymaga dalszego postępowania wyjaśniającego lub koordynacji działań z innym organem nadzorczym, osoba, której dane dotyczą, powinna zostać o tym uprzednio poinformowana. Aby ułatwić wnoszenie skarg, każdy organ nadzorczy powinien zastosować takie środki jak udostępnienie formularza skargi, który można wypełnić także elektronicznie, przy czym nie należy wykluczać innych sposobów komunikacji.

(142) Jeżeli osoba, której dane dotyczą, uzna, że naruszane są jej prawa wynikające z niniejszego rozporządzenia, powinna mieć ona prawo zlecić podmiotowi, organizacji lub zrzeszeniu – które nie mają charakteru zarobkowego, zostały ustanowione zgodnie z prawem państwa członkowskiego, mają statutowo na celu interes publiczny i działają w dziedzinie ochrony danych osobowych – wniesienie skargi w swoim imieniu do organu nadzorczego, wykonanie prawa do środka ochrony prawnej przed sądem w imieniu osób, których dane dotyczą lub – o ile taką możliwość przewiduje prawo państwa członkowskiego – żądanie odszkodowania w imieniu osób, których dane dotyczą. Państwo członkowskie może wymagać, by taki podmiot, taka organizacja lub takie zrzeszenie niezależnie od zlecenia otrzymanego od osoby, której dane dotyczą, miały prawo wniesienia w tym państwie członkowskim skargi oraz miały prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli mają powody, by uznać, że w wyniku przetwarzania danych osobowych w sposób naruszający niniejsze rozporządzenie naruszone zostały prawa osoby, której dane dotyczą. Takiemu podmiotowi, takiej organizacji lub takiemu

zrzeszeniu nie może przysługiwać prawo do występowania o odszkodowanie w imieniu osoby, której dane dotyczą, jeżeli nie zostały do tego umocowane przez tę osobę.

(143) Każda osoba fizyczna lub prawna ma prawo wnieść do Trybunału Sprawiedliwości skargę o unieważnienie decyzji Europejskiej Rady Ochrony Danych na warunkach przewidzianych w art. 263 TFUE. Organy nadzorcze, których sprawa dotyczy, chcące takie decyzje zaskarżyć – jako adresaci takich decyzji – muszą wnieść skargę w terminie dwóch miesięcy od notyfikowania im tych decyzji, zgodnie z art. 263 TFUE. Jeżeli decyzje Europejskiej Rady Ochrony Danych bezpośrednio i indywidualnie dotyczą administratora, podmiotu przetwarzającego lub skarżącego, ten ostatni może wnieść skargę o unieważnienie tych decyzji w terminie dwóch miesięcy od ich publikacji na stronie internetowej Europejskiej Rady Ochrony Danych, zgodnie z art. 263 TFUE. Z zastrzeżeniem prawa wynikającego z art. 263 TFUE, każda osoba fizyczna lub prawna powinna mieć prawo do skutecznego środka ochrony prawnej przed właściwym sądem krajowym wobec decyzji organu nadzorczego wywołującej skutki prawne wobec tej osoby. Taka decyzja może dotyczyć w szczególności wykonywania przez organ nadzorczy uprawnień do prowadzenia postępowań wyjaśniających, uprawnień naprawczych i do wydawania zezwoleń lub oddalania lub odrzucania skarg. Prawo do skutecznego środka ochrony prawnej przed sądem nie dotyczy jednak niewiążących prawnie środków przyjętych przez organy nadzorcze, takich jak wydawane przez nie opinie czy zalecenia. Skarga przeciwko organowi nadzorczemu powinna być wnoszona do sądu państwa członkowskiego, w którym organ nadzorczy ma siedzibę, a postępowanie powinno się toczyć zgodnie z prawem tego państwa członkowskiego. Sądy te powinny wykonywać pełną jurysdykcję w sprawie, w tym w zakresie ustalenia okoliczności faktycznych i prawnych mających znaczenie dla rozstrzygnięcia sprawy.

Jeżeli organ nadzorczy odrzuci lub oddali skargę, skarżący może wnieść odwołanie do sądu tego samego państwa członkowskiego. W kontekście środków ochrony prawnej przed sądem dotyczących stosowania niniejszego rozporządzenia sądy krajowe uznające, że decyzja w tej kwestii jest niezbędna do wydania wyroku, mogą, a w przypadku przewidzianym w art. 267 TFUE – muszą, zwrócić się do Trybunału Sprawiedliwości o orzeczenie w trybie prejudycjalnym w sprawie wykładni prawa Unii, w tym niniejszego rozporządzenia. Ponadto jeżeli decyzja organu nadzorczego wdrażająca decyzję Europejskiej Rady Ochrony Danych zostanie zaskarżona przed sądem krajowym, a przedmiotem będzie ważność decyzji Europejskiej Rady Ochrony Danych, sąd krajowy nie jest uprawniony do stwierdzenia nieważności decyzji Europejskiej Rady Ochrony Danych, ale jeżeli uważa tę decyzję za nieważną, musi przekazać sprawę jej ważności Trybunałowi Sprawiedliwości zgodnie z art. 267 TFUE i jego wykładnią dokonaną przez Trybunał Sprawiedliwości. Sąd krajowy nie może jednak przekazać Trybunałowi Sprawiedliwości sprawy ważności decyzji Europejskiej Rady Ochrony Danych na wniosek osoby fizycznej lub prawnej, która miała możliwość wnieść skargę o unieważnienie

tej decyzji, w szczególności gdy decyzja ta bezpośrednio i indywidualnie jej dotyczyła, ale nie zrobiła tego w terminie przewidzianym w art. 263 TFUE.

(144) Jeżeli sąd, przed którym toczy się postępowanie przeciwko decyzji organu nadzorczego, ma powody przypuszczać, że przed sądem właściwym innego państwa członkowskiego wszczęto postępowanie w sprawie tego samego przetwarzania – na przykład w tym samym przedmiocie w związku z przetwarzaniem prowadzonym przez tego samego administratora lub przez ten sam podmiot przetwarzający lub odnośnie do tej samej przyczyny – powinien skontaktować się z tym sądem, aby potwierdzić, czy takie powiązane postępowanie się odbywa. Jeżeli przed sądem w innym państwie członkowskim toczy się powiązane postępowanie, każdy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić postępowanie lub może – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji na rzecz sądu, przed którym jako pierwszym wszczęto postępowanie, jeżeli sąd ten ma jurysdykcję w danej sprawie, a jego prawo zezwala na połączenie takich powiązanych postępowań. Postępowania uznaje się za powiązane, jeżeli związek między nimi jest tak ścisły, że celowe jest ich łączne rozpatrzenie i rozstrzygnięcie, tak by uniknąć ryzyka zapadnięcia sprzecznych orzeczeń w odrębnych postępowaniach.

(145) W przypadku postępowania przeciwko administratorowi lub podmiotowi przetwarzającemu skarżący powinien mieć możliwość wybrania, do którego sądu chce wnieść skargę: do sądu w państwie członkowskim, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną, czy do sądu w państwie członkowskim, w którym osoba, której dane dotyczą, ma miejsce zamieszkania, o ile administrator nie jest organem publicznym państwa członkowskiego działającym w ramach wykonywania swoich uprawnień publicznych.

(146) Za szkodę, którą dana osoba poniosła wskutek przetwarzania w sposób naruszający niniejsze rozporządzenie, powinno przysługiwać odszkodowanie od administratora lub podmiotu przetwarzającego. Administrator lub podmiot przetwarzający powinni jednak zostać zwolnieni z odpowiedzialności prawnej, jeżeli udowodnią, że szkoda w żadnym razie nie powstała z ich winy. Pojęcie szkody należy interpretować szeroko, w świetle orzecznictwa Trybunału Sprawiedliwości, w sposób w pełni odzwierciedlający cele niniejszego rozporządzenia. Nie ma to wpływu na roszczenia z tytułu szkód wynikających z naruszenia innych przepisów prawa Unii lub prawa państwa członkowskiego. Przetwarzanie dokonywane w sposób naruszający niniejsze rozporządzenie obejmuje także przetwarzanie, które narusza akty delegowane i wykonawcze przyjęte na mocy niniejszego rozporządzenia oraz prawo państwa członkowskiego doprecyzowujące niniejsze rozporządzenie. Osoby, których dane dotyczą, powinny uzyskać pełne i skuteczne odszkodowanie za poniesione szkody. Jeżeli administratorzy lub podmioty przetwarzające uczestniczą w tym samym przetwarzaniu, każdy administrator lub podmiot przetwarzający powinien odpowiadać prawnie za całość szkody. Jeżeli jednak zostaną włączeni do jednego postępowania

sądowego zgodnie z prawem państwa członkowskiego, odszkodowaniem można obarczyć każdego z administratorów i każdy z podmiotów przetwarzających stosownie do ich winy za szkodę wynikłą z przetwarzania, o ile osobie, której dane dotyczą, zapewnione zostanie pełne i skuteczne odszkodowanie za poniesioną szkodę. Każdy administrator lub podmiot przetwarzający, który wypłacił pełne odszkodowanie, może następnie dochodzić roszczeń regresowych wobec innych administratorów lub podmiotów przetwarzających uczestniczących w tym samym przetwarzaniu.

(147) Jeżeli niniejsze rozporządzenie przewiduje szczegółowe przepisy o jurysdykcji – w szczególności odnośnie do postępowań w zakresie środków ochrony prawnej przed sądem, w tym odszkodowania, przeciwko administratorowi lub podmiotowi przetwarzającemu – ogólne przepisy o jurysdykcji, takie jak rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012[13], nie powinny naruszać stosowania takich szczegółowych przepisów.

(148) Aby egzekwowanie przepisów niniejszego rozporządzenia było skuteczniejsze, należy za jego naruszenie nakładać sankcje, w tym administracyjne kary pieniężne – oprócz lub zamiast odpowiednich środków nakładanych na mocy niniejszego rozporządzenia przez organ nadzorczy. Jeżeli naruszenie jest niewielkie lub jeżeli grożąca kara pieniężna stanowiłaby dla osoby fizycznej nieproporcjonalne obciążenie, można zamiast tego udzielić upomnienia. Powinno się jednak zwrócić należytą uwagę na charakter, wagę oraz czas trwania naruszenia, na to, czy naruszenie nie było umyślne, na działania podjęte dla zminimalizowania szkody, na stopień odpowiedzialności lub wszelkie mające znaczenie wcześniejsze naruszenia, na sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, na przestrzeganie środków nałożonych na administratora lub podmiot przetwarzający, na stosowanie kodeksów postępowania oraz wszelkie inne czynniki obciążające lub łagodzące. Nakładanie sankcji, w tym administracyjnych kar pieniężnych, powinno podlegać odpowiednim zabezpieczeniom proceduralnym zgodnym z ogólnymi zasadami prawa Unii i z Kartą praw podstawowych, w tym skutecznej ochronie prawnej i prawu do rzetelnego procesu.

