Uzasadnienie Rady: Stanowisko Rady (UE) nr 6/2016 w pierwszym czytaniu w sprawie przyjęcia rozporządzenia Parlamentu Europejskiego i Rady 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)

(2016/C 159/02)

I. WPROWADZENIE

W dniu 25 stycznia 2012 r. Komisja zaproponowała całościową reformę ochrony danych. Składają się na nią:

— wyżej wspomniany wniosek dotyczący ogólnego rozporządzenia o ochronie danych, które to rozporządzenie ma zastąpić dyrektywę z roku 1995 o ochronie danych (dawny filar pierwszy);

— wniosek dotyczący dyrektywy 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 oraz w sprawie swobodnego przepływu takich danych, która to dyrektywa ma zastąpić decyzję ramową z roku 2008 o ochronie danych (dawny filar trzeci).

W dniu 12 marca 2014 r. Parlament Europejski przyjął stanowisko w pierwszym czytaniu odnośnie do proponowanego rozporządzenia (dok. 7427/14).

W dniu 15 czerwca 2015 r. Rada wypracowała podejście ogólne, a tym samym dała prezydencji mandat do rozmów trójstronnych z Parlamentem Europejskim (dok. 9565/15).

Odpowiednio w dniu 17 i 18 grudnia 2015 r. Parlament Europejski i Rada – na szczeblu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz Komitetu Stałych Przedstawicieli – potwierdziły porozumienie w sprawie kompromisowego tekstu będącego wynikiem negocjacji trójstronnych.

Na posiedzeniach w dniu 12 lutego 2016 r. Rada wypracowała porozumienie polityczne w sprawie projektu rozporządzenia (dok. 5455/15). W dniu 8 kwietnia 2016 r. przyjęła zaś stanowisko w pierwszym czytaniu, w pełni zgodne z kompromisowym tekstem uzgodnionym podczas nieformalnych negocjacji z Parlamentem.

W 2012 r. opinię w sprawie rozporządzenia wydał Komitet Ekonomiczno-Społeczny (Dz.U. C 229 z 31.7.2012, s. 90).

Opinię w sprawie rozporządzenia wydał także Komitet Regionów (Dz.U. C 391 z 18.12.2012, s. 127).

Zasięgnięto opinii Europejskiego Inspektora Danych Osobowych: pierwszą opinię wydał on w 2012 r. (Dz.U. C 192 z 30.6.2012, s. 7), a drugą – w 2015 r. (Dz.U. C 301 z 12.9.2015, s. 1–8).

W dniu 1 października 2012 r. opinię wydała Agencja Praw Podstawowych.

II. CEL

Ogólne rozporządzenie o ochronie danych harmonizuje obowiązujące w Unii Europejskiej przepisy w tej dziedzinie. Ma wzmocnić prawa osób fizycznych do ochrony danych, ułatwić swobodny przepływ danych osobowych na jednolitym rynku, a także zmniejszyć obciążenia administracyjne.

III. ANALIZA STANOWISKA RADY W PIERWSZYM CZYTANIU

A. Uwagi ogólne

W obliczu celu wyznaczonego przez Radę Europejską: aby do końca 2015 r. wypracować porozumienie w sprawie reformy ochrony danych, Parlament Europejski i Rada przeprowadziły nieformalne negocjacje, starając się zbliżyć swoje stanowiska. Treść stanowiska Rady w pierwszym czytaniu w sprawie ogólnego rozporządzenia o ochronie danych (dalej „stanowisko Rady") jest odzwierciedleniem kompromisu wypracowanego przez obu współustawodawców z udziałem Komisji Europejskiej.

Stanowisko Rady podtrzymuje cele dyrektywy 95/46/WE: chroni prawa do ochrony danych oraz swobodę przepływu danych. Jednocześnie stara się dostosować obowiązujące przepisy o ochronie danych do faktu, że w wyniku zmian technologicznych i globalizacji ilość przetwarzanych danych osobowych stale rośnie. Aby proponowane rozporządzenie sprawdziło się także w przyszłości, stanowisko Rady proponuje przepisy neutralne pod względem technologicznym.

