KOMISJA
EUROPEJSKA

Bruksela, dnia 29.5.2019 r.
COM(2019) 250 final

KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Wytyczne dotyczące rozporządzenia w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej

Spis treści

Niniejszy dokument został przygotowany przez Komisję Europejską wyłącznie do celów informacyjnych. Nie zawiera on żadnej oficjalnej interpretacji rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej ani nie stanowi decyzji lub stanowiska Komisji Europejskiej. Pozostaje on bez uszczerbku dla wszelkich tego typu decyzji lub stanowisk Komisji Europejskiej i uprawnień Trybunału Sprawiedliwości Unii Europejskiej do interpretowania rozporządzenia zgodnie z traktatami UE.

1 Wprowadzenie

W gospodarce, która jest w coraz większym stopniu oparta na danych, przepływy danych znajdują się w centrum procesów biznesowych w przedsiębiorstwach różnej wielkości i we wszystkich branżach. Nowe technologie cyfrowe otwierają nowe możliwości dla ogółu społeczeństwa, przedsiębiorstw i organów administracji publicznej w Unii Europejskiej („UE").

W celu dalszego zwiększania transgranicznej wymiany danych i pobudzenia gospodarki opartej na danych w listopadzie 2018 r. Parlament Europejski i Rada przyjęły rozporządzenie (UE) 2018/1807 w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej[1] („rozporządzenie w sprawie swobodnego przepływu danych nieosobowych") na podstawie wniosku Komisji Europejskiej („Komisja"). Rozporządzenie stosuje się od dnia 28 maja 2019 r. Zasadę swobodnego przepływu danych osobowych określono w rozporządzeniu (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („ogólne rozporządzenie o ochronie danych")[2]. W związku z tym istnieją obecnie kompleksowe ramy wspólnej europejskiej przestrzeni danych i swobodnego przepływu wszystkich danych w Unii Europejskiej[3].

Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych daje przedsiębiorstwom pewność prawa w kwestii przetwarzania ich danych w dowolnym miejscu w UE, zwiększa zaufanie do usług w zakresie przetwarzania danych i przeciwdziała uzależnieniu od jednego dostawcy. Zwiększy to możliwości wyboru dla klientów, poprawi wydajność i zachęci do stosowania technologii chmury, co przyniesie przedsiębiorstwom w UE znaczne oszczędności. Jedno z badań pokazuje, że przedsiębiorstwa w UE mogą zaoszczędzić 20-50 % kosztów IT, przenosząc dane do chmury[4].

Dzięki tym dwóm rozporządzeniom dane mogą swobodnie przepływać między państwami członkowskimi, co umożliwia użytkownikom usług przetwarzania danych korzystanie z danych zgromadzonych na różnych rynkach UE w celu zwiększenia ich wydajności i konkurencyjności. Użytkownicy mogą w związku z tym w pełni skorzystać z korzyści skali zapewnianych przez duży rynek UE, poprawiając swoją konkurencyjność w skali światowej oraz zwiększając wzajemne powiązania w ramach europejskiej gospodarki opartej na danych.

---

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej, Dz.U. L 303 z 28.11.2018, s. 59.

[2] 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), Dz.U. L 119 z 4.5.2016, s. 1.

[3] Ogólne rozporządzenie o ochronie danych ma również zastosowanie do Europejskiego Obszaru Gospodarczego (EOG) obejmującego Islandię, Liechtenstein i Norwegię. Podobnie rozporządzenie w sprawie swobodnego przepływu danych nieosobowych zostało oznaczone jako mające znaczenie dla EOG.

[4] Deloitte: *Measuring the economic impact of cloud computing in Europe*, SMART 2014/0031, 2016 r. Dostępne w internecie pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=41184

Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych ma trzy istotne cechy:

- Co do zasady państwom członkowskim zakazuje się w nim wprowadzania wymogów dotyczących lokalizacji danych. Wyjątki od tej zasady mogą być uzasadnione jedynie względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności.
- Ustanawia się w nim mechanizm współpracy mający zapewnić, aby właściwe organy w dalszym ciągu miały możliwość korzystania z wszelkich praw, jakie posiadają, w celu uzyskania dostępu do danych przetwarzanych w innym państwie członkowskim.
- Zapewnia ono dla stosownego sektora zachęty do opracowania – przy wsparciu Komisji – samoregulacyjnych kodeksów postępowania dotyczących zmiany usługodawców i przenoszenia danych.

Cel niniejszych wytycznych

Niniejsze wytyczne stanowią spełnienie wymogu określonego w art. 8 ust. 3 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych, w którym zobowiązuje się Komisję do opublikowania wskazówek na temat wzajemnych powiązań między tym rozporządzeniem a ogólnym rozporządzeniem o ochronie danych, „w szczególności w odniesieniu do zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe".

Niniejsze wytyczne mają stanowić pomoc dla użytkowników – zwłaszcza małych i średnich przedsiębiorstw – w zrozumieniu wzajemnych powiązań między rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych a ogólnym rozporządzeniem o ochronie danych[5]. Dlatego też w wytycznych odniesiono się w szczególności do: (i) pojęć danych nieosobowych i danych osobowych; (ii) zasad swobodnego przepływu danych oraz zakazu stosowania wymogów dotyczących lokalizacji danych na mocy obu rozporządzeń; oraz (iii) pojęcia przenoszenia danych w rozumieniu rozporządzenia w sprawie swobodnego przepływu danych nieosobowych. Wytyczne obejmują również wymogi w zakresie samoregulacji określone w obu rozporządzeniach.

Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych obejmuje jedynie „dane inne niż dane osobowe", przy czym te ostatnie są zdefiniowane w ogólnym rozporządzeniu o ochronie danych. Ogólne rozporządzenie o ochronie danych reguluje przetwarzanie danych osobowych, które stanowi zasadniczy element unijnych ram ochrony danych[6]. Weszło ono w życie w państwach członkowskich w dniu 25 maja 2018 r.

[5] Motyw 37 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[6]
– 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), Dz.U. L 119 z 4.5.2016, s. 1.
– Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1725 z dnia 23 października 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.U. L 295 z 21.11.2018, s. 39.

W rozporządzeniu tym ustanawia się zharmonizowane przepisy mające na celu ochronę osób w UE/EOG w związku z przetwarzaniem ich danych osobowych oraz w sprawie swobodnego przepływu takich danych. Ogólne rozporządzenie o ochronie danych: (i) określa, jakie informacje stanowią dane osobowe; (ii) ustanawia podstawę prawną ich przetwarzania; oraz (iii) określa m.in. prawa i obowiązki, których należy przestrzegać podczas przetwarzania tych danych[7]. W odniesieniu do zasady swobodnego przepływu danych osobowych art. 1 ust. 3 ogólnego rozporządzenia o ochronie danych stanowi, że „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".

W większości rzeczywistych sytuacji zbiór danych najprawdopodobniej będzie składał się zarówno z danych osobowych, jak i danych nieosobowych. Zbiór taki często nazywa się „mieszanym zbiorem danych". W sekcji 2.2 poniżej wyjaśniono bardziej szczegółowo wzajemne powiązania między rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych a ogólnym rozporządzeniem o ochronie danych w odniesieniu do mieszanych zbiorów danych.

Aby zapewnić przejrzystość, w rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych i w ogólnym rozporządzeniu o ochronie danych nie ma sprzecznych obowiązków.

– Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylająca decyzję ramową Rady 2008/977/WSiSW, Dz.U. L 119 z 4.5.2016, s. 89.

– 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 (obecnie trwa procedura wprowadzania do niej zmian).

[7] Aby uzyskać dalsze wytyczne dotyczące różnych aspektów rozporządzenia 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) i europejskich przepisów o ochronie danych – zob. strona internetowa Europejskiej Rady Ochrony Danych, która wydała szereg wytycznych zgodnie z art. 70 ogólnego rozporządzenia o ochronie danych, dostępnych pod adresem: https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_pl Na stronie tej zamieszczono również odniesienia do wytycznych, zaleceń i innych dokumentów opublikowanych przez poprzednika Europejskiej Rady Ochrony Danych – Grupę Roboczą Art. 29. Ponadto, aby zwiększyć świadomość obywateli i przedsiębiorstw w zakresie rozporządzenia 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), Komisja opublikowała komunikat w sprawie ochrony danych – wytyczne Komisji dotyczące bezpośredniego stosowania ogólnego rozporządzenia o ochronie danych (COM(2018) 43 final), który dostępny jest pod adresem: https://eur-lex.europa.eu/legal-content/PL/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043

2 Wzajemne powiązania między rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych a ogólnym rozporządzeniem o ochronie danych – mieszane zbiory danych

2.1 Pojęcie danych nieosobowych w rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych

Celem rozporządzenia w sprawie swobodnego przepływu danych nieosobowych[8] jest zapewnienie swobodnego przepływu danych innych niż dane osobowe. W treści całego rozporządzenia używa się pojęcia „dane", które to pojęcie należy rozumieć jako „dane inne niż dane osobowe zdefiniowane w art. 4 pkt 1 rozporządzenia (UE) 2016/679 [ogólne rozporządzenie o ochronie danych]"[9]. Tego rodzaju dane, w niniejszym dokumencie nazywane również „**danymi nieosobowymi**", definiuje się przez przeciwstawienie ich (*a contrario*) danym osobowym zdefiniowanym w ogólnym rozporządzeniu o ochronie danych.