(149) Państwa członkowskie powinny mieć możliwość ustanawiania przepisów przewidujących sankcje karne za naruszenie niniejszego rozporządzenia, w tym za naruszenie krajowych przepisów przyjętych na jego mocy i w jego granicach. Sankcje karne mogą również obejmować pozbawienie zysków wynikających z naruszenia niniejszego rozporządzenia. Jednak nałożenie sankcji karnych za naruszenie takich krajowych przepisów oraz nałożenie sankcji administracyjnych nie powinno prowadzić do naruszenia zasady ne bis in idem, zgodnie z wykładnią Trybunału Sprawiedliwości.

[13] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1215/2012 z dnia 12 grudnia 2012 r. w sprawie jurysdykcji i uznawania orzeczeń sądowych oraz ich wykonywania w sprawach cywilnych i handlowych (Dz.U. L 351 z 20.12.2012, s. 1).

(150) W celu wzmocnienia i zharmonizowania sankcji administracyjnych za naruszenie niniejszego rozporządzenia każdy organ nadzorczy powinien być uprawniony do nakładania administracyjnych kar pieniężnych. W niniejszym rozporządzeniu należy wymienić rodzaje naruszeń oraz wskazać górną granicę i kryteria ustalania związanych z nimi administracyjnych kar pieniężnych, które właściwy organ nadzorczy powinien określać indywidualnie dla każdego przypadku z uwzględnieniem wszystkich stosownych okoliczności danej sytuacji, z należytym uwzględnieniem w szczególności charakteru, wagi, czasu trwania naruszenia i jego konsekwencji, a także środków podjętych w celu zastosowania się do obowiązków wynikających z niniejszego rozporządzenia oraz w celu zapobieżenia konsekwencjom naruszenia lub w celu zminimalizowania tych konsekwencji. Jeżeli administracyjna kara pieniężna jest nakładana na przedsiębiorstwo, to „przedsiębiorstwo" należy do tych celów rozumieć zgodnie z art. 101 i 102 TFUE. Jeżeli administracyjna kara pieniężna jest nakładana na osobę niebędącą przedsiębiorstwem, organ nadzorczy, ustalając właściwą wysokość kary pieniężnej, powinien wziąć pod uwagę ogólny poziom dochodów w danym państwie członkowskim oraz sytuację ekonomiczną tej osoby. Aby wspierać spójne stosowanie administracyjnych kar pieniężnych, można także użyć mechanizmu spójności. Państwa członkowskie powinny określić, czy i w jakim zakresie administracyjnym karom pieniężnym powinny podlegać organy publiczne. Nałożenie administracyjnej kary pieniężnej lub wydanie ostrzeżenia nie wpływa na stosowanie innych uprawnień organów nadzorczych ani innych sankcji na mocy niniejszego rozporządzenia.

(151) Systemy prawne Danii i Estonii nie przewidują administracyjnych kar pieniężnych określonych w niniejszym rozporządzeniu. Przepisy o administracyjnych karach pieniężnych można stosować tak, że w Danii właściwy sąd krajowy będzie nakładać grzywnę jako sankcję karną, a w Estonii organ nadzorczy będzie nakładać grzywnę w ramach postępowania o wykroczenie, pod warunkiem że takie stosowanie przepisów w tych państwach członkowskich będzie mieć skutek równoważny administracyjnej karze pieniężnej nakładanej przez organ nadzorczy. Dlatego właściwy sąd krajowy powinien brać pod uwagę zalecenie organu nadzorczego, który postuluje nałożenie grzywny. Nakładane grzywny muszą być w każdym przypadku skuteczne, proporcjonalne i odstraszające.

(152) W sytuacjach, w których niniejsze rozporządzenie nie harmonizuje sankcji administracyjnych, lub w razie potrzeby w innych przypadkach, na przykład w razie poważnego naruszenia niniejszego rozporządzenia, państwa członkowskie powinny wdrożyć system przewidujący skuteczne, proporcjonalne i odstraszające sankcje. Charakter takich sankcji (karny lub administracyjny) powinno określać prawo państwa członkowskiego.

(153) Prawo państw członkowskich powinno godzić przepisy regulujące wolność wypowiedzi i informacji, w tym wypowiedzi dziennikarskiej, akademickiej, artystycznej lub literackiej, z prawem do ochrony danych osobowych na mocy niniejszego rozpo-

rządzenia. Przetwarzanie danych osobowych jedynie do celów dziennikarskich lub do celów wypowiedzi akademickiej, artystycznej lub literackiej powinno podlegać wyjątkom lub odstępstwom od niektórych przepisów niniejszego rozporządzenia, jeżeli jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, przewidzianymi w art. 11 Karty praw podstawowych. Powinno mieć to zastosowanie w szczególności do przetwarzania danych osobowych w dziedzinie audiowizualnej oraz w archiwach i bibliotekach prasowych. Państwa członkowskie powinny więc przyjąć akty prawne określające odstępstwa i wyjątki niezbędne do zapewnienia równowagi między tymi prawami podstawowymi. Państwa członkowskie powinny przyjąć takie odstępstwa i wyjątki w odniesieniu do zasad ogólnych, praw przysługujących osobie, której dane dotyczą, administratora i podmiotu przetwarzającego, przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych, niezależnych organów nadzorczych, współpracy i spójności oraz szczególnych sytuacji przetwarzania danych. Jeżeli odstępstwa i wyjątki różnią się zależnie od państwa członkowskiego, zastosowanie powinno mieć prawo państwa członkowskiego, któremu podlega administrator. Aby uwzględnić, jak ważna dla każdego demokratycznego społeczeństwa jest wolność wypowiedzi, pojęcia dotyczące tej wolności, takie jak dziennikarstwo, należy interpretować szeroko.

(154) Niniejsze rozporządzenie pozwala uwzględnić przy stosowaniu jego przepisów zasadę publicznego dostępu do dokumentów urzędowych. Publiczny dostęp do dokumentów urzędowych można uznać za interes publiczny. Organ publiczny lub podmiot publiczny powinny móc publicznie ujawniać dane osobowe z dokumentów przez siebie przechowywanych, jeżeli takie ujawnienie jest przewidziane przepisami prawa Unii lub prawa państwa członkowskiego, któremu organ ten lub podmiot podlegają. Przepisy takie powinny godzić publiczny dostęp do dokumentów urzędowych i ponowne wykorzystywanie informacji sektora publicznego z prawem do ochrony danych osobowych, i dlatego mogą przewidywać niezbędne uwzględnienie prawa do ochrony danych osobowych na podstawie niniejszego rozporządzenia. Wzmianka o organach i podmiotach publicznych powinna w tym kontekście dotyczyć wszystkich organów lub innych podmiotów objętych prawem państwa członkowskiego dotyczącym publicznego dostępu do dokumentów. Dyrektywa Parlamentu Europejskiego i Rady 2003/98/WE[14] nie narusza ani w żaden sposób nie wpływa na stopień ochrony osób fizycznych w związku z przetwarzaniem danych osobowych wynikający z przepisów prawa Unii i prawa państwa członkowskiego, a w szczególności nie zmienia obowiązków i praw przewidzianych w niniejszym rozporządzeniu. Dyrektywa ta nie powinna mieć zastosowania w szczególności do dokumentów, do których – w ramach systemów dostępu – dostęp jest wykluczony lub ograniczony z powodu ochrony danych osobowych, ani do fragmentów dokumentów dostępnych w ramach tych systemów, ale zawierających dane osobowe,

[14] Dyrektywa 2003/98/WE Parlamentu Europejskiego i Rady z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego (Dz.U. L 345 z 31.12.2003, s. 90).

których ponowne wykorzystanie zostało określone w prawie jako niezgodne z prawem o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych.

(155) W prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem, w szczególności warunki, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę, w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

(156) Przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych powinno podlegać odpowiednim zabezpieczeniom praw i wolności osoby, której dane dotyczą, zgodnie z niniejszym rozporządzeniem. Zabezpieczenia te powinny polegać na wdrożeniu środków technicznych i organizacyjnych zapewniających w szczególności poszanowanie zasady minimalizacji danych. Dalsze przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych można prowadzić, jeżeli administrator ocenił, czy celów tych nie można osiągnąć przetwarzaniem danych osobowych, które albo od początku albo już dłużej nie pozwalają identyfikować osób, których dane dotyczą, pod warunkiem że istnieją odpowiednie zabezpieczenia (takie jak pseudonimizacja danych osobowych). Państwa członkowskie powinny ustanowić odpowiednie zabezpieczenia w odniesieniu do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Państwa członkowskie powinny mieć możliwość ustanowienia – na określonych warunkach i z zastrzeżeniem odpowiednich zabezpieczeń dla osób, których dane dotyczą – szczegółowych uregulowań i wyjątków od wymogu udzielenia informacji oraz prawa do sprostowania lub usuwania danych osobowych, do „bycia zapomnianym", do ograniczenia przetwarzania i do przenoszenia danych oraz do sprzeciwu, gdy dane osobowe są przetwarzane do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Takie warunki i zabezpieczenia mogą skutkować szczegółowymi procedurami wykonywania tych praw przez osoby, których dane dotyczą – jeżeli jest to właściwe w świetle celów, którym służy konkretne przetwarzanie – oraz środkami technicznymi i organizacyjnymi mającymi ograniczyć przetwarzanie danych osobowych w myśl zasad proporcjonalności i konieczności. Przetwarzanie danych osobowych do celów naukowych powinno też być zgodne z innymi odpowiednimi przepisami, takimi jak przepisy o próbach klinicznych.

(157) Łącząc ze sobą informacje z rejestrów, naukowcy mogą uzyskać nową, wartościową wiedzę na przykład o częstych chorobach, takich jak choroba układu krążenia, rak czy depresja. Korzystając z rejestrów, można uściślić wyniki badań naukowych, gdyż będą się one opierać na większej próbie. W naukach społecznych badania oparte na rejestrach pozwalają naukowcom uzyskać kluczową wiedzę o długoterminowych współzależnościach wielu czynników społecznych, na przykład bezrobocia czy edukacji z innymi czynnikami bytowymi. Wyniki badań uzyskane z rejestrów dostarczają solidnej, dobrej jakościowo wiedzy, która może posłużyć do opracowywania i realizowania polityki opartej na wiedzy, podnieść jakość życia wielu osób, a także zwiększyć skuteczność usług społecznych itp. Dla ułatwienia badań naukowych dopuszcza się przetwarzanie danych osobowych do celów badań naukowych z zastrzeżeniem odpowiednich warunków i zabezpieczeń przewidzianych w prawie Unii lub w prawie państwa członkowskiego.

(158) Jeżeli dane osobowe są przetwarzane do celów archiwalnych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do danych osobowych osób zmarłych. Organy lub podmioty publiczne lub podmioty prywatne posiadające wpisy będące przedmiotem interesu publicznego powinny zgodnie z prawem Unii lub prawem państwa członkowskiego mieć prawny obowiązek nabywania, ochrony, oszacowywania, systematyzowania, opisywania, przekazywania, promowania, rozpowszechniania i udostępniania wpisów o trwałej wartości dla ogólnego interesu publicznego. Państwa członkowskie powinny także mieć możliwość zezwolenia na dalsze przetwarzanie danych osobowych do celów archiwalnych, na przykład z myślą o dostarczeniu konkretnych informacji o postawie politycznej w dawnych systemach państw totalitarnych, o przypadkach ludobójstwa, zbrodniach przeciwko ludzkości (zwłaszcza holokauście) czy zbrodniach wojennych.