Aby ochrona osób fizycznych w całej Unii była spójna i aby nie dopuścić do rozbieżności hamujących swobodę przepływu danych osobowych na rynku wewnętrznym, stanowisko Rady zasadniczo przewiduje jeden zestaw przepisów do bezpośredniego zastosowania w całej Unii. Harmonizacja ta pozwoli wyeliminować rozdrobnienie prawne wynikające z wdrożenia dyrektywy 95/46 przez państwa członkowskie za pomocą zróżnicowanych praw. Jednak aby uwzględnić wymogi szczególnych sytuacji związanych z przetwarzaniem danych (np. w sektorze publicznym), stanowisko Rady pozwala państwom członkowskim uszczegółowić w prawie krajowym zastosowanie przepisów rozporządzenia.

Prawo do ochrony danych osobowych to prawo podstawowe zapisane w art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej. Ponadto art. 16 Traktatu o funkcjonowaniu Unii Europejskiej głosi, że każda osoba – niezależnie od obywatelstwa czy miejsca zamieszkania – ma prawo do ochrony danych osobowych jej dotyczących i że należy określić zasady odnoszące się do tej kwestii oraz do kwestii swobodnego przepływu takich danych. Stanowisko Rady określa więc zasady i przepisy dotyczące ochrony osób fizycznych w związku z przetwarzaniem ich danych osobowych.

Aby osiągnąć cele rozporządzenia, stanowisko Rady zwiększa rozliczalność administratorów (odpowiedzialnych za określanie celów i sposobów przetwarzania danych osobowych) i podmiotów przetwarzających (odpowiedzialnych za przetwarzanie danych osobowych w imieniu administratora), starając się promować faktyczną kulturę ochrony danych. Bazując na tym założeniu, rozporządzenie posługuje się podejściem opartym na ryzyku – pozwalającym różnicować obowiązki administratora i podmiotu przetwarzającego zależnie od ryzyka, z jakim wiąże się prowadzone przez nich przetwarzanie. Ponadto do przestrzegania przepisów o ochronie danych mają się przyczynić kodeksy postępowania i mechanizmy certyfikacji. Takie podejście nie jest nadmiernie nakazowe i redukuje obciążenia administracyjne, nie ograniczając jednak przestrzegania przepisów. Ponadto do stosowania rozporządzenia mają skłaniać administratorów potencjalne kary o odstraszającym charakterze.

Nowe przepisy o ochronie danych zawarte w stanowisku Rady dają także silniejsze, egzekwowalne prawa obywatelom. Zyskają oni lepszą kontrolę nad własnymi danymi osobowymi, a tym samym będą mogli z większym zaufaniem korzystać z transgranicznych usług on-line, to zaś pobudzi jednolity rynek cyfrowy. Szczególnej ochrony wymagają dzieci, które mogą być mniej świadome swoich praw oraz zagrożeń związanych z przetwarzaniem danych osobowych.

Ponadto stanowisko Rady wzmacnia niezależność organów nadzorczych, a równocześnie harmonizuje ich zadania i uprawnienia. Zasady współpracy w sprawach transgranicznych między organami nadzorczymi oraz – w stosownym przypadku – między organami nadzorczymi a Komisją (mechanizm spójności) przyczynią się do spójnego stosowania rozporządzenia w całej Unii Europejskiej. Da to większą pewność prawa i ograniczy obciążenia administracyjne. W przypadku przetwarzania transgranicznego administratorzy i podmioty przetwarzające zyskają też – dzięki mechanizmowi kompleksowej współpracy – pojedynczego interlokutora, a w przypadku sporów – wiążącą decyzję nowo utworzonej Europejskiej Rady Ochrony Danych. Mechanizm taki pozwoli spójniej stosować rozporządzenie. Ponadto da większą pewność prawa i ograniczy obciążenia administracyjne.

Stanowisko Rady przewiduje również kompleksowe ramy przekazywania danych osobowych z Unii Europejskiej odbiorcom w państwach trzecich lub w organizacjach międzynarodowych i zapewnia – w porównaniu z dyrektywą 95/46/WE – nowe narzędzia.

B. **Kwestie kluczowe**

Podczas nieformalnych negocjacji Rada i Parlament Europejski – przy udziale Komisji Europejskiej – zbliżyły swoje stanowiska, które przedstawione były odpowiednio w podejściu ogólnym Rady i w stanowisku Parlamentu Europejskiego z pierwszego czytania. Stanowisko Rady w pierwszym czytaniu w pełni odzwierciedla wypracowany kompromis. Poniżej omówiono kwestie kluczowe dla tego dokumentu.