Dane osobowe

Ogólne rozporządzenie o ochronie danych stanowi, że: „»dane osobowe« oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (»osobie, której dane dotyczą«); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej".

Szeroka definicja danych osobowych jest zamierzona i pozostała zasadniczo niezmieniona w ogólnym rozporządzeniu o ochronie danych w porównaniu z wcześniejszymi przepisami[10]. Różne aspekty definicji danych osobowych, takie jak „wszelkie informacje", „o", „zidentyfikowanej lub możliwej do zidentyfikowania", zostały już rozważone przez Grupę Roboczą Art. 29[11] w Opinii 4/2007 w sprawie pojęcia danych osobowych z dnia 20 czerwca 2007 r., WP 136.

---

[8] Art. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[9] Zob. art. 3 pkt 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[10] Zob. art. 2 lit. a) dyrektywy 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 (data zakończenia obowiązywania: 24 maja 2018 r., uchylona ogólnym rozporządzeniem o ochronie danych). Zob. również orzecznictwo Trybunału Sprawiedliwości w sprawie definicji danych osobowych, w którym uznaje się szeroką interpretację tego pojęcia, na przykład wyrok Trybunału Sprawiedliwości z dnia 29 stycznia 2009 r., Productores de Música de España (Promusicae) v Telefónica de España SAU, C-275/06, ECLI:EU:C:2008:54; wyrok Trybunału Sprawiedliwości z dnia 24 listopada 2011 r., Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), C-70/10, ECLI:EU:C:2011:771; wyrok Trybunału Sprawiedliwości z dnia 19 października 2016 r., Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779.

[11] Grupa Robocza Art. 29 była organem doradczym, który doradzał Komisji w kwestiach dotyczących ochrony danych i który pomagał w tworzeniu zharmonizowanej polityki w zakresie ochrony danych w UE. Po

Powszechną praktyką w obszarach takich jak badania naukowe jest pseudonimizacja danych osobowych w celu ukrycia tożsamości danej osoby. **Pseudonimizacja** to przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie bez użycia dodatkowych informacji. Te dodatkowe informacje są przechowywane osobno i są zabezpieczone za pomocą środków organizacyjnych lub technicznych (np. szyfrowanie)[12,13]. Dane opatrzone pseudonimem wciąż jednak uznaje się za informacje o osobie możliwej do zidentyfikowania, jeżeli można je przypisać tej osobie przy użyciu dodatkowych informacji[14]. Zgodnie z ogólnym rozporządzeniem o ochronie danych dane takie **stanowią dane osobowe**.

Dane nieosobowe

Dane niebędące „danymi osobowymi" w rozumieniu definicji zawartej w ogólnym rozporządzeniu o ochronie danych są **danymi nieosobowymi**. Dane nieosobowe można podzielić na kategorie według pochodzenia na:

- po pierwsze, dane, które pierwotnie nie odnosiły się do zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, takie jak dane dotyczące warunków pogodowych wygenerowane przez czujniki zamontowane na turbinach wiatrowych lub dane dotyczące potrzeb w zakresie konserwacji maszyn przemysłowych;

- po drugie, dane, które pierwotnie były danymi osobowymi, ale poddano je następnie **anonimizacji**[15]. „Anonimizacja" danych osobowych różni się od pseudonimizacji (zob. wyżej), gdyż prawidłowo zanonimizowanych danych nie można przypisać konkretnej osobie nawet przy użyciu dodatkowych danych[16], a zatem są to dane nieosobowe.

---

wejściu w życie ogólnego rozporządzenia o ochronie danych dnia 25 maja 2018 r. Grupa Robocza Art. 29 zastąpiła Europejska Rada Ochrony Danych.

12 Zob. art. 4 pkt 5 rozporządzenia 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), w którym zdefiniowano pojęcie „pseudonimizacji".

13 Na przykład w przypadku badania dotyczącego skutków nowego leku należałoby mówić o pseudonimizacji, jeżeli dane osobowe uczestników badania zastąpiono by w dokumentacji badania niepowtarzalnymi atrybutami (np. numerem lub kodem), a ich dane osobowe przechowywano by osobno, wraz z przypisanymi im niepowtarzalnymi atrybutami, w zabezpieczonym dokumencie (np. w bazie danych chronionej hasłem).

14 Zob. motyw 26 rozporządzenia 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).

15 Zob. motyw 26 rozporządzenia 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), w którym to motywie stwierdza się, że „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".

16 Zob. wyrok Trybunału Sprawiedliwości z dnia 19 października 2016 r., Patrick Breyer v Bundesrepublik Deutschland, C-582/14, ECLI:EU:C:2016:779. Trybunał Sprawiedliwości orzekł, że dynamiczny adres IP może stanowić dane osobowe, nawet jeżeli osoba trzecia (np. dostawca usług internetowych) jest w posiadaniu dodatkowych danych umożliwiających zidentyfikowanie osoby fizycznej.

Ocena, czy dane zanonimizowano prawidłowo, zależy od konkretnych i niepowtarzalnych okoliczności każdego pojedynczego przypadku[17]. Na podstawie kilku przykładów ponownej identyfikacji zbiorów danych, które miały zostać zanonimizowane, wykazano, że dokonanie takiej oceny może być trudne[18]. Aby ustalić, czy osoba fizyczna jest możliwa do zidentyfikowania, należy przyjrzeć się wszystkim środkom, co do których istnieje uzasadnione prawdopodobieństwo, że mogą zostać wykorzystane przez administratora lub inną osobę w celu identyfikacji osoby fizycznej w sposób bezpośredni lub pośredni[19].

Przykłady danych nieosobowych

- Dane, które zagregowano do tego stopnia, że poszczególne wydarzenia (takie jak indywidualne podróże osoby za granicę lub jej typowe trasy podróży, które stanowią dane osobowe) nie są już możliwe do zidentyfikowania, można zakwalifikować jako dane anonimowe[20]. Anonimowe dane wykorzystuje się na przykład w statystykach lub w sprawozdaniach ze sprzedaży (na przykład w celu dokonania oceny popularności produktu lub jego cech).
- Dane dotyczące transakcji wysokich częstotliwości w sektorze finansowym lub dane dotyczące rolnictwa precyzyjnego, które pomagają w monitorowaniu i optymalizacji użycia pestycydów, składników odżywczych i wody.

Jeżeli jednak dane nieosobowe mogą w jakikolwiek sposób zostać powiązane z osobą fizyczną, powodując możliwość zidentyfikowania takiej osoby w sposób bezpośredni albo pośredni, dane należy uznać za dane osobowe.

Możliwość identyfikacji osoby fizycznej musi stanowić środek, co do którego istniałoby uzasadnione prawdopodobieństwo, że zostanie on wykorzystany w celu identyfikacji osoby fizycznej w sposób bezpośredni lub pośredni.

[17] Anonimizacji danych należy zawsze dokonywać przy użyciu najnowszych nowoczesnych technik anonimizacji.

[18] Przykłady ponownej identyfikacji danych, które miały zostać zanonimizowane, można znaleźć w badaniu dotyczącym przyszłych przepływów danych przeprowadzonym dla Komisji Przemysłu, Badań Naukowych i Energii (ITRE) Parlamentu Europejskiego przez C. Blackmana i S. Forge'a: *Data Flows – Future Scenarios: In-Depth Analysis for the ITRE Committee,* 2017 r., s. 22, ramka 2, które jest dostępne w internecie pod adresem: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/607362/IPOL_IDA(2017)607362_EN.pdf

[19] Zob. motyw 26 rozporządzenia (UE) 2016/679 (ogólne rozporządzenie o ochronie danych), zgodnie z którym „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".

[20] Zob. Grupa Robocza Art. 29: *Opinia 05/2014 w sprawie technik anonimizacji*, przyjęta w dniu 10 kwietnia 2014, WP 216, s. 9: „powstały zbiór danych można zakwalifikować jako anonimowy jedynie w przypadku, gdy administrator danych zagregowałby dane, osiągając poziom, na którym nie istnieje już możliwość zidentyfikowania poszczególnych wydarzeń. Na przykład: jeżeli organizacja gromadzi dane dotyczące przemieszczania się osoby fizycznej, wzorce podróżowania tej osoby na poziomie zdarzenia nadal kwalifikowałyby się jako dane osobowe w odniesieniu do każdej strony, o ile administrator danych (lub jakakolwiek inna strona) nadal ma dostęp do oryginalnych danych pierwotnych, nawet jeżeli ze zbioru udostępnionego osobom trzecim usunięto elementy umożliwiające bezpośrednią identyfikację. Jeżeli jednak administrator danych usunąłby dane pierwotne i dostarczył osobom trzecim tylko statystyki zagregowane na wysokim poziomie, takim jak »w poniedziałki trasą X jeździ o 160 % więcej pasażerów niż we wtorki«, statystyki te kwalifikowałyby się jako dane anonimowe".