(159) Jeżeli dane osobowe są przetwarzane do celów badań naukowych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. W niniejszym rozporządzeniu przetwarzanie danych osobowych do celów badań naukowych należy interpretować szeroko, obejmując tym pojęciem na przykład rozwój technologiczny i demonstrację, badania podstawowe, badania stosowane oraz badania finansowane ze środków prywatnych. Ponadto należy uwzględnić cel Unii określony w art. 179 ust. 1 TFUE, którym jest utworzenie europejskiej przestrzeni badawczej. Wyrażenie „do celów badań naukowych" powinno obejmować także badania prowadzone w interesie publicznym w dziedzinie zdrowia publicznego. Z uwagi na specyfikę przetwarzania danych osobowych do celów badań naukowych zastosowanie powinny mieć specjalne warunki, w szczególności w odniesieniu do publikacji lub innego ujawniania danych osobowych w kontekście celów badań naukowych. Jeżeli wynik badań naukowych, w szczególności w kontekście zdrowotnym, uzasadnia dalsze środki w interesie osoby, której dane dotyczą, do środków tych powinny mieć zastosowanie przepisy ogólne niniejszego rozporządzenia.

(160) Jeżeli dane osobowe są przetwarzane w celu badań historycznych, niniejsze rozporządzenie powinno mieć zastosowanie także do takiego przetwarzania. Powinno to dotyczyć m.in. badań historycznych i badań do celów genealogicznych; należy jednak pamiętać, że niniejsze rozporządzenie nie powinno mieć zastosowania do osób zmarłych.

(161) Do celów wyrażenia zgody na udział w badaniach naukowych podczas prób klinicznych zastosowanie powinny mieć stosowne przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 536/2014[15].

(162) Jeżeli dane osobowe są przetwarzane do celów statystycznych, niniejsze rozporządzenie powinno mieć zastosowanie do takiego przetwarzania. Prawo Unii lub prawo państwa członkowskiego powinny – w granicach niniejszego rozporządzenia – określać treść statystyczną, kontrolę dostępu, warunki przetwarzania danych osobowych do celów statystycznych oraz odpowiednie środki mające chronić prawa i wolności osoby, której dane dotyczą, oraz gwarantować poufność statystyczną. Wyrażenie „cele statystyczne" oznacza każdą operację zbierania i przetwarzania danych osobowych niezbędnych do badań statystycznych lub do opracowywania wyników statystycznych. Z kolei wyniki statystyczne mogą następnie służyć do dalszych celów, m.in. do celów badań naukowych. Wyrażenie „cel statystyczny" sugeruje, że wynikiem przetwarzania do celów statystycznych nie są dane osobowe, lecz dane zbiorcze, i że wynik ten lub te dane osobowe nie służą za podstawę środków czy decyzji dotyczących konkretnych osób fizycznych.

(163) Należy chronić informacje poufne, które organy statystyczne Unii i państw członkowskich gromadzą do celów opracowywania oficjalnych statystyk europejskich i krajowych. Statystyki europejskie należy projektować, tworzyć i rozpowszechniać zgodnie z zasadami statystycznymi przewidzianymi w art. 338 ust. 2 TFUE, przy czym statystyki krajowe powinny być także zgodne z prawem państwa członkowskiego. Dalsze szczegółowe informacje o statystycznej poufności statystyki europejskiej zawiera rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 223/2009[16].

(164) W odniesieniu do uprawnień organów nadzorczych do uzyskania od administratora lub podmiotu przetwarzającego dostępu do danych osobowych oraz do pomieszczeń, państwa członkowskie mogą – w granicach niniejszego rozporządzenia – przyjąć przepisy szczegółowe mające chronić obowiązek zachowania tajemnicy za-

[15] Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 536/2014 z dnia 16 kwietnia 2014 r. w sprawie badań klinicznych produktów leczniczych stosowanych u ludzi oraz uchylenia dyrektywy 2001/20/WE (Dz.U. L 158 z 27.5.2014, s. 1).

[16] 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, s. 164).

wodowej lub innej równoważnej tajemnicy, o ile jest to niezbędne, by pogodzić prawo do ochrony danych osobowych z obowiązkiem zachowania tajemnicy zawodowej. Pozostaje to bez uszczerbku dla istniejących obowiązków państw członkowskich, by tam, gdzie tego wymaga prawo Unii, przyjąć przepisy o tajemnicy zawodowej.

(165) Niniejsze rozporządzenie nie narusza statusu przyznanego kościołom oraz związkom lub wspólnotom wyznaniowym na mocy prawa konstytucyjnego obowiązującego w państwach członkowskich i nie narusza tego statusu – jak uznano w art. 17 TFUE.

(166) Aby spełnić cele niniejszego rozporządzenia, mianowicie chronić podstawowe prawa i wolności osób fizycznych, w szczególności prawo do ochrony danych osobowych, oraz zagwarantować swobodny przepływ danych osobowych w Unii, należy przekazać Komisji uprawnienia do przyjmowania aktów zgodnie z art. 290 TFUE.

Akty delegowane powinny zostać w szczególności przyjęte w odniesieniu do kryteriów i wymogów obowiązujących w mechanizmach certyfikacji, w odniesieniu do informacji przedstawianych za pomocą standardowych znaków graficznych oraz w odniesieniu do procedur ustanawiania takich znaków. Szczególnie ważne jest, aby w czasie swoich prac przygotowawczych Komisja prowadziła odpowiednie konsultacje, w tym na szczeblu eksperckim. W trakcie przygotowywania i opracowywania aktów delegowanych Komisja powinna zapewnić jednoczesne, terminowe i odpowiednie przekazywanie stosownych dokumentów Parlamentowi Europejskiemu i Radzie.

(167) Aby zapewnić jednolite warunki wdrażania niniejszego rozporządzenia, należy powierzyć Komisji uprawnienia wykonawcze, tak jak to przewiduje niniejsze rozporządzenie. Uprawnienia te powinny być wykonywane zgodnie z rozporządzeniem (UE) nr 182/2011. W tym kontekście Komisja powinna rozważyć wprowadzenie szczególnych środków dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw.

(168) Procedurę sprawdzającą należy stosować do przyjmowania aktów wykonawczych w odniesieniu do: standardowych klauzul umownych między administratorami a podmiotami przetwarzającymi oraz między podmiotami przetwarzającymi; kodeksów postępowania; technicznych standardów i mechanizmów certyfikacji; odpowiedniego stopnia ochrony zapewnianego przez państwo trzecie, terytorium lub określony sektor w tym państwie trzecim lub organizację międzynarodową; standardowych klauzul ochrony danych; formatów i procedur wymiany informacji drogą elektroniczną między administratorami, pomiotami przetwarzającymi i organami nadzorczymi na potrzeby wiążących reguł korporacyjnych; wzajemnej pomocy; oraz uzgodnień w sprawie wymiany informacji drogą elektroniczną między organami nadzorczymi oraz między organami nadzorczymi a Europejską Radą Ochrony Danych.

(169) Komisja powinna przyjmować akty wykonawcze mające natychmiastowe zastosowanie, jeżeli z dostępnych dowodów wynika, że państwo trzecie, terytorium

lub określony sektor w tym państwie trzecim lub organizacja międzynarodowa nie zapewniają odpowiedniego stopnia ochrony, i jeżeli zachodzi szczególnie pilna potrzeba działania.

(170) Ponieważ celu niniejszego rozporządzenia, mianowicie zapewnienia równoważnego stopnia ochrony osób fizycznych i swobodnego przepływu danych osobowych w całej Unii, nie mogą w wystarczającym stopniu osiągnąć państwa członkowskie, natomiast z uwagi na zakres i skutki proponowanego działania możliwe jest lepsze jego osiągnięcie na szczeblu unijnym, Unia może przyjąć środki zgodnie z zasadą pomocniczości, o której mowa w art. 5 Traktatu o Unii Europejskiej (TUE). Zgodnie z zasadą proporcjonalności określoną w tym samym artykule niniejsze rozporządzenie nie wykracza poza zakres niezbędny do osiągnięcia tego celu.

(171) Niniejszym rozporządzeniem należy uchylić dyrektywę 95/46/WE. Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów. Jeżeli przetwarzanie ma za podstawę zgodę w myśl dyrektywy 95/46/WE, osoba, której dane dotyczą, nie musi ponownie wyrażać zgody, jeżeli pierwotny sposób jej wyrażenia odpowiada warunkom niniejszego rozporządzenia; dzięki temu administrator może kontynuować przetwarzanie po dacie rozpoczęcia stosowania niniejszego rozporządzenia. Decyzje przyjęte przez Komisję oraz zezwolenia wydane przez organy nadzorcze na podstawie dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

(172) Zgodnie z art. 28 ust. 2 rozporządzenia (WE) nr 45/2001 przeprowadzono konsultacje z Europejskim Inspektorem Ochrony Danych, który wydał opinię w dniu 7 marca 2012 r.[17]

(173) Niniejsze rozporządzenie powinno mieć zastosowanie do wszystkich tych kwestii dotyczących ochrony podstawowych praw i wolności w związku z przetwarzaniem danych osobowych, które nie podlegają szczególnym obowiązkom mającym ten sam cel określonym w dyrektywie Parlamentu Europejskiego i Rady 2002/58/WE[18]**, w tym obowiązkom nałożonym na administratora oraz prawom osób fizycznych. Aby doprecyzować związek między niniejszym rozporządzeniem a dyrektywą 2002/58/WE, dyrektywę tę należy odpowiednio zmienić. Gdy niniejsze rozporządzenie zostanie przyjęte, dyrektywa 2002/58/WE powinna zostać poddana przeglądowi, w szczególności w celu zapewnienia jej spójności z niniejszym rozporządzeniem,**

PRZYJMUJĄ NINIEJSZE ROZPORZĄDZENIE:

[17] Dz.U. C 192 z 30.6.2012, s. 7.

[18] 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, s. 37).

ROZDZIAŁ I
Przepisy ogólne

Artykuł 1
Przedmiot i cele

1. W niniejszym rozporządzeniu ustanowione zostają przepisy o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych oraz przepisy o swobodnym przepływie danych osobowych.
2. Niniejsze rozporządzenie chroni podstawowe prawa i wolności osób fizycznych, w szczególności ich prawo do ochrony danych osobowych.
3. Nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

1. Komentowany artykuł wskazuje przedmiot i cele regulacji rozporządzenia 2016/679. Przedmiotem regulacji jest ochrona osób fizycznych w związku z przetwarzaniem danych osobowych. Zagwarantowanie ochrony osób, których dane poddawane są przetwarzaniu, ma umożliwić swobodny przepływ danych osobowych w Unii Europejskiej. Prawo do ochrony danych osobowych, do którego odnosi się komentowany przepis, jest jednym z podstawowych praw i wolności chronionych na mocy rozporządzenia. Ustęp 3 zawiera ponadto ogólny zakaz ograniczania bądź zakazywania swobodnego przepływu danych w UE ze względu na ochronę danych osobowych.