1. ***Zakres stosowania***

1.1. **Materialny zakres stosowania rozporządzenia i rozdzielność względem dyrektywy o egzekwowaniu prawa**

Stanowisko Rady głosi, że ogólne rozporządzenie o ochronie danych ma zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących lub mających stanowić część ustrukturyzowanego zbioru danych dostępnych według szczegółowych kryteriów. Zakres materialny rozporządzenia i zakres dyrektywy nie pokrywają się. Jasno stwierdzono, że rozporządzenie nie ma zastosowania do przetwarzania danych osobowych przez właściwe organy do zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w tym do ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom. Tym samym organy ścigania (zwłaszcza policja) będą mogły zasadniczo posługiwać się systemem ochrony danych przewidzianym w dyrektywie, jednak mimo tej odrębności osoby objęte ich operacjami zyskają spójną i szeroką ochronę danych osobowych.

1.2. **Instytucje i organy UE**

Aby osoby, których dane dotyczą, były jednolicie i spójnie chronione w związku z przetwarzaniem ich danych osobowych, w stanowisku Rady zaznaczono, że po przyjęciu ogólnego rozporządzenia o ochronie danych należy w niezbędnym zakresie zmodyfikować rozporządzenie (WE) 45/2001 mające zastosowanie do instytucji, organów i jednostek organizacyjnych UE, tak by można było zacząć je stosować w tym samym momencie co rozporządzenie.

1.3. **Wyjątek dla gospodarstw domowych**

Aby ustanawiane przepisy nie były dla osób fizycznych niepotrzebnie obciążające, stanowisko Rady przewiduje, że 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.

1.4. **Terytorialny zakres stosowania**

Pod względem zakresu terytorialnego stanowisko Rady daje administratorom i podmiotom przetwarzającym równe szanse: obejmuje wszystkich administratorów i wszystkie podmioty przetwarzające, niezależnie od tego, czy mają jednostkę organizacyjną w Unii, czy też nie.

Po pierwsze, rozporządzenie stwierdza, że przepisy o ochronie danych mają zastosowanie do przetwarzania danych osobowych w związku z działalnością prowadzoną przez jednostkę organizacyjną administratora lub podmiotu przetwarzającego w Unii, niezależnie od tego, czy samo przetwarzanie odbywa się w Unii. Po drugie, aby ochrona danych przysługiwała nawet wtedy, gdy administrator lub podmiot przetwarzający nie mają jednostki organizacyjnej w Unii, rozporządzenie ma zastosowanie do przetwarzania przez nich danych osobowych osób przebywających w Unii, jeśli czynności przetwarzania wiążą się z oferowaniem towarów lub usług takim osobom w Unii lub z monitorowaniem ich zachowania w Unii. Takie sprecyzowanie zakresu daje administratorom i osobom, których dane dotyczą (tzn. osobom fizycznym, których dane są przetwarzane), także większą pewność prawa.

Stanowisko Rady przewiduje też, że jeżeli administratorzy lub podmioty przetwarzające nie mają jednostki organizacyjnej w Unii, ale są objęci rozporządzeniem, to osoby, których dane dotyczą, i organy nadzorcze muszą mieć punkt kontaktowy w UE: administratorzy lub podmioty przetwarzające muszą na piśmie wyznaczyć przedstawiciela w Unii. Aby nie nakładać niepotrzebnych obciążeń administracyjnych, z obowiązku tego zwolniono przetwarzanie, którego nie uznaje się za mogące powodować ryzyko naruszenia praw i wolności osób fizycznych, oraz przetwarzanie przez organ lub podmiot publiczny państwa trzeciego.

2. ***Zasady dotyczące przetwarzania danych osobowych***

Zasady ochrony danych mają zastosowanie do wszelkich informacji o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, w tym do informacji, których nie da się już przypisać konkretnej osobie bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie („pseudonimizacja"). Rozporządzenie w dużej mierze przejmuje zasady przetwarzania danych

osobowych zawarte w dyrektywie 95/46. Jednocześnie modyfikuje zasadę minimalizacji danych, dostosowując ją do realiów cyfrowych oraz starając się odpowiednio wyważyć z jednej strony ochronę danych osobowych, a z drugiej – możliwość przetwarzania danych przez administratorów.