Na przykład jeżeli sprawozdanie z kontroli jakości na linii produkcyjnej umożliwia powiązanie danych z poszczególnymi pracownikami fabryki (np. z tymi, którzy ustawiają parametry produkcji), dane będą kwalifikować się jako dane osobowe i będzie miało zastosowanie ogólne rozporządzenie o ochronie danych. Te same zasady mają zastosowanie, gdy rozwój technologii i analityki danych umożliwia przekształcenie danych zanonimizowanych w dane osobowe. [21]

Ponieważ definicja danych osobowych odnosi się do „osób fizycznych", zbiory danych zawierające nazwy i dane kontaktowe osób prawnych są co do zasady danymi nieosobowymi[22]. W niektórych sytuacjach mogą one jednak stanowić dane osobowe[23]. Będzie tak na przykład, gdy nazwa osoby prawnej jest taka sama jak imię i nazwisko osoby fizycznej, do której osoba prawna należy, lub gdy informacje dotyczą zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej[24].

2.2 Mieszane zbiory danych

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych oraz w ogólnym rozporządzeniu o ochronie danych zastosowano dwa różne podejścia do swobodnego przepływu danych w UE.

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych ustanowiono ogólny zakaz nakładania wymogów dotyczących lokalizacji danych nieosobowych. W art. 4 ust. 1 tego rozporządzenia zakazuje się nakładania wymogów dotyczących lokalizacji danych, chyba że są one uzasadnione względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności.

Poza wysokim poziomem ochrony danych osobowych ogólne rozporządzenie o ochronie danych zapewnia swobodny przepływ danych osobowych. Zgodnie z art. 1 ust. 3 tego rozporządzenia „nie ogranicza się ani nie zakazuje swobodnego przepływu danych osobowych w Unii z powodów odnoszących się do ochrony osób fizycznych w związku

---

[21] Jeżeli dane osobowe są przetwarzane niezgodnie z prawem lub jeżeli ich przetwarzanie w inny sposób narusza przepisy ogólnego rozporządzenia o ochronie danych, osoby, których dane dotyczą (osoby fizyczne), będą miały zgodnie z ogólnym rozporządzeniem o ochronie danych prawo do wniesienia skargi do krajowego organu nadzorczego (organu ochrony danych) w UE lub do wniesienia skutecznego środka zaskarżenia do sądu krajowego. Zadania, właściwość i uprawnienia krajowych organów nadzorczych uregulowano w rozdziale VI sekcja 2 ogólnego rozporządzenia o ochronie danych.

[22] Motyw 14 rozporządzenia 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) stanowi, że: „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". Należy to jednak odczytywać w świetle definicji danych osobowych zawartej w art. 4 pkt 1 ogólnego rozporządzenia o ochronie danych.

[23] Zob. wyrok Trybunału Sprawiedliwości z dnia 9 listopada 2010 r. w sprawach połączonych Volker und Markus Schecke GbR, C-92/09 i Hartmut Eifert, C-93/09 v Land Hessen, ECLI:EU:C:2010:662, pkt 52.

[24] https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/application-regulation/do-data-protection-rules-apply-data-about-company_pl

z przetwarzaniem danych osobowych". Łącznie w obu rozporządzeniach przewidziano swobodny przepływ „wszystkich" danych w obrębie UE. Przepisy szczegółowe omówiono szerzej w sekcjach 3.1 i 3.2.

Mieszany zbiór danych składa się zarówno z danych osobowych, jak i z danych nieosobowych. Mieszane zbiory danych reprezentują większość zbiorów danych wykorzystywanych w gospodarce opartej na danych i są powszechne ze względu na rozwój technologiczny, np. internet rzeczy (tj. łączność cyfrowa między przedmiotami), sztuczna inteligencja i technologie umożliwiające analizowanie dużych zbiorów danych.

Przykłady mieszanych zbiorów danych:

- wpis przedsiębiorstwa w rejestrze podatkowym zawierający imię i nazwisko oraz numer telefonu dyrektora zarządzającego przedsiębiorstwa;
- zbiory danych w banku, zwłaszcza te zawierające informacje o klientach oraz szczegółowe informacje dotyczące transakcji, np. usług płatniczych (karty kredytowe i debetowe), aplikacje do zarządzania relacjami z partnerami (ang. *partner relationship management*, PRM) i umowy kredytowe, dokumenty zawierające zarówno dane dotyczące osób fizycznych, jak i osób prawnych;
- zanonimizowane dane statystyczne instytucji badawczej oraz wstępnie zebrane surowe dane, takie jak odpowiedzi poszczególnych respondentów na pytania w badaniu statystycznym;
- bazy wiedzy przedsiębiorstwa na temat problemów informatycznych oraz ich rozwiązań opartych na sprawozdaniach z poszczególnych incydentów informatycznych;
- dane dotyczące internetu rzeczy, w przypadku których niektóre dane pozwalają na przyjęcie założeń na temat możliwych do zidentyfikowania osób (np. obecność pod danym adresem i schematy użytkowania); oraz
- analiza operacyjnych danych dziennika pracy sprzętu produkcyjnego w przemyśle wytwórczym.

Przykład: usługi zarządzania relacjami z klientami (ang. *customer relationship management*, CRM)

Niektóre banki korzystają z usług zarządzania relacjami z klientami (CRM) dostarczanych przez osoby trzecie, które wymagają udostępnienia danych klienta w środowisku zarządzania relacjami z klientami. Dane przechowywane w ramach usługi CRM będą obejmowały wszelkie informacje niezbędne do skutecznego zarządzania interakcjami z klientem, takie jak kod pocztowy i adres e-mail, numer telefonu, zakupione produkty i usługi oraz sprawozdania ze sprzedaży, w tym zagregowane dane. Dane takie mogą zatem obejmować zarówno dane osobowe klientów, jak i ich dane nieosobowe.

Jeżeli chodzi o mieszane zbiory danych, rozporządzenie w sprawie swobodnego przepływu danych nieosobowych[25] stanowi, że:

„W przypadku zbiorów danych obejmujących zarówno dane osobowe, jak i nieosobowe niniejsze rozporządzenie ma zastosowanie do części zbioru złożonej z danych nieosobowych. W przypadku gdy w zbiorze danych dane osobowe i nieosobowe są nierozerwalnie związane, niniejsze rozporządzenie pozostaje bez uszczerbku dla stosowania rozporządzenia (UE) 2016/679".

Oznacza to, że w przypadku zbioru danych złożonego zarówno z danych osobowych, jak i nieosobowych:

- do części zbioru danych obejmującej dane nieosobowe zastosowanie ma rozporządzenie w sprawie swobodnego przepływu danych nieosobowych;
- do części zbioru danych obejmującej dane osobowe zastosowanie ma przepis ogólnego rozporządzenia o ochronie danych dotyczący swobodnego przepływu[26]; oraz
- jeżeli część obejmująca dane nieosobowe i część obejmująca dane osobowe są ze sobą „nierozerwalnie związane", prawa i obowiązki dotyczące ochrony danych wynikające z ogólnego rozporządzenia o ochronie danych mają w pełni zastosowanie do całego mieszanego zbioru danych również wtedy, gdy dane osobowe stanowią jedynie niewielką część zbioru danych[27].

Interpretacja ta jest zgodna z prawem do ochrony danych osobowych zagwarantowanym w Karcie praw podstawowych Unii Europejskiej[28] oraz z motywem 8 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych[29]. Motyw 8 tego rozporządzenia stanowi, że nie ma ono wpływu na „ramy prawne w zakresie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych (...), w szczególności na [ogólne rozporządzenie o ochronie danych] (...) oraz dyrektywy (...) (UE) 2016/680 oraz 2002/58/WE".

Praktyczny przykład:

Przedsiębiorstwo działające w UE oferuje swoje usługi za pośrednictwem platformy. Przedsiębiorstwa przesyłają na tę platformę swoje dokumenty zawierające mieszane zbiory danych. Jako „administrator" przedsiębiorstwo przesyłające dokumenty musi upewnić się, że

[25] Art. 2 ust. 2 tego rozporządzenia.

[26] Art. 1 ust. 3 rozporządzenia 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). Zob. również sekcja 3.2 poniżej.

[27] Jak wspomniano w *dokumencie roboczym służb Komisji dotyczącym oceny skutków towarzyszącej wnioskowi w sprawie rozporządzenia Parlamentu Europejskiego i Rady w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej* (SWD(2017) 304 final), część 1/2, s. 3, „niezależnie od tego, jak dużo danych osobowych zawierają mieszane zbiory danych, należy w pełni przestrzegać RODO [ogólnego rozporządzenia o ochronie danych] w odniesieniu do danych osobowych stanowiących część takiego zbioru".