2. Artykuł 1 rozporządzenia stanowi odpowiednik art. 1 dyrektywy 95/46/WE, wskazującego cele i zakres przedmiotowy regulacji. Dowodzi to, iż komentowane rozporządzenie stanowi kontynuację unormowań prawnych obowiązujących od ponad 20 lat, opiera się w swojej konstrukcji na dotychczasowych przepisach, niekiedy tylko je uzupełniając lub modyfikując. Zasadnicza zmiana podejścia prawodawcy europejskiego dotyczy nie tyle treści regulacji, ile jej formy – dyrektywa wymagająca implementacji została zastąpiona rozporządzeniem, które ma być stosowane wprost, a jedynie uzupełnione

przepisami krajowymi w niewielkim zakresie przedmiotowym (m.in. o uszczegółowienie przepisów dotyczących organu nadzorczego i procedury), natomiast rozwiązania merytoryczne bazują na dotychczasowych konstrukcjach prawnych. Z tego powodu określenie przeprowadzonej reformy jako „rewolucji" w ochronie danych wydaje się przesadne, należy raczej uznać, że mamy do czynienia z podejściem ewolucyjnym, zmierzającym do zapewnienia spójności regulacji w całej UE, w celu poprawy skuteczności ochrony danych osobowych oraz uwzględnienia postępu technicznego.

3. Podstawową materią regulowaną w rozporządzeniu 2016/679, a wskazaną w ust. 1 komentowanego artykułu, jest ochrona osób fizycznych w związku z przetwarzaniem danych osobowych, określana skrótowo mianem ochrony danych osobowych. Warto jednak podkreślić, że istotą regulacji nie jest ochrona samych danych jako dóbr chronionych, ale ochrona osób fizycznych (każdego człowieka) przed negatywnymi konsekwencjami wynikającymi z niezgodnego z prawem przetwarzania danych. Przy takim podejściu prawodawcy ochrona danych jest instrumentem pozwalającym chronić osoby, których dane dotyczą, w związku z procesami przetwarzania danych.

4. Użyte w komentowanym przepisie określenia „dane osobowe" oraz „przetwarzanie" zostały zdefiniowane w słowniczku zawartym w art. 4 rozporządzenia 2016/679. Danymi osobowymi są informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, natomiast przetwarzaniem są operacje dokonywane na danych osobowych. Szerzej na temat znaczenia, jakie przepisy rozporządzenia przypisują tym pojęciom, patrz komentarz do art. 4.

5. Prawo do ochrony danych osobowych jest prawem gwarantowanym zarówno w krajowym, jak i unijnym porządku prawnym. Na płaszczyźnie krajowej regulacji prawo do ochrony danych osobowych znajduje oparcie w przepisie art. 51 Konstytucji RP. Przepis ten określa podstawowe uprawnienia składające się na prawo do ochrony danych osobowych, w kwestiach szczegółowych odsyłając do regulacji ustawowej.

6. W okresie minionych 20 lat problematyka ochrony danych osobowych była regulowana w krajowym prawodawstwie przepisami ustawy z 29.08.1997 r. o ochronie danych osobowych (Dz.U. z 2016 r. poz. 922 ze zm.) oraz licznymi przepisami szczególnymi. Na gruncie tych przepisów, a zwłaszcza art. 1 ust. 1 u.o.d.o.1997, stanowiącego, iż każdy ma prawo do ochrony dotyczących go danych osobowych, rozważano istotę, charakter oraz zakres tego prawa.

W piśmiennictwie przedmiotu przyjmuje się, że prawo do ochrony danych osobowych stanowi refleks ogólnej zasady autonomii informacyjnej człowieka i swego rodzaju emanację ogólnego prawa do prywatności, gwarantowanego w art. 47 Konstytucji RP, ze względu na to, że dane osobowe są częścią życia prywatnego bądź posługiwanie się danymi dotyczącymi innej osoby wkracza w przyznaną jej kompetencję do decydo-

wania o swoim życiu osobistym (por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych. Komentarz*, Warszawa 2015, s. 260–261).

Wywodząca się z prawa niemieckiego koncepcja autonomii informacyjnej jednostki jest przyjmowana również na gruncie prawa polskiego, co dostrzec można zarówno w poglądach doktrynalnych, jak też w judykaturze. W wyroku z 19.02.2002 r. (U 3/01, OTK-A 2002/1, poz. 3) Trybunał Konstytucyjny stwierdził, że tzw. autonomia informacyjna jednostki (gwarantowana w art. 51 Konstytucji RP), oznaczająca prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami znajdującymi się w posiadaniu innych podmiotów, są elementami składowymi prawa do ochrony prawnej życia prywatnego, gwarantowanego w art. 47 Konstytucji RP (na temat autonomii informacyjnej w orzecznictwie TK szerzej por. P. Litwiński, *Zasada autonomii informacyjnej w orzecznictwie Trybunału Konstytucyjnego a stosowanie przepisów o ochronie danych osobowych* [w:] *Ochrona danych osobowych w Polsce z perspektywy dziesięciolecia*, red. P. Fajgielski, Lublin 2008, s. 169–184). Jednak – na co zwrócił uwagę w literaturze M. Safjan – zakres autonomii informacyjnej jednostki stale zmniejsza się, co jest spowodowane przesuwaniem ciężaru ochrony jednostki i jej prywatności w kierunku instytucjonalnych, publicznoprawnych instytucji i środków. Prowadzi to do kreowania swoistego pozoru autonomii informacyjnej, ponieważ jednostka będąca pod silną presją wymagań współczesnej cywilizacji ma coraz mniejszy wpływ na zakres udostępnianej o sobie informacji (M. Safjan, *Prawo do prywatności i ochrona danych osobowych w społeczeństwie informatycznym*, PiP 2002/6, s. 5).

Gdy chodzi o charakter prawa do ochrony danych, to w piśmiennictwie przedmiotu prezentowane są różne poglądy: od pojmowania tego prawa w sposób zbliżony do ochrony dóbr osobistych (a nawet kreowania dobra osobistego w postaci autonomii informacyjnej człowieka), do ujmowania go w kategoriach własnościowych (przy traktowaniu danych osobowych jako swoistego niematerialnego dobra przysługującego osobie, której dane dotyczą). Szerzej na temat różnych koncepcji por. J. Barta, P. Fajgielski, R. Markiewicz, *Ochrona danych osobowych...*, s. 262 i n. oraz wskazaną tam literaturę; na ten temat patrz także: M. Sakowska-Baryła, *Prawo do ochrony danych osobowych*, Wrocław 2015, s. 92 i n.

7. Obecnie podstawą prawną ochrony danych osobowych w państwach członkowskich UE są przepisy komentowanego rozporządzenia, uzupełniane krajowymi regulacjami. Przepisy rozporządzenia są stosowane wprost, bez potrzeby implementacji, natomiast krajowe akty normatywne uzupełniają przepisy unijne m.in. o uregulowania odnoszące się do organów nadzorczych, norm proceduralnych oraz niektórych kwestii szczegółowych.

8. W porządku prawnym UE prawo do ochrony danych osobowych jest jednym z praw podstawowych, które zostało zagwarantowane w art. 8 ust. 1 Karty praw podstawowych UE

oraz art. 16 ust. 1 TFUE, o czym przypomina motyw 1 preambuły. W myśl wskazanych powyżej przepisów każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Zgodnie z art. 8 ust. 2 Karty praw podstawowych UE, dane osobowe powinny być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą; każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania, natomiast ust. 3 wskazanego tu artykułu stanowi, iż przestrzeganie tych zasad podlega kontroli niezależnego organu.

Przepis art. 16 ust. 2 TFUE uprawnia Parlament Europejski i Radę UE do tego, aby stanowiąc zgodnie ze zwykłą procedurą ustawodawczą, określiły zasady dotyczące ochrony osób fizycznych w zakresie przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii oraz przez państwa członkowskie w wykonywaniu działań wchodzących w zakres zastosowania prawa Unii, a także zasady dotyczące swobodnego przepływu takich danych. W odniesieniu do unijnych instytucji i organów zasady zostały określone w rozporządzeniu Parlamentu Europejskiego i Rady 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.Urz. UE L 295, s. 39 i n.), natomiast zasady ochrony danych przez państwa członkowskie regulowane są przepisami komentowanego rozporządzenia.

9. W ust. 2 komentowanego artykułu wskazano, że rozporządzenie chroni nie tylko prawo do ochrony danych osobowych, ale także inne podstawowe prawa i wartości. W motywie 4 preambuły wyjaśniono, że rozporządzenie nie narusza praw podstawowych, wolności i zasad uznanych w Karcie praw podstawowych – zapisanych w traktatach – w szczególności prawa do poszanowania życia prywatnego i rodzinnego, domu oraz komunikowania się, ochrony danych osobowych, wolności myśli, sumienia i religii, wolności wypowiedzi i informacji, wolności prowadzenia działalności gospodarczej, prawa do skutecznego środka prawnego i dostępu do bezstronnego sądu oraz różnorodności kulturowej, religijnej i językowej.

Prawo do ochrony danych osobowych nie ma charakteru absolutnego i podlega ograniczeniom, z uwagi na inne chronione prawem dobra i wartości. Motyw 4 preambuły wskazuje, iż przetwarzanie danych osobowych należy zorganizować w taki sposób, aby służyło ludzkości, a prawo do ochrony danych osobowych należy postrzegać w kontekście jego funkcji społecznej i wyważyć względem innych praw podstawowych w myśl zasady proporcjonalności.

Jednym z podstawowych obszarów, na których zarysowuje się widoczny konflikt między prawem do ochrony danych a innymi prawami i wolnościami, jest dostęp do informacji publicznej. W tym zakresie mamy do czynienia z dwoma odmiennymi prawami, które trudno ze sobą pogodzić, jednak prawodawca krajowy stara się łagodzić występujący na tym polu konflikt, określając zasady udostępniania informacji publicznej (w tym także informacji stanowiących dane osobowe, ingerujących w sferę prywatności) w przepisach ustawy z 6.09.2001 r. o dostępie do informacji publicznej (Dz.U. z 2020 r. poz. 2176). Szerzej na ten temat zob.: M. Sakowska-Baryła, *Dostęp do informacji publicznej a ochrona danych osobowych*, Wrocław 2014; I. Kamińska, M. Rozbicka-Ostrowska, *Ochrona danych osobowych a prawo do informacji publicznej,* Warszawa 2021 oraz wskazaną tam literaturę.

10. Ochrona praw osób, których dane poddawane są przetwarzaniu, nie jest jedynym celem komentowanej regulacji prawnej. Ustęp 3 komentowanego artykułu stanowi, iż rozporządzenie nie ogranicza ani też nie zakazuje swobodnego przepływu danych osobowych w UE z powodów odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych. Prawodawca unijny przyjmuje, iż jednym z celów, jakie mogą być osiągnięte dzięki zapewnieniu w UE jednolitego i spójnego stosowania oraz egzekwowania przepisów o ochronie danych osobowych, jest swobodny przepływ danych osobowych między podmiotami z krajów członkowskich. W preambule zwrócono uwagę na znaczne zwiększenie transgranicznych przepływów danych, postęp techniczny i globalizację, które pociągają za sobą potrzebę zapewnienia wysokiego stopnia ochrony danych, przy jednoczesnym zagwarantowaniu swobodnego przepływu danych osobowych. Swobodny przepływ danych w UE ma przyczynić się do rozwoju gospodarki cyfrowej na rynku wewnętrznym. Szerzej na ten temat por. motywy 5–10 preambuły.