3. ***Zgodność przetwarzania z prawem***

3.1. **Warunki zgodności przetwarzania z prawem**

Aby zagwarantować pewność prawa, stanowisko Rady – opierając się na dyrektywie 95/46 – stwierdza, że przetwarzanie danych osobowych jest zgodne z prawem wyłącznie w przypadkach, gdy spełniony jest co najmniej jeden z następujących warunków:

— zgoda osoby, której dane dotyczą, na jeden lub kilka konkretnych celów;

— umowa;

— obowiązek prawny;

— ochrona żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

— zadanie realizowane w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

— prawnie uzasadnione interesy realizowane przez administratora lub stronę trzecią.

Spośród warunków tych dwa zasługują na szersze omówienie: zgoda oraz prawnie uzasadnione interesy realizowane przez administratora lub stronę trzecią.

3.1.1. *Zgoda*

Aby umożliwić przetwarzanie danych, osoba, której dane dotyczą, może wyrazić na nie zgodę w drodze jednoznacznej, potwierdzającej czynności, która wyraża jej dobrowolne, konkretne, świadome i jednoznaczne przyzwolenie na przetwarzanie dotyczących jej danych osobowych. Zgoda taka dotyczy wszystkich czynności przetwarzania dokonywanych w tym samym celu lub w tych samych celach. Jeżeli przetwarzanie służy różnym celom, potrzebna jest zgoda na wszystkie. Ponadto administrator musi być w stanie wykazać, że osoba, której dane dotyczą, taką zgodę wyraziła. Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania nie oznaczają zatem zgody. Zdefiniowanie zgody pozwoli trzymać się dorobku prawnego regulującego stosowanie tego pojęcia na bazie dyrektywy 95/46/WE, a zarazem przyczyni się do jednakowego rozumienia i stosowania tego pojęcia w całej Unii Europejskiej.

Ponadto, aby zadbać o prawa osób, których dane dotyczą, do ochrony danych, doprecyzowano, że jeżeli osoby takie wyraziły zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, to żadna część oświadczenia, która narusza rozporządzenie, nie jest wiążąca. Co więcej, oceniając, czy zgodę wyrażono dobrowolnie, należy w jak największym stopniu uwzględnić, czy m.in. od zgody na przetwarzanie danych nie uzależniono wykonania umowy, jeśli do wykonania tej umowy przetwarzanie to nie jest niezbędne.

Ponadto, aby umożliwić wyjątki od ogólnego zakazu przetwarzania szczególnych kategorii danych osobowych, stanowisko Rady przewiduje dla nich próg wyższy niż dla innych rodzajów przetwarzania, gdyż na przetwarzanie danych wrażliwych osoba, której dane dotyczą, musi wyrazić wyraźną zgodę.

Szczególny system ochronny stanowisko Rady przewiduje w przypadku dzieci i ich zgody w przypadku usług społeczeństwa informacyjnego. Przetwarzanie danych osobowych dziecka, które nie ukończyło (maksymalnie) 16 lat, jest zgodne z prawem, jeśli uwzględniając dostępną technologię, można – podejmując rozsądne starania – zweryfikować, że zgodę wyraziła lub ją zaaprobowała osoba sprawująca nad dzieckiem opiekę lub władzę rodzicielską. Państwa członkowskie, które uważają, że stosowniejsza byłaby niższa granica wiekowa, mogą ustalić ją niżej, ale nie poniżej 13 lat.

3.1.2. *Prawnie uzasadniony interes administratora*

Przetwarzanie danych osobowych może być zgodne z prawem, jeżeli jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią. Takie prawnie uzasadnione interesy nie wystarczają jednak, aby przetwarzanie było zgodne z prawem, jeżeli nadrzędny charakter wobec nich mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, zwłaszcza gdy osobą tą jest dziecko.