[28] Karta praw podstawowych Unii Europejskiej, Dz.U. C 362 z 26.10.2012, s. 391.

[29] Motyw 8 tego rozporządzenia.

przetwarzanie jest zgodne z ogólnym rozporządzeniem o ochronie danych. Przetwarzając zbiór danych w imieniu administratora, przedsiębiorstwo oferujące usługi („podmiot przetwarzający") musi przechowywać i przetwarzać dane zgodnie z ogólnym rozporządzeniem o ochronie danych, np. aby zapewnić, że gwarantowany jest odpowiedni poziom bezpieczeństwa danych, między innymi za pomocą szyfrowania.

Pojęcie „nierozerwalnie związane" nie zostało zdefiniowane w żadnym ze wspomnianych dwóch rozporządzeń[30]. Ze względów praktycznych może ono odnosić się do sytuacji, w której zbiór danych zawiera zarówno dane osobowe, jak i dane nieosobowe, których rozdzielenie jest albo niemożliwe, albo administrator stwierdził, że byłoby nieefektywne pod względem ekonomicznym bądź niemożliwe z technicznego punktu widzenia. Na przykład przy zakupie systemów do zarządzania relacjami z klientami (CRM) i raportowania sprzedaży przedsiębiorstwo musiałoby podwoić koszty oprogramowania komputerowego, kupując osobne oprogramowanie do zarządzania relacjami z klientami (dane osobowe) oraz systemy do raportowania sprzedaży (dane zagregowane / dane nieosobowe) w oparciu o dane dotyczące CRM.

Podzielenie zbioru danych prawdopodobnie znacząco zmniejszy również wartość zbioru danych. Ponadto zmieniający się charakter danych (zob. sekcja 2.1) utrudnia wyraźne rozróżnienie, a tym samym oddzielenie poszczególnych kategorii danych.

Co ważne, w żadnym z omawianych dwóch rozporządzeń nie zobowiązuje się przedsiębiorstw do podziału zbiorów danych, w odniesieniu do których są one administratorami lub podmiotami przetwarzającymi.

W konsekwencji mieszany zbiór danych będzie zasadniczo podlegać obowiązkom dotyczącym administratorów danych oraz podmiotów przetwarzających i będzie funkcjonował z poszanowaniem praw osób, których dane dotyczą, ustanowionych w ogólnym rozporządzeniu o ochronie danych.

Przetwarzanie danych dotyczących zdrowia

Dane dotyczące zdrowia mogą stanowić część mieszanego zbioru danych. Przykłady obejmują elektroniczną dokumentację medyczną, badania kliniczne i zbiory danych zebranych za pomocą różnych mobilnych aplikacji dotyczących zdrowia i dobrostanu (takich jak aplikacje służące do pomiaru stanu zdrowia, przypominające o braniu leków lub służące do śledzenia postępów w aktywnościach sportowych)[31]. Wraz z postępem technologicznym wyraźny podział na dane osobowe i nieosobowe w tych zbiorach danych coraz bardziej się

[30] Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych i ogólne rozporządzenie o ochronie danych.

[31] Opracowywanie i funkcjonowanie mobilnych aplikacji zdrowotnych wymagają rygorystycznego przestrzegania przepisów ogólnego rozporządzenia o ochronie danych. Wymogi te zostaną doprecyzowane w kodeksie postępowania w zakresie prywatności dotyczącym aplikacji zdrowotnych, nad którym trwają obecnie prace. Więcej informacji na temat stanu prac nad kodeksem można znaleźć pod adresem: https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps

zaciera. W konsekwencji przetwarzanie tych danych musi być zgodne z ogólnym rozporządzeniem o ochronie danych, zwłaszcza (biorąc pod uwagę, że dane dotyczące zdrowia to zgodnie z rozporządzeniem szczególna kategoria danych) z art. 9, w którym określono ogólny zakaz dotyczący przetwarzania szczególnych kategorii danych i wyjątki od tego zakazu.

Dane zawarte w mieszanych zbiorach danych obejmujących dane dotyczące zdrowia mogą być wartościowym źródłem informacji, np. do celów dalszych badań medycznych, do celów pomiaru skutków ubocznych przepisanych leków, do celów statystyki dotyczącej chorób lub do celów rozwijania nowych usług w zakresie opieki zdrowotnej lub leczenia. Przepisy ogólnego rozporządzenia o ochronie danych muszą być jednak przestrzegane przy wykonywaniu wstępnych operacji przetwarzania oraz przy przeprowadzaniu dalszych operacji przetwarzania danych. Każde takie przetwarzanie danych dotyczących zdrowia musi mieć zatem ważną podstawę prawną[32] i odpowiednie uzasadnienie, musi być bezpieczne i zapewniać wystarczające zabezpieczenia.

Ponadto niezwykle istotne jest, aby osoby fizyczne i przedsiębiorstwa miały pewność prawa i zaufanie do przetwarzania danych. Ma to również zasadnicze znaczenie dla gospodarki opartej na danych. Oba rozporządzenia zapewniają realizację tego założenia i oba służą osiągnięciu celu, jakim jest nienaruszanie zasady swobodnego przepływu danych.

3 Swobodny przepływ danych oraz usunięcie wymogów dotyczących lokalizacji danych

W niniejszej sekcji wyjaśniono bardziej szczegółowo pojęcie wymogów dotyczących lokalizacji danych na podstawie rozporządzenia w sprawie swobodnego przepływu danych nieosobowych oraz pojęcie zasady swobodnego przepływu określone w ogólnym rozporządzeniu o ochronie danych. Chociaż adresatami tych przepisów są państwa członkowskie, precyzyjniejszy obraz tego, w jaki sposób oba rozporządzenia przyczyniają się do swobodnego przepływu wszystkich danych w obrębie UE, może okazać się przydatny dla przedsiębiorstw.

3.1 Swobodny przepływ danych nieosobowych

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych[33] „zakazuje się nakładania wymogów dotyczących lokalizacji danych, chyba że są one uzasadnione względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności”.

Wymogi dotyczące lokalizacji danych definiuje się[34] jako „każdy obowiązek, zakaz, warunek, ograniczenie lub innego rodzaju wymóg określony w przepisach ustawowych,

[32] Zob. art. 6 ust. 1 rozporządzenia 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).

[33] Art. 4 ust. 1 tego rozporządzenia.

wykonawczych lub administracyjnych państwa członkowskiego lub wynikający z powszechnych i spójnych praktyk administracyjnych w państwie członkowskim i w podmiotach prawa publicznego, w tym w dziedzinie zamówień publicznych, bez uszczerbku dla dyrektywy 2014/24/UE, który narzuca wymóg przetwarzania danych na terytorium danego państwa członkowskiego lub utrudnia przetwarzanie danych w jakimkolwiek innym państwie członkowskim"[35].'

Zgodnie z tą definicją środki ograniczające swobodny przepływ danych w UE mogą przybierać różne formy. Mogą one być określone w przepisach ustawowych, wykonawczych i administracyjnych lub wręcz wynikać z powszechnych i spójnych praktyk administracyjnych. Ponadto zakaz nakładania wymogów dotyczących lokalizacji danych obejmuje zarówno bezpośrednie, jak i pośrednie środki, które ograniczałyby swobodny przepływ danych nieosobowych.

Bezpośrednie wymogi dotyczące lokalizacji danych mogą obejmować np. obowiązek przechowywania danych w konkretnej lokalizacji geograficznej (np. serwery muszą znajdować się w konkretnym państwie członkowskim) lub obowiązek spełnienia szczególnych krajowych wymogów technicznych (np. dane muszą być przygotowane w określonych krajowych formatach).

Pośrednie wymogi dotyczące lokalizacji danych, które utrudniałyby przetwarzanie danych nieosobowych w jakimkolwiek innym państwie członkowskim, mogą przybierać różne formy. Mogą one obejmować wymogi stosowania rozwiązań technologicznych, które zostały certyfikowane lub zatwierdzone w danym państwie członkowskim, lub inne wymogi skutkujące utrudnianiem przetwarzania danych poza określonym obszarem geograficznym lub określonym terytorium w Unii Europejskiej[36,37].

W ocenie, czy dany środek stanowi pośredni wymóg dotyczący lokalizacji danych, należy uwzględnić specyficzne okoliczności każdego konkretnego przypadku.

---

[34] Art. 3 pkt 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[35] Należy zauważyć, że brak pewności prawa co do zakresu uzasadnionych i nieuzasadnionych wymogów dotyczących lokalizacji danych w jeszcze większym stopniu ogranicza uczestnikom rynku i podmiotom sektora publicznego możliwości wyboru w odniesieniu do miejsca przetwarzania danych (zob. motyw 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej).