W literaturze przedmiotu wskazuje się także inne (bardziej szczegółowe) cele, których realizacji ma służyć komentowane rozporządzenie, w tym m.in. zapewnienie możliwości lepszego reagowania na wyzwania stawiane przez szybki rozwój nowych technologii i postępującą globalizację, przy jednoczesnym zachowaniu technologicznej neutralności ram prawnych (por. A. Grzelak, *Główne cele ogólnego rozporządzenia o ochronie danych* [w:] *Ogólne rozporządzenie o ochronie danych osobowych. Wybrane zagadnienia*, red. M. Kawecki, T. Osiej, Warszawa 2017, s. 21).

11. Swobodny przepływ danych między państwami członkowskimi UE ma być możliwy dzięki zagwarantowaniu jednolitego i spójnego poziomu ochrony danych, któremu służyć ma m.in. ustalenie reguł dotyczących terytorialnego i podmiotowego zakresu stosowania rozporządzenia, określonych w art. 4 oraz rozbudowanych mechanizmów współpracy między organami nadzorczymi, uregulowanych w przepisach art. 60 i n. rozporządzenia.

Artykuł 2
Materialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.
2. Niniejsze rozporządzenie nie ma zastosowania do przetwarzania danych osobowych:
- **a) w ramach działalności nieobjętej zakresem prawa Unii;**
- **b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;**
- **c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;**
- **d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.**

3. Do przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne Unii zastosowanie ma rozporządzenie (WE) nr 45/2001. Rozporządzenie (WE) nr 45/2001 oraz inne unijne akty prawne mające zastosowanie do takiego przetwarzania danych osobowych zostają dostosowane do zasad i przepisów niniejszego rozporządzenia zgodnie z art. 98.
4. Niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy 2000/31/WE, w szczególności dla zasad odpowiedzialności usługodawców będących pośrednikami, o których to zasadach mowa w art. 12–15 tej dyrektywy.

1. Komentowany artykuł wyznacza zakres przedmiotowy rozporządzenia 2016/679, określa wyłączenia obowiązku jego stosowania, wskazuje przepisy właściwe dla przetwarzania danych przez instytucje, organy i jednostki organizacyjne UE, a także relacje rozporządzenia do przepisów dyrektywy o handlu elektronicznym.

2. Przepis art. 2 rozporządzenia stanowi odpowiednik art. 3 dyrektywy 95/46/WE. Zasadniczo zakres przedmiotowy obu regulacji jest tożsamy i obejmuje przetwarzanie danych osobowych w sposób zautomatyzowany oraz przetwarzanie danych w sposób inny niż zautomatyzowany w przypadku przetwarzania danych w zbiorze. Podobnie zostały również ukształtowane wyłączenia, przy czym w rozporządzeniu wyraźnie wskazano zakres regulacji poddanej odrębnym przepisom: dyrektywy 2016/680 (patrz art. 2 lit. d oraz motyw 19 komentowanego rozporządzenia), rozporządzenia (WE) nr 45/2001 (odesłanie to jest już nieaktualne, z uwagi na to, że wskazane rozporządzenie zostało zastąpione przez rozporządzenie 2018/1725, o czym szerzej będzie mowa poniżej), a także dyrektywy 2000/31/WE.

3. Przepisy rozporządzenia 2016/679 mają zastosowanie do przetwarzania danych osobowych, a więc do wykonywania na danych osobowych operacji, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie (szerzej na temat pojęcia przetwarzania i poszczególnych czynności, które mieszczą się w zakresie tego pojęcia, por. komentarz do art. 4).

Obowiązek stosowania komentowanego rozporządzenia wiąże się nie tylko z przetwarzaniem danych, ale także z zaistnieniem jednej z dwóch przesłanek wskazanych w komentowanym przepisie:

1) przetwarzanie danych osobowych odbywa się w sposób całkowicie lub częściowo zautomatyzowany albo
2) przetwarzanie odbywa się w sposób inny niż zautomatyzowany, a dane osobowe stanowią lub mają stanowić część zbioru danych.

Dla dokonania oceny, czy komentowane rozporządzenie znajduje zastosowanie, nie wystarczy zatem stwierdzić, czy ma miejsce przetwarzanie danych, ale trzeba jeszcze ocenić, czy przetwarzanie jest zautomatyzowane (tzn. jest dokonywane z wykorzystaniem środków służących do automatycznego przetwarzania danych – najczęściej komputerów), a jeżeli przetwarzanie nie ma takiego charakteru (tzn. jest dokonywane w sposób tradycyjny, ręcznie), to czy dane, które w taki sposób są przetwarzane, stanowią część zbioru danych albo mają stanowić zbiór (są gromadzone po to, aby zostały włączone do zbioru).

W motywie 15 preambuły wyjaśniono, że aby zapobiec poważnemu ryzyku obchodzenia prawa, ochrona osób fizycznych powinna być neutralna pod względem technicznym i nie powinna zależeć od stosowanych technik. Oznacza to, że objęcie zakresem przedmiotowym regulacji zarówno przetwarzania dokonywanego w sposób zautomatyzowany, jak też przetwarzania ręcznego dokonywanego w zbiorach danych ma pozwolić na zapobieganie próbom obchodzenia przepisów poprzez przenoszenie danych na nośniki papierowe.

4. Komentowane rozporządzenie nie definiuje pojęcia „przetwarzanie danych w sposób całkowicie lub częściowo zautomatyzowany". W piśmiennictwie przedmiotu przyjmuje się, że jest to zabieg świadomy związany z wolą zachowania neutralności technologicznej regulacji, co pociąga za sobą konieczność szerokiej wykładni tego pojęcia (por. D. Lubasz [w:] *RODO. Ogólne rozporządzenie o ochronie danych. Komentarz*, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, s. 126).

5. Przetwarzanie danych osobowych ma charakter zautomatyzowany w przypadku, gdy operacje na danych osobowych wykonywane są za pomocą urządzeń pozwalających na

automatyczne działanie (a więc wykonujących samoczynnie określone czynności bez konieczności wykonywania każdej czynności przez człowieka). Procesy przetwarzania danych osobowych realizowane są najczęściej za pomocą systemów informatycznych pozwalających zautomatyzować czynności, poprawić efektywność przetwarzania przy jednoczesnym zwiększeniu szybkości i obniżeniu kosztów wykonywania tego rodzaju działań. Jednak przetwarzanie danych w sposób zautomatyzowany może być dokonywane w różny sposób, przy wykorzystaniu rozmaitych narzędzi pozwalających na automatyzację procesów przetwarzania.

Typowym przykładem przetwarzania danych osobowych w sposób zautomatyzowany w systemie informatycznym jest przetwarzanie dokonywane w bazie danych, a więc programie komputerowym służącym przetwarzaniu danych. Ze zautomatyzowanym przetwarzaniem danych mamy do czynienia także w sytuacji, gdy wykorzystywane są do tego celu proste programy biurowe (edytory tekstu, arkusze kalkulacyjne).

Komentowany przepis nie wymaga, aby wszystkie czynności mieszczące się w zakresie przetwarzania realizowane były w sposób zautomatyzowany – wystarczy, że tylko niektóre operacje dokonywane będą w taki sposób, aby uznać, że przetwarzanie jest częściowo zautomatyzowane, co pociąga za sobą konieczność stosowania przepisów rozporządzenia.

W przypadku zautomatyzowanego przetwarzania danych kwestia, czy dane przetwarzane są w zbiorze danych czy też poza nim, nie jest istotna dla oceny obowiązku stosowania przepisów rozporządzenia. Jest to uzasadnione m.in. faktem, iż w rozległych sieciach teleinformatycznych trudno byłoby stwierdzić, czy w danym przypadku mamy do czynienia ze zbiorem danych, natomiast formuła zautomatyzowanego przetwarzania stwarza szerokie możliwości wykonywania operacji na danych osobowych, w tym ich szybkiego wyszukiwania.

6. Przetwarzanie danych osobowych w sposób niezautomatyzowany (komentowany przepis zawiera sformułowanie: „inny niż zautomatyzowany") ma miejsce w przypadku, gdy do przetwarzania danych nie są wykorzystywane (choćby częściowo) urządzenia służące automatyzacji, a procesy przetwarzania danych realizowane są metodami tradycyjnymi (poszczególne czynności składające się na przetwarzanie są wykonywane ręcznie). Z taką formą przetwarzania wiąże się stosowanie tradycyjnych nośników informacji – dane są zapisane zazwyczaj na papierze. W przypadku przetwarzania danych w sposób niezautomatyzowany komentowane rozporządzenie znajduje zastosowanie, gdy przetwarzane dane stanowią część zbioru danych lub mają stanowić część zbioru danych. Zbiorem danych w rozumieniu rozporządzenia jest uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie (szerzej na temat pojęcia „zbiór danych" por. komentarz

do art. 4). W motywie 15 preambuły stwierdzono, iż zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów, nie powinny być objęte zakresem rozporządzenia.

Prawodawca koncentruje się na procesach zautomatyzowanego przetwarzania danych osobowych z uwagi na to, że stanowią one dominującą metodę przetwarzania danych i z nimi wiążą się najpoważniejsze zagrożenia praw osób, których dane są przetwarzane. Jednakże całkowite pozostawienie poza obszarem regulacji niezautomatyzowanego przetwarzania danych prawodawca uznał za niecelowe, z uwagi na to, że tego rodzaju procesy nadal występują i również mogą pociągać za sobą istotne zagrożenia. Dlatego obowiązkiem stosowania rozporządzenia objęte zostały również tradycyjne procesy przetwarzania, pod warunkiem że przetwarzanie prowadzone jest w zbiorze danych lub dane osobowe mają stanowić część zbioru danych.

Użyte w komentowanym przepisie określenie „dane stanowią część zbioru danych lub mają stanowić część zbioru danych" oznacza, że obowiązek stosowania przepisów rozporządzenia dotyczy nie tylko danych, które już są częścią zbioru (zostały do zbioru włączone i są przetwarzane w zbiorze), ale także danych, które są gromadzone po to, aby je do zbioru włączyć. Istotny więc jest zamiar, który towarzyszy zbieraniu danych.

Typowym przykładem przetwarzania danych osobowych w sposób niezautomatyzowany jest przetwarzanie dokonywane manualnie w papierowych ewidencjach, kartotekach, skorowidzach czy też innych tego rodzaju tradycyjnych zbiorach danych.

Szerzej na temat pojęcia przetwarzania por. komentarz do art. 4.