Aby stwierdzić, czy prawnie uzasadniony interes istnieje, należy przeprowadzić ocenę, m.in. tego, czy w czasie i w kontekście, w którym dane osobowe są zbierane, osoba, której dane dotyczą, ma rozsądne przesłanki, by się spodziewać, że może nastąpić przetwarzanie danych w tym celu. Za działanie wykonywane w prawnie uzasadnionym interesie można uznać przetwarzanie danych osobowych do celów marketingu bezpośredniego. Ponieważ dla organów publicznych prawną podstawę przetwarzania danych osobowych powinien określić ustawodawca, nie dotyczy to przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

3.2. **Szczegółowe przepisy państw członkowskich dostosowujące stosowanie rozporządzenia**

Stanowisko Rady pozwala państwom członkowskim zachować lub wprowadzić bardziej szczegółowe przepisy dostosowujące stosowanie przepisów rozporządzenia, jeżeli przetwarzanie danych osobowych służy wypełnieniu obowiązku prawnego lub jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Przewidziano ponadto wyjątki, szczególne wymogi i inne środki względem konkretnych operacji przetwarzania, w których państwa członkowskie godzą prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, publicznym dostępem do dokumentów urzędowych; przetwarzaniem krajowych numerów identyfikacyjnych; przetwarzaniem danych w kontekście zatrudnienia oraz przetwarzaniem danych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

3.3. **Dalsze przetwarzanie**

Stanowisko Rady stwierdza, że przetwarzanie danych osobowych w celu innym niż cel, w którym dane te zostały pierwotnie zebrane, jest zgodne z prawem wyłącznie wtedy, gdy jest zgodne z celami, w których dane te zostały pierwotnie zebrane. Jeżeli jednak osoba, której dane dotyczą, wyrazi zgodę lub jeżeli podstawą przetwarzania jest prawo Unii lub prawo państwa członkowskiego stanowiące w demokratycznym społeczeństwie niezbędny i proporcjonalny środek służący realizacji w szczególności ważnych celów leżących w ogólnym interesie publicznym, administrator może dokonać dalszego przetwarzania danych osobowych bez względu na jego zgodność z pierwotnymi celami. W przypadku dalszego przetwarzania wzmocniono prawa osób, których dane dotyczą, zwłaszcza prawo do informacji oraz prawo do sprzeciwu wobec takiego dalszego przetwarzania, jeżeli nie jest ono niezbędne do wykonania zadania realizowanego w interesie publicznym.

Aby ustalić, czy cel dalszego przetwarzania danych osobowych jest zgodny z celem, w którym dane te zostały pierwotnie zebrane, administrator musi uwzględnić m.in. wszelkie powiązania pomiędzy pierwotnymi celami a celami zamierzonego dalszego przetwarzania, kontekst, w którym dane osobowe zostały zebrane (w szczególności rozsądne oczekiwania osoby, której dane dotyczą, co do dalszego wykorzystania danych oparte na jej powiązaniu z administratorem), charakter danych osobowych, konsekwencje zamierzonego dalszego przetwarzania dla osoby, której dane dotyczą, oraz istnienie odpowiednich zabezpieczeń zarówno podczas pierwotnej, jak i zamierzonej operacji dalszego przetwarzania.

3.4. **Przetwarzanie szczególnych kategorii danych osobowych**

Dane osobowe, które z racji swego charakteru są szczególnie wrażliwe, wymagają szczególnej ochrony, gdyż kontekst ich przetwarzania może powodować wysokie ryzyko naruszenia podstawowych praw i wolności osób fizycznych. Dlatego zasadniczo stanowisko Rady podtrzymuje podejście zastosowane w dyrektywie 95/46 i zakazuje przetwarzania szczególnych kategorii danych osobowych.

W ramach wyjątku od tej zasady dopuszczono przetwarzanie danych wrażliwych w pewnych ściśle wskazanych sytuacjach, np. gdy osoba, której dane dotyczą, wyraziła wyraźną zgodę, gdy przetwarzanie jest niezbędne ze względu na ważny interes publiczny lub ze względu na inne cele, m.in. w dziedzinie zdrowia.

Ponadto stanowisko Rady przewiduje, że państwa członkowskie mogą wprowadzić dalsze warunki (w tym ograniczenia) przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia. Warunki te nie mogą jednak zakłócać swobodnego przepływu danych w Unii.