[36] Motyw 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[37] Zob. dwa badania poświęcone wymogom dotyczącym lokalizacji danych przeprowadzone przez przyjęciem rozporządzenia w sprawie swobodnego przepływu danych nieosobowych: 1) Godel, M. i in.: *Facilitating cross border data flows in the Digital Single Market*, SMART nr 2015/2016, dokument dostępny w internecie pod adresem: http://ec.europa.eu/newsroom/document.cfm?doc_id=41185 oraz 2) Time.lex, Spark Legal Network i Tech4i2: *Cross-border data flow in the digital single market: study on data localisation restrictions*, SMART nr 2015/0054, dokument dostępny w internecie pod adresem: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=46695

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych[38] odniesiono się do pojęcia **bezpieczeństwa publicznego** zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej. Bezpieczeństwo publiczne „obejmuje zarówno bezpieczeństwo wewnętrzne, jak i zewnętrzne danego państwa członkowskiego[39], a także kwestie ochrony publicznej, w szczególności w celu ułatwienia prowadzenia postępowań przygotowawczych, wykrywania i ścigania przestępstw. Zakłada ono istnienie rzeczywistego i wystarczająco poważnego zagrożenia dla jednego z podstawowych interesów społecznych[40], takiego jak zagrożenie dla funkcjonowania instytucji i podstawowych usług publicznych oraz życia ludności, a także ryzyko poważnego zakłócenia stosunków zagranicznych lub pokojowego współistnienia narodów, lub zagrożenie dla interesów wojskowych".

Ponadto każdy wymóg dotyczący lokalizacji danych uzasadniony ze względów bezpieczeństwa publicznego musi być proporcjonalny. Zgodnie z orzecznictwem Trybunału Sprawiedliwości Unii Europejskiej zasada proporcjonalności wymaga, aby zastosowane środki były właściwe do zapewnienia osiągnięcia wyznaczonego celu i aby nie wykraczały poza zakres niezbędny do osiągnięcia tego celu[41].

Aby zapewnić przejrzystość, zakaz nakładania wymogów dotyczących lokalizacji danych pozostaje bez uszczerbku dla już istniejących ograniczeń określonych w prawie Unii[42].

Ponadto w rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych nie nakłada się żadnych obowiązków na przedsiębiorstwa ani nie ogranicza się ich swobody zawierania umów określających lokalizację przetwarzania ich danych.

Od państw członkowskich wymaga się, by publicznie udostępniały – za pośrednictwem **krajowego centralnego internetowego punktu informacyjnego** (krajowe strony internetowe) – informacje o wszelkich mających zastosowanie na ich terytorium wymogach dotyczących lokalizacji danych. Muszą one je aktualizować lub przekazywać aktualne

---

38 Motyw 19 tego rozporządzenia.

39 Zob. na przykład wyrok Trybunału Sprawiedliwości z dnia 23 listopada 2010 r. Land Baden-Württemberg v Tsakouridis, C-145/09, ECLI:EU:C:2010:708, pkt 43 oraz wyrok z dnia 4 kwietnia 2017 r., Sahar Fahimian v Bundesrepublik Deutschland, C-544/15, ECLI:EU:C:2017:225, pkt 39.

40 Zob. na przykład wyrok Trybunału Sprawiedliwości z dnia 22 grudnia 2008 r. Komisja Wspólnot Europejskich v Republika Austrii, C-161/07, ECLI:EU:C:2008:759, pkt 35 oraz orzecznictwo, o którym mowa w tym wyroku, a także wyrok z dnia 26 marca 2009 r., Komisja Wspólnot Europejskich v Republika Włoska, C-326/07, ECLI:EC:C:2009:193, pkt 70 oraz orzecznictwo, o którym mowa w tym wyroku.

41 Zob. na przykład wyrok Trybunału Sprawiedliwości z dnia 8 lipca 2010 r., Afton Chemical Limited v Secretary of State for Transport, C-343/09, ECLI:EU:C:2010:419, pkt 45 oraz orzecznictwo przywołane w tym wyroku.

42 Zob. na przykład art. 245 ust. 2 dyrektywy 2006/112/WE z dnia 28 listopada 2006 r. w sprawie wspólnego systemu podatku od wartości dodanej, który stanowi, że „państwa członkowskie mogą zobowiązać podatników mających siedzibę na ich terytorium do powiadomienia ich o miejscu przechowywania faktur, jeżeli znajduje się ono poza terytorium danego państwa członkowskiego". Wymóg ten należy jednak odczytywać zgodnie z art. 249, który stanowi, że: „w przypadku gdy podatnik przechowuje faktury, które wystawia lub otrzymuje, za pomocą środków elektronicznych gwarantujących dostęp on–line do danych i gdy miejsce przechowywania znajduje się w państwie członkowskim innym niż państwo, w którym podatnik ma siedzibę, właściwym organom w państwie członkowskim, w którym podatnik ma siedzibę, przysługuje do celów niniejszej dyrektywy prawo dostępu do takich faktur za pomocą środków elektronicznych, prawo do ich pobierania i wykorzystywania w zakresie określonym przepisami państwa członkowskiego, w którym podatnik ma siedzibę, i w stopniu wymaganym przez te organy do celów kontrolnych".

informacje na temat takich wymogów centralnemu punktowi informacyjnemu ustanowionemu na mocy innego aktu Unii[43]. Dla wygody przedsiębiorstw oraz w celu zapewnienia im łatwego dostępu do stosownych informacji w całej UE Komisja zamierza opublikować linki do tych punktów informacyjnych w portalu Twoja Europa[44].

3.2 Swobodny przepływ danych osobowych

Ogólne rozporządzenie o ochronie danych[45] stanowi, że „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".

Jeżeli państwo członkowskie nakłada wymogi dotyczące lokalizacji danych osobowych z powodów innych niż ochrona danych osobowych, konieczna będzie ocena tych wymogów w kontekście przepisów dotyczących podstawowych wolności oraz dozwolonych podstaw odstąpienia od tych wolności określonych w Traktacie o funkcjonowaniu Unii Europejskiej[46,47], a także w kontekście stosownych przepisów UE, takich jak dyrektywa usługowa[48] i dyrektywa w sprawie handlu elektronicznego[49].

Przykład:

W prawie krajowym wymaga się, by lista płac była zlokalizowana w danym państwie członkowskim ze względów związanych z kontrolą regulacyjną, np. przez krajowy organ podatkowy. Taki przepis krajowy wykracza poza zakres art. 1 ust. 3 ogólnego rozporządzenia o ochronie danych, gdyż powody są inne niż ochrona danych osobowych. Konieczna będzie natomiast ocena tego wymogu w kontekście przepisów dotyczących podstawowych wolności oraz dozwolonych podstaw odstąpienia od tych wolności określonych w Traktacie o funkcjonowaniu Unii Europejskiej.

[43] Art. 4 ust. 4 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[44] https://europa.eu/youreurope/index.htm

[45] Art. 1 ust. 3 rozporządzenia 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).

[46] Wersja skonsolidowana Traktatu o funkcjonowaniu Unii Europejskiej, Dz.U. C 326 z 26.10.2012, s. 47.

[47] Zob. również wyrok Trybunału Sprawiedliwości z dnia 19 czerwca 2008 r., Komisja Wspólnot Europejskich v Wielkie Księstwo Luksemburga, C-319/06, ECLI:EU:C:2008:350, pkt 90–91: Trybunał stwierdził, że obowiązek dostępności i przechowywania określonych dokumentów w określonym państwie członkowskim stanowi ograniczenie dla swobody świadczenia usług; uzasadnienie, że dostępność dokumentów ułatwia, „co do zasady, wypełnienie zadań kontrolnych władz tego państwa", nie jest wystarczające.

[48] Dyrektywa 2006/123/WE Parlamentu Europejskiego i Rady z dnia 12 grudnia 2006 r. dotycząca usług na rynku wewnętrznym, Dz.U. L 376 z 27.12.2006, s. 36.

[49] 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.

W ogólnym rozporządzeniu o ochronie danych[50] uznaje się, że państwa członkowskie mogą wprowadzić warunki, w tym ograniczenia, w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. Jak określono w motywie 53, tego rodzaju ograniczenia krajowe nie powinny jednak utrudniać swobodnego przepływu danych osobowych w Unii, jeżeli warunki te odnoszą się do transgranicznego przetwarzania takich danych. Jest to zgodne z art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, w którym określono podstawę prawną przyjmowania przepisów dotyczących prawa do ochrony danych osobowych oraz zasady dotyczące swobodnego przepływu takich danych.

3.3 Zakres rozporządzenia w sprawie swobodnego przepływu danych nieosobowych

Jak już wspomniano, celem rozporządzenia w sprawie swobodnego przepływu danych nieosobowych jest zapewnienie swobodnego przepływu danych nieosobowych „na terytorium Unii”[51]. Nie ma ono zatem zastosowania w przypadku operacji przetwarzania, które mają miejsce poza UE, oraz w przypadku wymogów dotyczących lokalizacji danych związanych z takim przetwarzaniem[52,53].