7. Z komentowanego przepisu wynika, że przetwarzanie danych, które odbywa się w sposób niezautomatyzowany (ręcznie), a przetwarzane dane nie stanowią (lub nie mają stanowić) zbioru, nie jest objęte zakresem przedmiotowym, a zatem w tym przypadku komentowane rozporządzenie nie znajduje zastosowania. Dotyczy to przede wszystkim tzw. tekstów potoczystych, które nie stanowią zbiorów danych w rozumieniu komentowanego rozporządzenia (np. książki lub artykuły prasowe w postaci ciągłego, zwartego tekstu), czy też pojedynczych informacji, które nie są gromadzone w celu utworzenia zbioru bądź włączenia do istniejącego już zbioru.

8. Zakres przedmiotowy komentowanego rozporządzenia jest zbliżony do zakresu przedmiotowego dotychczasowej krajowej regulacji – określonego w art. 2 u.o.d.o.1997. Prawodawca polski w art. 2 ust. 1 u.o.d.o.1997 posłużył się sformułowaniem „dane osobowe są lub mogą być przetwarzane w zbiorach danych", natomiast w ust. 2 wskazał dwie postaci przetwarzania danych: niezautomatyzowaną (w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych) oraz zautomatyzowaną

(w systemach informatycznych), podkreślając, iż w tym drugim przypadku ustawa ma zastosowanie także do przetwarzania danych poza zbiorem danych.

Można uznać, że wskazany powyżej zakres przedmiotowy rozporządzenia 2016/679 i u.o.d.o.1997 jest zbliżony. Należy jednak podkreślić, że rozporządzenie unijne nie przewiduje wyłączenia (ani też ograniczenia) stosowania przepisów do tzw. zbiorów doraźnych, które przewidziane było w polskiej ustawie.

Zgodnie z art. 2 ust. 3 u.o.d.o.1997 do zbiorów danych osobowych sporządzanych doraźnie, wyłącznie ze względów technicznych, szkoleniowych lub w związku z dydaktyką w szkołach wyższych, a po ich wykorzystaniu niezwłocznie usuwanych albo poddanych anonimizacji, miały zastosowanie jedynie przepisy rozdziału 5, dotyczące zabezpieczenia danych. Tego rodzaju ograniczenie stosowania przepisów u.o.d.o.1997 miało jednak stosunkowo niewielkie znaczenie praktyczne ze względu na konieczność kumulatywnego spełnienia wskazanych w przepisie przesłanek (co np. w administracji publicznej zwykle nie było możliwe z racji konieczności przechowywania danych po ich wykorzystaniu w celach archiwalnych). Prawodawca unijny nie przewidział w komentowanym rozporządzeniu tego rodzaju konstrukcji prawnej, co oznacza, że doraźność (krótkotrwały charakter przetwarzania połączony z realizacją specyficznych celów) nie zwalnia z obowiązku stosowania przepisów o ochronie danych osobowych.

Prawodawca unijny, określając zakres przedmiotowy, nie posłużył się odniesieniem do systemów informatycznych, jak uczynił to wcześniej prawodawca krajowy. W komentowanym artykule mowa o przetwarzaniu danych w sposób zautomatyzowany, co należy uznać za określenie znacznie bardziej pojemne i neutralne technologicznie. Z uwagi na konwergencję informatyki, telekomunikacji i mediów oraz konsekwencje wynikające z tego procesu, takie podejście wydaje się uzasadnione. Ocena, czy w konkretnym przypadku mamy do czynienia z systemem informatycznym, może pociągać za sobą wątpliwości, podczas gdy znacznie łatwiej można stwierdzić, czy mamy do czynienia z przetwarzaniem danych w sposób całkowicie lub choćby częściowo zautomatyzowany.

9. Na kanwie komentowanego przepisu może pojawić się wątpliwość dotycząca obowiązku stosowania przepisów na etapie gromadzenia danych, w sytuacji gdy zbieranie danych nie jest realizowane w sposób zautomatyzowany, a dane nie znalazły się jeszcze w zbiorze danych. Literalna wykładnia przepisu mogłaby sugerować, że na wskazanym powyżej etapie przetwarzania rozporządzenie nie znajduje zastosowania. Jednak taka interpretacja nie wydaje się prawidłowa z uwagi na to, że prawodawca unijny nakazuje objęcie ochroną nie tylko danych stanowiących część zbioru, ale także danych mających stanowić część zbioru, tzn. gromadzonych z zamiarem włączenia tych danych do zbioru (ang. *are intended to form part of a filing system*). Podobną wykładnię przyjmowano także na gruncie u.o.d.o.1997 (por. A. Mednis, *Ustawa o ochronie danych osobowych. Komentarz*, Warszawa 1999, s. 15).

Dla obowiązku stosowania rozporządzenia nie jest konieczne, aby wszystkie czynności przetwarzania dokonywane były w sposób zautomatyzowany, wystarczy, że tylko niektóre z nich są zautomatyzowane, a inne (np. gromadzenie) nie muszą być realizowane w taki sposób, mogą być wykonywane ręcznie. W tym zakresie częściowo nadal aktualne wydaje się być stanowisko wyrażone w postanowieniu SN z 11.12.2000 r. (II KKN 438/00, OSNKW 2001/3–4, poz. 33), wydanym na gruncie u.o.d.o.1997, zgodnie z którym każdy ma prawo do ochrony dotyczących go danych osobowych, a nie jedynie ten, czyje dane znalazły się już w zbiorze. Stanowisko takie jest prezentowane także w najnowszym piśmiennictwie przedmiotu odnoszącym się do komentowanego rozporządzenia (por. P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych. Komentarz*, red. P. Litwiński, Warszawa 2018, s. 141).

10. W ust. 2 komentowanego artykułu określone zostały cztery grupy wyłączeń stosowania rozporządzenia. Jeżeli przetwarzanie danych dokonywane jest w ramach jednego ze wskazanych tu zakresów, to rozporządzenie 2016/679 nie znajduje w tym przypadku zastosowania, gdyż albo procesy te nie są poddane regulacji prawnej, albo są objęte innymi regulacjami.

11. Pierwszym z wyłączeń stosowania rozporządzenia 2016/679, określonym w ust. 2 lit. a komentowanego przepisu, jest przetwarzanie danych osobowych w ramach działalności nieobjętej zakresem prawa UE. Chodzi tu o szeroko pojęte działania, odnoszące się do bezpieczeństwa narodowego.

Wyłączenie stosowania przepisów o ochronie danych osobowych (u.o.d.o.2018 i rozporządzenia 2016/679), odnoszące się do bezpieczeństwa narodowego, przewidziane zostało również w art. 6 u.o.d.o.2018. Dotyczy ono: 1) przetwarzania danych osobowych przez jednostki sektora finansów publicznych, w zakresie, w jakim przetwarzanie to jest konieczne do realizacji zadań mających na celu zapewnienie bezpieczeństwa narodowego, jeżeli przepisy szczególne przewidują niezbędne środki ochrony praw i wolności osoby, której dane dotyczą; 2) działalności służb specjalnych. Szerzej na temat tego wyłączenia por. komentarz do art. 6 u.o.d.o.2018.

12. Drugie z wyłączeń stosowania rozporządzenia 2016/679, wskazane w ust. 2 lit. b komentowanego artykułu, dotyczy przetwarzania danych osobowych przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE, a więc działań dotyczących wspólnej polityki zagranicznej i bezpieczeństwa UE.

13. Trzecie wyłączenie, ustanowione w ust. 2 lit. c komentowanego przepisu, dotyczy przetwarzania danych osobowych przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze. W motywie 18 preambuły wyjaśniono, że chodzi

o aktywność prowadzoną „bez związku z działalnością zawodową lub handlową". Dalej wyjaśniono, że „działalność osobista lub domowa może między innymi polegać na korespondencji i przechowywaniu adresów, podtrzymywaniu więzi społecznych oraz działalności internetowej podejmowanej w ramach takiej działalności. Niniejsze rozporządzenie ma jednak zastosowanie do administratorów lub podmiotów przetwarzających, którzy udostępniają środki przetwarzania danych osobowych na potrzeby takiej działalności osobistej lub domowej". W oparciu o komentowany przepis uzupełniony wyjaśnieniem zawartym w preambule można przyjąć, że aktywność osób fizycznych na portalach społecznościowych (niemająca związku z działalnością zawodową lub handlową) zasadniczo będzie mieścić się w ramach wyłączenia stosowania rozporządzenia, natomiast dostawcy usług internetowych poddani zostali obowiązkowi stosowania przepisów o ochronie danych osobowych.

Wskazane wyłączenie stosowania rozporządzenia stanowi odpowiednik wyłączenia przewidzianego w art. 3a ust. 1 pkt 1 u.o.d.o.1997, na mocy którego przepisy u.o.d.o.1997 nie miały zastosowania do osób fizycznych, które przetwarzały dane wyłącznie w celach osobistych lub domowych. Jako przykłady tego rodzaju przetwarzania wskazuje się zazwyczaj przetwarzanie danych w prywatnych notatnikach teleadresowych, prywatnych komputerach czy innych prywatnych urządzeniach umożliwiających zautomatyzowane przetwarzanie danych (np. smartfonach, tabletach). Coraz częściej jednak dane nie są przechowywane na nośniku pozostającym w dyspozycji podmiotu danych, a są umieszczane na serwerach w sieci (w tzw. chmurze obliczeniowej), co zasadniczo nie wyklucza możliwości uznania tego rodzaju czynności za mające charakter osobisty lub domowy.

Przy zestawieniu brzmienia dotychczasowych krajowych przepisów z brzmieniem komentowanego przepisu rozporządzenia może pojawić się wątpliwość, czy użyte tam określenia są tożsame. W art. 3a ust. 1 pkt 1 u.o.d.o.1997 prawodawca posłużył się określeniem „w celach osobistych lub domowych", natomiast w art. 2 ust. 2 lit. c komentowanego rozporządzenia użyte zostało sformułowanie „w ramach czynności o czysto osobistym lub domowym charakterze". Wskazana różnica polega na nieco innym ujęciu – w krajowych przepisach akcentowano cele przetwarzania, natomiast w przepisach unijnych akcentuje się charakter czynności przetwarzania.

Zawarte w komentowanym przepisie zastrzeżenie, zgodnie z którym z omawianego wyłączenia mogą skorzystać jedynie osoby fizyczne, podobnie do rozwiązania zawartego w u.o.d.o.1997, wyklucza możliwość skutecznego powoływania się na to wyłączenie przez przedsiębiorców, spółki czy też inne jednostki organizacyjne (stowarzyszenia, fundacje), nawet jeżeli skala przetwarzania danych osobowych przez te podmioty jest niewielka, a charakter przetwarzania niekomercyjny. Określenie czynności o czysto osobistym lub domowym charakterze nie może być odnoszone do podmiotów innych niż osoby fizyczne.

14. W praktyce ocena, czy w danym przypadku przetwarzanie danych osobowych ma miejsce w ramach czynności o czysto osobistym lub domowym charakterze, może budzić wątpliwości. W tym kontekście można wspomnieć o wyroku TSUE z 11.12.2014 r., C-212/13, František Ryneš v. Úřad pro ochranu osobních údajů (LEX nr 1551850), wydanym jeszcze na gruncie dyrektywy 95/46/WE, w którym Trybunał uznał, że wykorzystywanie systemu kamer zainstalowanego przez osobę fizyczną na jej domu rodzinnym, monitorującego również przestrzeń publiczną, nie stanowi przetwarzania danych w trakcie czynności o czysto osobistym lub domowym charakterze. Orzeczenie to spotkało się z krytyką w piśmiennictwie przedmiotu (por. krytyczną glosę M. Czerniawskiego do wyroku TSUE z 11.12.2014 r., C-212/13, LEX 2015).