Zgodnie z art. 2 ust. 1 zakres rozporządzenia ogranicza się zatem do przetwarzania elektronicznych danych nieosobowych w UE, które jest:

(a) świadczone jako usługa na rzecz użytkowników mających miejsce zamieszkania lub siedzibę w UE, niezależnie od tego, czy dostawca usługi ma swoją siedzibę w Unii czy poza nią; lub
(b) prowadzone na potrzeby własne przez osobę fizyczną mającą miejsce zamieszkania w UE lub osobę prawną mającą siedzibę w UE.

Przykłady:

Art. 2 ust. 1 lit. a) rozporządzenia w sprawie swobodnego przepływu danych nieosobowych:

- Dostawca usług w chmurze mający siedzibę w USA świadczy usługi przetwarzania na rzecz klientów mających miejsce zamieszkania lub siedzibę w UE. Dostawca usług w chmurze zarządza swoją działalnością za pomocą serwerów zlokalizowanych na terytorium UE, gdzie są przechowywane lub w inny sposób przetwarzane dane jego

[50] Art. 9 ust. 4 rozporządzenia 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).

[51] Zob. art. 1 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[52] Zob. motyw 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[53] W rozporządzeniu przyjęto szeroką definicję „przetwarzania” (art. 3 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej) i, jak podkreślono w motywie 17, rozporządzenie powinno mieć zastosowanie do jak najszerzej rozumianego przetwarzania danych, obejmującego wykorzystanie wszelkiego rodzaju systemów informatycznych.

europejskich klientów. Dostawca usług w chmurze nie musi być właścicielem infrastruktury znajdującej się w UE, ale może również na przykład wynajmować przestrzeń serwerową w UE. Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych ma zastosowanie do takiego przetwarzania danych.

- Dostawca usług w chmurze mający siedzibę w Japonii oferuje swoje usługi europejskim klientom. Jego zdolności operacyjne w zakresie przetwarzania są zlokalizowane w Japonii i tam odbywają się wszystkie czynności przetwarzania. Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych nie ma w tym przypadku zastosowania, jeżeli wszystkie czynności przetwarzania odbywają się poza UE[54].

Art. 2 ust. 1 lit. b) rozporządzenia w sprawie swobodnego przepływu danych nieosobowych:

- Małe europejskie przedsiębiorstwo typu start-up z państwa członkowskiego A postanawia zwiększyć skalę działania przez otwarcie zakładu w państwie członkowskim B. Aby zminimalizować koszty, przedsiębiorstwo decyduje się na centralizację gromadzenia i przetwarzania danych przez nowy zakład na swoim serwerze, który znajduje się w państwie członkowskim A. Państwa członkowskie nie mogą zakazać takich działań w zakresie centralizacji zaplecza informatycznego, chyba że jest to uzasadnione względami bezpieczeństwa publicznego zgodnie z zasadą proporcjonalności.

Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych nie ma wprawdzie zastosowania, jeśli wszystkie czynności przetwarzania danych nieosobowych są prowadzone poza UE, ale należy przestrzegać ogólnego rozporządzenia o ochronie danych, w przypadku gdy częścią zbioru danych są dane osobowe. W każdym przypadku należy przestrzegać zasad dotyczących przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych na podstawie ogólnego rozporządzenia o ochronie danych[55].

[54] Należy zauważyć, że rozporządzenie Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej nie dotyczy wymogów dotyczących lokalizacji danych nałożonych przez państwa członkowskie w odniesieniu do przechowywania danych nieosobowych w państwach trzecich, a które to wymogi mogą istnieć w krajowych porządkach prawnych. Aby zapewnić przejrzystość, ogólne rozporządzenie o ochronie danych ma zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w UE przez administratora lub podmiot przetwarzający niemających jednostek organizacyjnych w UE, 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 (zob. art. 3 ust. 2 ogólnego rozporządzenia o ochronie danych).

[55] Więcej informacji na temat przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych można znaleźć na stronie internetowej Komisji pod adresem: https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/obligations/what-rules-apply-if-my-organisation-transfers-data-outside-eu_pl oraz w *komunikacie Komisji do Parlamentu Europejskiego i Rady pt. Wymiana i ochrona danych osobowych w zglobalizowanym świecie*, COM(2017) 7 final, dostępnym pod adresem: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2017 %3A7 %3AFIN Jeżeli chodzi o Japonię, dnia 23 stycznia 2019 r. Komisja przyjęła decyzję stwierdzającą odpowiedni stopień ochrony danych osobowych, w której przewidziano swobodny przepływ danych osobowych między tymi dwiema gospodarkami na podstawie gwarancji solidnej ochrony.

3.4 Działania związane z wewnętrzną organizacją państw członkowskich

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych nie zobowiązuje się państw członkowskich do zlecania na zewnątrz świadczenia usług w zakresie danych nieosobowych, które chcą one świadczyć we własnym zakresie lub organizować w sposób inny niż w drodze zamówień publicznych[56].

Art. 2 ust. 3 akapit drugi rozporządzenia w sprawie swobodnego przepływu danych nieosobowych stanowi, że:

„niniejsze rozporządzenie pozostaje bez uszczerbku dla przepisów ustawowych, wykonawczych i administracyjnych dotyczących **wewnętrznej organizacji** państw członkowskich, przyznających organom publicznym i podmiotom prawa publicznego zdefiniowanym w art. 2 ust. 1 pkt 4 dyrektywy 2014/24/UE[57] uprawnienia i obowiązki w zakresie **przetwarzania danych bez wynikającego ze stosunku umownego wynagrodzenia na rzecz podmiotów prywatnych**, jak również dla przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich, które przewidują zasady wykonywania tych uprawnień i obowiązków”[58].

Mogą istnieć uzasadnione interesy, które uzasadniałyby wybór tego rodzaju świadczenia usług przetwarzania danych „we własnym zakresie”, w tym „insourcingu”, lub wzajemnych uzgodnień między organami administracji publicznej. Typowe przykłady obejmują wykorzystanie „chmury rządowej” lub zlecanie przez rząd świadczenia usług przetwarzania danych na rzecz instytucji i organów publicznych scentralizowanej agencji informatycznej.

W rozporządzeniu w sprawie swobodnego przepływu danych nieosobowych zachęca się jednak państwa członkowskie do rozważenia korzyści ekonomicznych i innych korzyści wynikających ze zlecenia świadczenia usług zewnętrznym dostawcom[59],[60]. Gdy tylko organy krajowe zaczną zlecać przetwarzanie danych w ramach „outsourcingu” podmiotom prywatnym za wynagrodzeniem wynikającym ze stosunku umownego, a przetwarzanie

---

[56] Motyw 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[57] Art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE, Dz.U. L 94 z 28.3.2014, s. 65, stanowi, że „»podmiot prawa publicznego« oznacza podmiot, który posiada wszystkie następujące cechy: a) został utworzony w konkretnym celu zaspokajania potrzeb w interesie ogólnym, które nie mają charakteru przemysłowego ani handlowego; b) posiada osobowość prawną; oraz c) jest finansowany w przeważającej części przez państwo, władze regionalne lub lokalne lub inne podmioty prawa publicznego; bądź jego zarząd podlega nadzorowi ze strony tych władz lub podmiotów; bądź ponad połowa członków jego organu administrującego, zarządzającego lub nadzorczego została wyznaczona przez państwo, władze regionalne lub lokalne, lub przez inne podmioty prawa publicznego”.

[58] W motywie 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej stwierdza się, że rozporządzenie to pozostaje bez uszczerbku dla dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE.

[59] Motyw 14 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

[60] Zewnętrzny dostawca usług to dowolny podmiot niebędący „podmiotem prawa publicznego” w rozumieniu art. 2 ust. 1 pkt 4 dyrektywy Parlamentu Europejskiego i Rady 2014/24/UE z dnia 26 lutego 2014 r. w sprawie zamówień publicznych, uchylającej dyrektywę 2004/18/WE, Dz.U. L 94 z 28.3.2014, s. 65.

danych odbywa się w UE, takie przetwarzanie jest objęte rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych, co oznacza, że zasada swobodnego przepływu danych nieosobowych ma zastosowanie do ogólnych i administracyjnych praktyk organów krajowych. Muszą one zwłaszcza powstrzymać się od wprowadzania ograniczeń w zakresie lokalizacji danych, np. w ramach procedur udzielania zamówień publicznych[61].

4 Podejścia samoregulacyjne wspierające swobodny przepływ danych

Samoregulacja przyczynia się do innowacji i zaufania wśród uczestników rynku i może pomóc w lepszym reagowaniu na zmiany na rynku. W niniejszej sekcji przedstawiono przegląd inicjatyw samoregulacyjnych w zakresie przetwarzania danych osobowych i nieosobowych.

4.1 Przenoszenie danych i zmiana dostawcy usług w chmurze

Jednym z celów rozporządzenia w sprawie przepływu danych nieosobowych jest uniknięcie uzależnienia od jednego dostawcy. Praktyki te występują wtedy, gdy użytkownicy nie mogą zmienić dostawcy usług, ponieważ ich dane są „zablokowane" w systemie dostawcy, na przykład ze względu na szczególny format danych lub ustalenia umowne, i nie mogą być przenoszone poza system informatyczny dostawcy. Przenoszenie danych bez przeszkód jest ważnym czynnikiem umożliwiającym użytkownikom swobodne dokonywanie wyboru dostawcy usług przetwarzania danych, a tym samym zapewniającym rozwój skutecznej konkurencji na rynku.

Przenoszenie danych między przedsiębiorstwami staje się coraz ważniejsze w wielu sektorach cyfrowych, w tym w sektorze usług w chmurze.

Zgodnie z art. 6 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych, aby przyczynić się do rozwoju konkurencyjnej gospodarki opartej na danych, Komisja wspiera i ułatwia opracowywanie samoregulacyjnych kodeksów postępowania na poziomie Unii („kodeksy postępowania"). Stanowi on podstawę dla sektora do opracowywania samoregulacyjnych kodeksów postępowania dotyczących zmiany dostawcy usług i przenoszenia danych między różnymi systemami informatycznymi.

Przy opracowywaniu takich kodeksów postępowania dotyczących przenoszenia danych należy uwzględnić szereg aspektów, w szczególności:

- **najlepsze praktyki** w zakresie ułatwiania zmiany dostawcy usług i przenoszenia danych z wykorzystaniem formatów ustrukturyzowanych, powszechnie używanych i nadających się do odczytu maszynowego;
- **minimalne wymogi informacyjne** mające na celu zapewnienie użytkownikom profesjonalnym, przed zawarciem umowy, wystarczająco dokładnych i jasnych informacji na temat następujących kwestii: procesów, wymogów technicznych, ram czasowych i opłat, które mają zastosowanie w przypadku, gdy użytkownik profesjonalny chce

[61] Motyw 13 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

zmienić dostawcę usług lub przenieść dane z powrotem do własnych systemów informatycznych;

- **podejścia w zakresie systemów certyfikacji** ułatwiających porównywanie usług w chmurze; oraz
- **plany działania w zakresie komunikacji** w celu upowszechniania wiedzy o kodeksach postępowania.

Na rynku usług w chmurze Komisja zaczęła ułatwiać pracę grup roboczych zajmujących się usługami w chmurze na jednolitym rynku cyfrowym, skupiających ekspertów w dziedzinie usług w chmurze i użytkowników profesjonalnych, w tym małe i średnie przedsiębiorstwa. Na obecnym etapie jedna podgrupa opracowuje samoregulacyjne kodeksy postępowania dotyczące przenoszenia danych i zmiany dostawcy usług w chmurze (grupa robocza SWIPO)[62], zaś inna podgrupa pracuje nad rozwojem certyfikacji bezpieczeństwa usług w chmurze (grupa robocza CSPCERT)[63].

Grupa robocza SWIPO opracowuje kodeksy postępowania obejmujące całe spektrum usług w chmurze: infrastruktura jako usługa (Infrastructure as a Service, IaaS), platforma jako usługa (Platform as a Service, PaaS) i oprogramowanie jako usługa (Software as a Service, SaaS).

Komisja oczekuje, że poszczególne kodeksy postępowania zostaną uzupełnione **wzorcowymi klauzulami umownymi**[64]. Umożliwi to dostateczną precyzję techniczną i prawną w zakresie praktycznego wdrażania i stosowania kodeksów postępowania, co będzie miało szczególne znaczenie dla małych i średnich przedsiębiorstw. Planuje się, że projekty wzorcowych klauzul umownych zostaną przygotowane po opracowaniu kodeksów postępowania (co powinno nastąpić do dnia 29 listopada 2019 r.).

Zgodnie z art. 8 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych Komisja do dnia 29 listopada 2022 r. oceni wykonanie tego rozporządzenia. Umożliwi to dokonanie oceny: (i) wpływu na swobodny przepływ danych w Europie; (ii) stosowania rozporządzenia, zwłaszcza w odniesieniu do mieszanych zbiorów danych; (iii) zakresu, w jakim państwa członkowskie skutecznie zniosły istniejące nieuzasadnione ograniczenia dotyczące lokalizacji danych; oraz (iv) efektywności rynkowej kodeksów postępowania w dziedzinie przenoszenia danych i zmiany dostawcy usług w chmurze.

[62] Cloud Switching and Porting Data Working Group (Grupa Robocza ds. Przenoszenia Danych i Zmiany Dostawcy Usług w Chmurze).

[63] European Cloud Service Provider Certification Working Group (Grupa Robocza ds. Certyfikacji Europejskich Dostawców Usług w Chmurze). Zob. również sekcja 4.3.

[64] Zob. motyw 30 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej.

Pojęcie przenoszenia i powiązanie z ogólnym rozporządzeniem o ochronie danych

Oba rozporządzenia[65] odnoszą się do przenoszenia danych i celu, jakim jest ułatwienie przenoszenia danych z jednego środowiska informatycznego do drugiego, tj. do systemów innego dostawcy albo do systemów własnych. Zapobiega to uzależnieniu od jednego dostawcy i sprzyja konkurencji między dostawcami usług. Rozporządzenia różnią się jednak pod względem podejścia do przenoszenia, jeżeli chodzi o relację między docelowymi grupami interesów oraz charakter prawny przepisów.

Prawo do przenoszenia danych osobowych na podstawie art. 20 ogólnego rozporządzenia o ochronie danych skupia się na relacji między osobą, której dane dotyczą, a administratorem. Dotyczy ono prawa osoby, której dane dotyczą, do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych, które dostarczyła administratorowi, oraz do przesłania tych danych innemu administratorowi lub do własnych magazynów danych bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe[66]. Zazwyczaj osoby, których dane dotyczą, są w tej relacji konsumentami różnych usług online, którzy chcą zmienić dostawcę tych usług.

Art. 6 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych nie przewiduje prawa użytkowników profesjonalnych do przenoszenia danych, ale obejmuje podejście oparte na samoregulacji i uwzględniające dobrowolne kodeksy postępowania dla tego sektora. Jednocześnie odnosi się on do sytuacji, w której użytkownik profesjonalny zlecił w ramach outsourcingu przetwarzanie swoich danych osobie trzeciej oferującej usługi przetwarzania danych[67]. Zgodnie z art. 3 pkt 8 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych pojęcie „użytkownik profesjonalny" może obejmować zarówno osoby fizyczne, jak i prawne, w tym organy publiczne lub podmioty prawa publicznego, korzystające lub ubiegające się o skorzystanie z usługi przetwarzania danych do celów związanych z ich działalnością handlową, gospodarczą, rzemieślniczą, zawodową lub wykonywanym zadaniem.

W praktyce przenoszenie danych zgodnie z art. 6 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych dotyczy interakcji B2B między użytkownikiem profesjonalnym (którego w przypadkach obejmujących przetwarzanie danych osobowych można zakwalifikować jako „administratora" zgodnie z ogólnym rozporządzeniem o ochronie

[65] Art. 6 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej oraz art. 20 rozporządzenia 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).

[66] Zob. Grupa Robocza Art. 29: *Wytyczne dotyczące prawa do przenoszenia danych*. WP 242 rev.01, przyjęte w dniu 13 grudnia 2016 r., ostatnio zmienione i przyjęte w dniu 5 kwietnia 2017 r.

[67] Motyw 29 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2018/1807 z dnia 14 listopada 2018 r. w sprawie ram swobodnego przepływu danych nieosobowych w Unii Europejskiej stanowi: „Podczas gdy indywidualni konsumenci korzystają z istniejących przepisów prawa Unii [tj. ogólnego rozporządzenia o ochronie danych], brak jest ułatwień dla tych użytkowników, którzy chcą zmienić dostawcę usług w ramach swojej działalności gospodarczej lub zawodowej".

danych) a dostawcą usług (którego należy analogicznie zakwalifikować w niektórych przypadkach jako „podmiot przetwarzający').

Mimo różnic mogą pojawić się sytuacje, w których przenoszenie danych byłoby objęte zarówno rozporządzeniem w sprawie swobodnego przepływu danych nieosobowych, jak i ogólnym rozporządzeniem o ochronie danych w odniesieniu do mieszanych zbiorów danych.

Przykład:

Przedsiębiorstwo korzystające z usług w chmurze postanawia zmienić dostawcę tego rodzaju usług i przenieść wszystkie dane do nowego dostawcy. Zmianę dostawcy usług i przenoszenie danych uwzględniono w umowie zawartej między klientem a dostawcą usług w chmurze. Jeżeli dotychczasowy dostawca usług w chmurze przestrzega kodeksów postępowania opracowanych na podstawie rozporządzenia w sprawie swobodnego przepływu danych nieosobowych, przenoszenie danych musi odbywać się zgodnie z wymogami określonymi w tych kodeksach.