Inna sytuacja faktyczna, która budzi wątpliwości, gdy chodzi o możliwość uznania za działania w ramach czynności o czysto osobistym lub domowym charakterze, dotyczy publikowania danych na stronach internetowych (w tym w serwisach społecznościowych). W opinii przyjętej jeszcze na gruncie dyrektywy 95/46/WE Grupa Robocza Art. 29 uznała, że przetwarzanie danych przez użytkowników w portalach społecznościowych mieści się – co do zasady – w zakresie czynności osobistych lub domowych, chyba że dostęp do tych danych mają inne osoby niż te, które zostały wybrane samodzielnie przez użytkownika, np. poprzez dodanie do kontaktów (por. *Opinia 5/2009 Grupy Roboczej Art. 29 w sprawie portali społecznościowych*, przyjęta 12.06.2009 r., WP 163).

15. Czynności o „czysto osobistym lub domowym charakterze" są przeciwieństwem czynności o charakterze zawodowym lub aktywności gospodarczej (działalność profesjonalna). Jednak osobistego lub domowego charakteru nie wykazują również formy aktywności, które nie mają wymiaru zawodowego, a przybierają wymiar społeczny; nie mają charakteru działalności gospodarczej, a działalności *non profit;* podobnie mogą one nie mieć charakteru profesjonalnego, a amatorski (np. aktywność osoby fizycznej w stowarzyszeniu, fundacji itp.). W tym zakresie powoływanie się na omawiane wyłączenie nie jest zasadne.

16. Istotną kwestią w kontekście omawianego wyłączenia jest także problem osiągania dochodów (zarobkowego charakteru) działalności. Za prawidłowe należy uznać stanowisko, zgodnie z którym osiąganie dochodów z działalności nie stoi w sprzeczności z czysto osobistym lub domowym charakterem wykonywanych czynności, o ile czynności te nie są wykonywane zawodowo lub w ramach działalności gospodarczej albo innego rodzaju zorganizowanej działalności (np. społecznej). Przykładem tego rodzaju działań może być sprzedaż przedmiotów z kolekcji, którą osoba fizyczna zgromadziła w ramach pasji kolekcjonerskiej. Podobne stanowisko w tej kwestii prezentują P. Litwiński, P. Barta, M. Kawecki, *Rozporządzenie UE w sprawie ochrony...*, red. P. Litwiński, s. 150, którzy jako przykład tego rodzaju sytuacji wskazują incydentalną sprzedaż własnego samochodu za pośrednictwem dedykowanych serwisów internetowych.

Odmienne stanowisko w tej kwestii prezentuje D. Lubasz, którego zdaniem wskazanie na osobisty lub domowy charakter przetwarzania co do zasady wyklucza możliwość objęcia omawianym wyłączeniem takiego przetwarzania, które choćby pośrednio przynosi korzyści majątkowe (por. D. Lubasz [w:] *RODO. Ogólne rozporządzenie...*, red. E. Bielak-Jomaa, D. Lubasz, s. 138).

17. W komentowanym przepisie rozporządzenia brak wyłączenia stanowiącego odpowiednik wyjątku, o którym była mowa w art. 3a ust. 1 pkt 2 u.o.d.o.1997, dotyczącego tranzytu danych (odnoszącego się do podmiotów z państw trzecich wykorzystujących środki techniczne znajdujące się na terytorium RP wyłącznie do przekazywania danych). Tego rodzaju wyłączenie nie jest już konieczne ze względu na to, że zakres podmiotowy rozporządzenia został ukształtowany odmiennie i zasadniczo nie obejmuje procesów ograniczających się do samego tranzytowego przesyłania danych.

18. W polskiej ustawie przewidziane było ponadto wyłączenie (ograniczenie) stosowania przepisów o ochronie danych osobowych dotyczące działalności dziennikarskiej, literackiej i artystycznej. Komentowane rozporządzenie nie wprowadza ogólnego wyłączenia ani też ograniczenia w tym zakresie, pozostawiając te kwestie do regulacji prawodawcy krajowemu (szerzej na ten temat por. komentarz do art. 85).

19. Czwarte z wyłączeń, uregulowane w ust. 2 lit. d komentowanego artykułu, odnosi się do przetwarzania danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Wyłączenie to jest naturalną konsekwencją poddania wskazanej materii odrębnej regulacji prawnej, zawartej w dyrektywie Parlamentu Europejskiego i Rady (UE) 2016/680 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (tzw. dyrektywie policyjnej).

Dyrektywa policyjna wymagała implementacji do prawa krajowego poszczególnych państw członkowskich UE. W Polsce implementacja wskazanej dyrektywy została dokonana ustawą z 14.12.2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (Dz.U. z 2019 r. poz. 125), która weszła w życie 6.02.2019 r. W okresie od dnia rozpoczęcia stosowania komentowanego rozporządzenia, do wejścia w życie ustawy implementującej tzw. dyrektywę policyjną – u.o.d.o.p. w zakresie przetwarzania danych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar zastosowanie miały wybrane przepisy u.o.d.o.1997 (szerzej

na ten temat por. komentarz do art. 175 u.o.d.o.2018). Problematyka przetwarzania i ochrony danych osobowych do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar została uregulowana w ustawie o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości inaczej niż w ogólnych przepisach rozporządzenia 2016/679 i u.o.d.o.2018. Ze względu na specyfikę tej dziedziny i odmienne ukształtowanie wielu mechanizmów prawnych nie zostanie ona omówiona w niniejszym komentarzu. Problematyka ta jest przedmiotem wielu opracowań szczegółowych (por. m.in. *Ochrona danych osobowych w sądach i prokuraturze,* red. A. Grzelak, Warszawa 2019; *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz,* red. A. Grzelak, Warszawa 2019; M. Kusak, P. Wiliński, *Ochrona danych osobowych w ściganiu przestępstw. Standardy krajowe i unijne,* Warszawa 2020 i wskazaną tam literaturę).

20. Ustęp 3 komentowanego przepisu dotyczy przetwarzania danych osobowych przez instytucje, organy i jednostki organizacyjne UE. W tym zakresie rozporządzenie nie znajduje zastosowania, ponieważ materia ta jest uregulowana odrębnie. Komentowany przepis zawiera odesłanie do rozporządzenia (WE) nr 45/2001 Parlamentu Europejskiego i Rady z 18.12.2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych (Dz.Urz. UE L 8 z 2001 r., s. 1, Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 26, s. 102). Jednak odesłanie to nie jest już aktualne, ponieważ wskazany akt normatywny utracił moc obowiązującą wskutek uchwalenia rozporządzenia Parlamentu Europejskiego i Rady 2018/1725 z 23.10.2018 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje, organy i jednostki organizacyjne Unii i swobodnego przepływu takich danych oraz uchylenia rozporządzenia (WE) nr 45/2001 i decyzji nr 1247/2002/WE (Dz.Urz. UE L 295, s. 39 i n.).

Wskazane w komentowanym przepisie akty normatywne zostały wydane w oparciu o przepisy dyrektywy 95/46/WE i ich treść w pierwotnym kształcie istotnie odbiegała od rozwiązań przyjętych w rozporządzeniu 2016/679. Dlatego też, aby zapewnić jednolitość i spójność regulacji odnoszących się do ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, konieczne było dokonanie zmian. Komentowany przepis nakłada obowiązek dostosowania treści tych aktów normatywnych do zasad i przepisów ogólnego rozporządzenia o ochronie danych zgodnie z art. 98. W myśl tego przepisu kompetencję do przedłożenia wniosków ustawodawczych dotyczących zmiany innych aktów prawnych UE dotyczących ochrony danych osobowych posiada Komisja Europejska.

21. Ustęp 4 komentowanego przepisu stanowi, iż rozporządzenie pozostaje bez uszczerbku dla stosowania dyrektywy o handlu elektronicznym – tj. dyrektywy 2000/31/WE

Parlamentu Europejskiego i Rady z 8.06.2000 r. w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) (Dz.Urz. WE L 178, s. 1; Dz.Urz. UE Polskie wydanie specjalne, rozdz. 13, t. 25, s. 399), w szczególności dla określonych w tej dyrektywie zasad odpowiedzialności usługodawców będących pośrednikami (art. 12–15 dyrektywy o handlu elektronicznym). Wskazane przepisy przewidują wyłączenia odpowiedzialności dostawców usług będących pośrednikami w przypadku usług: prostego przekazu danych (ang. *mere conduit*), krótkotrwałego przechowywania danych w celu przyspieszenia transmisji (ang. *caching*) oraz udostępniania zasobów systemu teleinformatycznego w celu przechowywania i udostępniania danych (ang. *hosting*). Również przepisy dyrektywy o handlu elektronicznym powinny zostać dostosowane do wymogów określonych w rozporządzeniu 2016/679.

Artykuł 3
Terytorialny zakres stosowania

1. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy przetwarzanie odbywa się w Unii.
2. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w Unii, jeżeli czynności przetwarzania wiążą się z:
a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.
3. Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych przez administratora niemającego jednostki organizacyjnej w Unii, ale posiadającego jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego.

1. Komentowany artykuł określa terytorialny i podmiotowy zakres stosowania rozporządzenia 2016/679. W ust. 1 wskazana została ogólna reguła, natomiast w ust. 2 i 3 unormowano wyjątki od reguły ogólnej.

2. Przepis art. 3 rozporządzenia jest odpowiednikiem art. 4 dyrektywy 95/46/WE, określającego terytorialny zakres stosowania (odpowiednie prawo krajowe). Między tymi przepisami dostrzec można kilka istotnych różnic.

Po pierwsze, rozporządzenie ma być stosowane wprost, dlatego zasadniczo nie odsyła do prawa krajowego, natomiast dyrektywa 95/46/WE stanowiła akt normatywny

wymagający implementacji, stąd zawiera odniesienia do przepisów obowiązujących w poszczególnych państwach członkowskich.

Po drugie, art. 4 dyrektywy 95/46/WE nie tylko wskazuje, kiedy przepisy o ochronie danych osobowych będą miały zastosowanie, ale rozstrzyga także o tym, które przepisy (przepisy którego z państw) powinny być stosowane, natomiast art. 3 rozporządzenia reguluje zakres terytorialny, a zarazem podmiotowy stosowania tego aktu normatywnego.

Kolejna różnica odnosi się do obszaru oddziaływania obu regulacji: zakres obowiązywania dyrektywy 95/46/WE był ograniczony do obszaru państw członkowskich UE, a podmioty spoza UE miały stosować dyrektywę, jeżeli przetwarzały dane z wykorzystaniem środków znajdujących się na terytorium państwa członkowskiego, natomiast zakres stosowania rozporządzenia został rozszerzony także na podmioty niemające jednostek organizacyjnych w Unii, ale przetwarzające dane osobowe osób przebywających w Unii, jeżeli przetwarzanie jest związane z oferowaniem towarów lub usług takim osobom lub monitorowaniem ich zachowania, bez względu na to, czy działania te są realizowane przy wykorzystaniu środków technicznych zlokalizowanych w UE.