Jeżeli częścią przenoszonych zbiorów danych są również dane osobowe, przenoszenie musi być zgodne ze wszystkimi odpowiednimi przepisami ogólnego rozporządzenia o ochronie danych, przy zapewnieniu w szczególności, aby nowy dostawca usług w chmurze przestrzegał mających zastosowanie wymogów, takich jak wymogi w zakresie bezpieczeństwa[68].

Przykład:

W przypadku gdy bank podejmuje decyzję o zmianie dostawcy usług w zakresie zarządzania relacjami z klientami (CRM), możliwe jest, że niektóre dane (osobowe i nieosobowe) będą musiały zostać przeniesione od dotychczasowego dostawcy do nowego. Dane te będą następnie podlegać różnym wymogom regulacyjnym – niektóre wymogom wynikającym z ogólnego rozporządzenia o ochronie danych, zaś inne wymogom wynikającym z rozporządzenia w sprawie swobodnego przepływu danych nieosobowych.

4.2 Kodeksy postępowania i systemy certyfikacji w zakresie ochrony danych osobowych

Kodeksy postępowania i systemy certyfikacji można wykorzystać do wykazania spełnienia obowiązków wynikających z ogólnego rozporządzenia o ochronie danych (zob. art. 24 ust. 3 i art. 28 ust. 5).

Zgodnie z art. 40 ust. 1 i art. 42 ust. 1 ogólnego rozporządzenia o ochronie danych państwa członkowskie, organy nadzorcze, Europejska Rada Ochrony Danych i Komisja powinny

[68] Zob. Grupa Robocza Art. 29: *Opinia 05/2012 w sprawie przetwarzania danych w chmurze obliczeniowej*, przyjęta w dniu 1 lipca 2012 r., WP 196, w której dokładniej określono sytuację i obowiązki użytkowników i dostawców usług w chmurze w odniesieniu do przetwarzania danych osobowych.

zachęcać sektor do opracowywania kodeksów postępowania oraz do ustanowienia mechanizmów certyfikacji w zakresie ochrony danych.

Stowarzyszenia lub inne podmioty reprezentujące szczególną kategorię administratorów lub podmiotów przetwarzających mogą opracować kodeks postępowania dla danego sektora. Projekt kodeksu musi zostać przedłożony odpowiedniemu właściwemu organowi nadzorczemu do zatwierdzenia[69]. Jeżeli projekt kodeksu postępowania dotyczy czynności przetwarzania w kilku państwach członkowskich, organ nadzorczy musi go przedłożyć przed zatwierdzeniem Europejskiej Radzie Ochrony Danych. Rada wyda następnie swoją opinię na temat tego, czy projekt kodeksu jest zgodny z ogólnym rozporządzeniem o ochronie danych.

Europejska Rada Ochrony Danych opublikowała Wytyczne 1/2019 w sprawie kodeksów postępowania i podmiotów monitorujących zgodnie z ogólnym rozporządzeniem o ochronie danych[70]. Wytyczne zawierają informacje na temat opracowywania kodeksów postępowania, kryteria ich zatwierdzania oraz inne przydatne informacje. Podobnie wydane przez Europejską Radę Ochrony Danych Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 ogólnego rozporządzenia o ochronie danych dostarczają informacji na temat certyfikacji na podstawie tego rozporządzenia oraz opracowywania i zatwierdzania kryteriów certyfikacji[71].

Przykłady kodeksów postępowania opracowanych przez branżę usług przetwarzania w chmurze:

Unijny kodeks postępowania dotyczący przetwarzania w chmurze, którego opracowanie ułatwiła Komisja, przygotowano we współpracy z Cloud Select Industry Group (C-SIG) na podstawie dyrektywy o ochronie danych[72], a następnie ogólnego rozporządzenia o ochronie danych. Unijny kodeks postępowania dotyczący przetwarzania w chmurze obejmuje pełne spektrum usług w chmurze – oprogramowanie jako usługę (SaaS), platformę jako usługę (PaaS) oraz infrastrukturę jako usługę (IaaS)[73].

---

69 Zob. art. 40 ust. 5 i art. 55 rozporządzenia 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).

70 Europejska Rada Ochrony Danych: *Wytyczne 1/2019 w sprawie kodeksów postępowania i podmiotów monitorujących zgodnie z rozporządzeniem 2016/679*, przyjęte w dniu 12 lutego 2019 r., wersja do konsultacji publicznych, dostępne w internecie pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12019-codes-conduct-and-monitoring-bodies-under_en

71 Europejska Rada Ochrony Danych: *Wytyczne 1/2018 dotyczące certyfikacji i określania kryteriów certyfikacji zgodnie z art. 42 i 43 rozporządzenia 2016/679*, przyjęte w dniu 23 stycznia 2019 r., dostępne w internecie pod adresem: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en

72 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 (data zakończenia obowiązywania: 24 maja 2018 r.).

73 Aby uzyskać więcej informacji na temat unijnego kodeksu postępowania dotyczącego przetwarzania w chmurze, zob.: https://eucoc.cloud/en/home.html

W kodeksie postępowania przyjętym przez dostawców usług infrastruktury do przetwarzania w chmurze w Europie (ang. Cloud Infrastructure Services Providers in Europe, CISPE)[74] skupiono się na dostawcach IaaS. Kodeks postępowania CISPE obejmuje wymogi dotyczące dostawców IaaS działających w charakterze podmiotów przetwarzających dane na podstawie ogólnego rozporządzenia o ochronie danych. Określono w nim również przepisy dotyczące struktury zarządzania na potrzeby wdrożenia i stosowania kodeksu.

Przyjęty przez **Cloud Security Alliance kodeks postępowania na rzecz zgodności z ogólnym rozporządzeniem o ochronie danych** skierowany jest do wszystkich stron zainteresowanych przetwarzaniem w chmurze i europejskimi przepisami dotyczącymi danych osobowych, takich jak dostawcy usług w chmurze, obecni i potencjalni klienci usług w chmurze, audytorzy usług w chmurze i doradcy w zakresie usług w chmurze (ang. *cloud broker*). Kodeks postępowania obejmuje pełne spektrum dostawców usług w chmurze[75].

4.3 Zwiększenie zaufania do transgranicznego przetwarzania danych – certyfikacja bezpieczeństwa

Jak stwierdzono w motywie 33 rozporządzenia w sprawie swobodnego przepływu danych nieosobowych, zwiększenie zaufania do bezpieczeństwa transgranicznego przetwarzania danych powinno zmniejszyć skłonność uczestników rynku i podmiotów sektora publicznego do traktowania lokalizacji danych jako zastępczej gwarancji bezpieczeństwa danych. Wraz z pakietem na rzecz cyberbezpieczeństwa zaproponowanym przez Komisję w 2017 r.[76] grupa robocza CSPCERT opracowuje zalecenia na potrzeby ustanowienia europejskiego systemu certyfikacji usług w chmurze, które zostaną przedstawione Komisji. System taki może ułatwić swobodny przepływ danych, umożliwić lepszą porównywalność usług w chmurze oraz zwiększyć popularność usług w chmurze. Komisja może zwrócić się do Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA) o przygotowanie systemu kandydującego zgodnie z odpowiednimi przepisami aktu o cyberbezpieczeństwie[77]. System taki może dotyczyć zarówno danych osobowych, jak i nieosobowych. Oprócz aktu o cyberbezpieczeństwie ogólne rozporządzenie o ochronie danych również można wykorzystać do wykazania istnienia odpowiednich zabezpieczeń dotyczących bezpieczeństwa danych, jak podkreślono w sekcji 4.2[78].

---

[74] Aby uzyskać więcej informacji na temat kodeksu postępowania CISPE, zob.: https://cispe.cloud/code-of-conduct/

[75] Aby uzyskać więcej informacji na temat kodeksu postępowania CSA, zob.: https://gdpr.cloudsecurityalliance.org/

[76] Więcej informacji można znaleźć pod adresem: https://ec.europa.eu/digital-single-market/en/cyber-security

[77] Rozporządzenie Parlamentu Europejskiego i Rady z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie).

[78] Zob. motyw 74 aktu o cyberbezpieczeństwie.

Uwagi końcowe

W sytuacji, gdy łańcuchy wartości mogą rozwijać się ponad granicami sektorowymi i państwowymi, zasadnicze znaczenie dla zdolności UE do pełnego wykorzystania potencjału tkwiącego w danych ma zagwarantowanie pewności prawa i osiągnięcie odpowiedniego poziomu zaufania do przetwarzania danych. Oba omawiane rozporządzenia zapewniają realizację tego założenia i oba służą osiągnięciu celu, jakim jest swobodny przepływ danych. Rozporządzenie w sprawie swobodnego przepływu danych nieosobowych i ogólne rozporządzenie o ochronie danych tworzą łącznie podstawę swobodnego przepływu wszystkich danych w Unii Europejskiej i wysoce konkurencyjnej europejskiej gospodarki opartej na danych.