3. Ogólną regułą przyjętą w rozporządzeniu 2016/679 jest stosowanie przepisów rozporządzenia do przetwarzania danych osobowych mającego związek z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w UE, przy czym prawnej doniosłości nie ma okoliczność, czy przetwarzanie danych odbywa się na obszarze UE, czy też poza nim (istotne jest, gdzie administrator bądź podmiot przetwarzający prowadzi działalność, a nie to, gdzie faktycznie prowadzone są procesy i zlokalizowane są środki przetwarzania danych).

Pośrednio komentowany przepis odnosi się także do zakresu podmiotowego regulacji. Prawodawca unijny nakazuje stosować przepisy komentowanego rozporządzenia zarówno administratorom (podmiotom, które ustalają cele i sposoby przetwarzania danych osobowych; szerzej na temat pojęcia „administrator" por. komentarz do art. 4), jak i podmiotom przetwarzającym (podmiotom, które przetwarzają dane osobowe w imieniu administratora; szerzej na temat pojęcia „podmiot przetwarzający" por. komentarz do art. 4) w przypadku, gdy przetwarzanie przez nich danych osobowych następuje w związku z działalnością ich jednostek organizacyjnych prowadzoną w UE.

Kluczowe znaczenie dla określenia zakresu podmiotowego komentowanego rozporządzenia ma pojęcie jednostki organizacyjnej. Określenie to nie zostało zdefiniowane w rozporządzeniu, jednakże w motywie 22 preambuły wyjaśniono, że pojęcie jednostki organizacyjnej zakłada skuteczne i faktyczne prowadzenie działalności poprzez stabilne struktury, przy czym forma prawna takich struktur nie jest istotna (nie ma zasadniczo znaczenia, czy chodzi o oddział, czy spółkę zależną posiadającą osobowość

prawną). Szerzej na temat pojęcia jednostki organizacyjnej por. komentarz do art. 4, odnoszący się do definicji „główna jednostka organizacyjna".

Dotyczy to zarówno podmiotów publicznych (m.in. administracji publicznej), jak też podmiotów prywatnych (np. spółek), przy czym podział na te dwie kategorie podmiotów nie został wyraźnie w komentowanym przepisie wskazany, odmiennie niż w art. 3 u.o.d.o.1997. Podział ten ma jednak istotne znaczenie w kontekście innych przepisów rozporządzenia (np. gdy chodzi o administracyjne kary pieniężne – por. komentarz do art. 83 rozporządzenia). W odniesieniu do sfery publicznej wskazanie jednostki organizacyjnej zasadniczo nie powinno nastręczać trudności, gdyż podmioty te mają siedzibę na obszarze naszego kraju. Znacznie bardziej skomplikowane struktury i zależności występują w sektorze prywatnym, stąd ustalenie jednostki organizacyjnej będzie miało tu istotne znaczenie.

Prawodawca unijny posłużył się określeniem „*establishment*", które w polskim tekście rozporządzenia nie zostało przetłumaczone jako siedziba, a jako jednostka organizacyjna. Takie ujęcie w zamierzeniu osób odpowiedzialnych za polski przekład tekstu rozporządzenia ma lepiej oddawać sens konstrukcji prawnej wykorzystanej w komentowanym przepisie i usuwać wątpliwości dotyczące m.in. oddziałów i przedstawicielstw przedsiębiorców.

Na tym tle uwidacznia się różnica w ujęciu prawnym zawartym w poprzedniej krajowej regulacji, a prezentowanym w komentowanym rozporządzeniu. Prawodawca polski w art. 3 ust. 2 u.o.d.o.1997 wiązał obowiązek stosowania przepisów o ochronie danych osobowych z faktem przetwarzania danych osobowych przez podmioty mające siedzibę na terytorium RP lub wykorzystujące środki techniczne znajdujące się na terytorium RP, w przypadku gdy podmioty te miały siedzibę w państwie trzecim. Przepis art. 3 rozporządzenia odmiennie kształtuje zakres terytorialny i podmiotowy regulacji. Na temat różnic między dotychczasowym a nowym stanem prawnym w omawianym zakresie por. M. Czerniawski, *Aktualny i projektowany zakres terytorialny unijnych przepisów o ochronie danych osobowych,* EPS 2015/5, s. 4–9.

4. Komentowany przepis wiąże obowiązek stosowania przepisów rozporządzenia z przetwarzaniem danych „mającym związek z działalnością". Oznacza to, że przetwarzanie danych osobowych może, ale nie musi być podstawową formą aktywności administratora – głównym przedmiotem jego działalności. W praktyce najczęściej przetwarzanie danych towarzyszy innym działaniom, których realizację umożliwia (np. pracodawca przetwarza dane swoich pracowników). Z odmienną sytuacją mamy do czynienia zazwyczaj w przypadku podmiotu przetwarzającego, którego aktywność koncentruje się na procesach przetwarzania danych na zlecenie administratora, choć i w odniesieniu do tego podmiotu mogą wystąpić sytuacje, gdy głównym przedmiotem jego aktywności są inne działania, którym przetwarzanie danych osobowych jedynie towarzyszy (np. z serwisowaniem sprzętu komputerowego zwykle wiąże się dostęp do danych osobowych).

5. Dla obowiązku stosowania rozporządzenia istotne jest prowadzenie działalności w UE, co nie musi oznaczać przetwarzania danych w UE. W praktyce coraz częściej zdarza się, że podmiot, który prowadzi działalność w określonym miejscu, dokonuje przetwarzania danych osobowych w innym miejscu (zwykle wykorzystując do tego możliwości, jakie dają sieci teleinformatyczne). Fakt przetwarzania danych w innym miejscu niż miejsce prowadzenia działalności przez jednostkę organizacyjną w UE nie zwalnia z obowiązku stosowania przepisów rozporządzenia.

6. Ustęp 2 komentowanego przepisu rozciąga obowiązek stosowania rozporządzenia na podmioty (administratorów oraz podmioty przetwarzające), które nie mają jednostek organizacyjnych w Unii Europejskiej, a przetwarzają dane osób przebywających w UE, pod warunkiem spełnienia jednej z dwóch następujących przesłanek:

1) czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii – niezależnie od tego, czy wymaga się od tych osób zapłaty; lub
2) czynności przetwarzania wiążą się z monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

Do tego rodzaju działań dochodzi zwykle z wykorzystaniem sieci teleinformatycznych (najczęściej sieci Internet). Jak wyjaśniono w motywie 23 preambuły, nałożenie na podmioty spoza UE obowiązku stosowania przepisów ma zapewnić, że osoby fizyczne, przebywające w UE, nie zostaną pozbawione ochrony przysługującej im na mocy rozporządzenia.

7. W piśmiennictwie przedmiotu przyjętą przez prawodawcę unijnego konstrukcję określa się jako koncepcję „nakierowania" (szerzej na ten temat por. M. Czerniawski, *Zakres terytorialny a pojęcie „jednostki organizacyjnej" w przepisach ogólnego rozporządzenia o ochronie danych – zarys problemu* [w:] *Ogólne rozporządzenie o ochronie danych. Aktualne problemy prawnej ochrony danych osobowych 2016*, red. G. Sibiga, Warszawa 2016, s. 22–28 i wskazaną tam literaturę).

8. W świetle motywu 23 preambuły, w celu stwierdzenia, czy pierwsza z przesłanek (oferowanie towarów lub usług osobom przebywającym w UE) została spełniona, należy ustalić, czy administrator lub podmiot przetwarzający planują oferować usługi osobom, których dane dotyczą, w co najmniej jednym państwie członkowskim UE, przy czym nie wystarczy sama dostępność w UE strony internetowej administratora, podmiotu przetwarzającego, pośrednika, adresu poczty elektronicznej lub innych danych kontaktowych (gdyż większość stron internetowych dostępna jest globalnie, a dane kontaktowe są również z reguły powszechnie dostępne), ani posługiwanie się językiem powszechnie stosowanym w państwie trzecim, w którym jednostkę organizacyjną ma administrator (np. językiem angielskim). Zgodnie ze wskazaniem zawartym w powołanym wyżej motywie preambuły, potwierdzeniem oczywistości faktu, że administrator planuje oferować w UE towary lub usługi osobom, których dane dotyczą, mogą być czynniki

takie jak: posługiwanie się językiem lub walutą powszechnie stosowanymi w co najmniej jednym państwie członkowskim oraz możliwość zamówienia towarów i usług w tym języku lub wzmianka o klientach lub użytkownikach znajdujących się w UE.

9. Warto podkreślić, że dla obowiązku stosowania przepisów rozporządzenia nie ma znaczenia to, czy za oferowane towary lub usługi wymagana jest zapłata. W praktyce wiele tzw. usług społeczeństwa informacyjnego (usług świadczonych drogą elektroniczną) oferowanych jest bez konieczności ponoszenia finansowego ciężaru związanego z korzystaniem z usługi (usługi te określa się często mianem „darmowych", np. darmowa poczta elektroniczna). Jednakże typowym rozwiązaniem jest finansowanie świadczenia tego rodzaju usług z zysków osiąganych dzięki działaniom marketingowym realizowanym w oparciu o dane osobowe usługobiorców, na podstawie wyrażanej przez te osoby zgody na przetwarzanie ich danych.

10. Drugą z przesłanek, której spełnienie również pociąga za sobą obowiązek stosowania przepisów komentowanego rozporządzenia przez podmioty niemające jednostki organizacyjnej w UE, jest przetwarzanie danych osób przebywających w UE związane z monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w UE. W motywie 24 preambuły wyjaśniono, że czynności przetwarzania można uznać za monitorowanie zachowania osób, których dane dotyczą, gdy osoby są obserwowane w Internecie, a zgromadzone dane osobowe są wykorzystywane do profilowania, w szczególności w celu podjęcia decyzji albo przeanalizowania lub prognozowania osobistych preferencji, zachowań i postaw.

Pojęcie profilowania zostało zdefiniowane w art. 4 pkt 4 rozporządzenia i oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się (szerzej na temat profilowania por. uwagi zawarte w komentarzu do art. 4).

11. Przyjęcie omówionej powyżej konstrukcji prawnej oznacza, że prawodawca unijny rozszerzył obowiązek stosowania komentowanego rozporządzenia na podmioty spoza UE. Takie rozwiązanie prawne nasuwa wątpliwości, gdy chodzi o jego skuteczność i możliwość egzekwowania.

12. Ustęp 3 komentowanego przepisu nakazuje stosować rozporządzenie w przypadku przetwarzania danych przez administratora, który nie ma jednostki organizacyjnej w Unii, ale posiada jednostkę organizacyjną w miejscu, w którym na mocy prawa międzynarodowego publicznego ma zastosowanie prawo państwa członkowskiego. W motywie 25 preambuły jako przykład tego rodzaju miejsc wskazano teren misji dyploma-