4. ***Mocniejsza pozycja osób, których dane dotyczą***

4.1. **Wprowadzenie**

Stanowisko Rady daje mocną pozycję osobom, których dane dotyczą, ponieważ wzmacnia przysługujące im prawa do ochrony danych, a na administratorów nakłada obowiązki. Wśród praw osób, których dane dotyczą, są: prawo do informacji, prawo dostępu do danych osobowych, prawo do sprostowania danych osobowych, prawo do usunięcia danych osobowych (w tym „prawo do bycia zapomnianym"), prawo do ograniczenia przetwarzania, prawo do przenoszenia danych, prawo do sprzeciwu czy prawo do niepodlegania decyzji opartej wyłącznie na automatycznym przetwarzaniu (w tym profilowaniu). W porównaniu z dyrektywą 95/46 prawa te w istotny sposób się zmieniły, o czym mowa poniżej.

Administratorzy mają obowiązek ułatwiać osobom, których dane dotyczą, wykonywanie przysługujących im praw oraz przetwarzać dane zgodnie z zasadą przejrzystości, zwłaszcza informując o prowadzonym przez siebie przetwarzaniu.

Jednak jeżeli dane osobowe przetwarzane przez administratora nie pozwalają mu zidentyfikować osoby, której dane dotyczą, nie ma on obowiązku uzyskania dodatkowych informacji w celu jej zidentyfikowania wyłącznie po to, by zastosować się do przepisów rozporządzenia.

Niezależnie od praw osób, których dane dotyczą, i od obowiązków administratorów stanowisko Rady podtrzymuje podejście zastosowane w dyrektywie 95/46 i pozwala ograniczać ogólne zasady i prawa osób fizycznych, jeżeli ograniczenia takie opierają się na prawie Unii lub prawie państwa członkowskiego. Ograniczenia muszą respektować istotę podstawowych praw i wolności oraz muszą być niezbędne i proporcjonalne w społeczeństwie demokratycznym w celu ochrony pewnych interesów publicznych.

4.2. **Przejrzystość**

W myśl zasady przejrzystości administratorzy muszą w związku przetwarzaniem danych osobowych udzielać informacji i prowadzić komunikację w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, zwłaszcza jeśli zwracają się do dziecka. Informacji muszą udzielać na piśmie lub w inny sposób, a w stosownym przypadku – elektronicznie.

Stanowisko Rady ponadto określa termin, w którym administrator musi odpowiedzieć na żądanie informacji, podjęcia komunikacji lub podjęcia wszelkich innych działań, i zasadniczo przewiduje ich bezpłatność. Jeżeli jednak żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, zwłaszcza ze względu na swój ustawiczny charakter, administrator może pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, albo może odmówić podjęcia żądanych działań. W takich przypadkach obowiązek wykazania, że żądanie ma ewidentnie nieuzasadniony lub nadmierny charakter, spoczywa na administratorze.

4.3. **Informacje i komunikacja ze strony administratora**

Aby z jednej strony udzielić osobom, których dane dotyczą, dostatecznych informacji o przetwarzaniu ich danych, a z drugiej – nie nakładać na administratorów uciążliwych obowiązków, stanowisko Rady przewiduje podejście dwuetapowe – zarówno gdy dane osobowe są zbierane od osoby, której dane dotyczą, jak i gdy są pozyskiwane w inny sposób. Po pierwsze, podczas pozyskiwania danych osobowych administrator ma obowiązek udzielić osobie, której dane dotyczą, informacji wymienionych w rozporządzeniu. Po drugie, musi udzielić informacji dodatkowych, także wymienionych w rozporządzeniu, które są niezbędne do rzetelnego i skutecznego przetwarzania. Administrator ma także poinformować osobę, której dane dotyczą, o tym, że zamierza dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały pierwotnie zebrane.

Administrator nie ma jednak obowiązku udzielić informacji przewidzianych w pierwszym albo drugim etapie, jeżeli osoba, której dane dotyczą, dysponuje już tymi informacjami. Jeżeli dane osobowe nie zostały pozyskane od osoby, której dane dotyczą, administrator nie udziela jej informacji, jeżeli utrwalenie danych osobowych lub ich ujawnienie innym podmiotom są wyraźnie przewidziane prawem lub udzielenie informacji danej osobie okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

Ponadto administratorzy mają obowiązek informować każdego z odbiorców, któremu ujawnili dane, o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych, chyba że okaże się to niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku. Administrator musi też poinformować osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba ta tego zażąda.

4.4. **Znaki graficzne**

Przejrzystość przetwarzania wymaga, by osoba, której dane dotyczą, była informowana o samym przetwarzaniu i o jego celach. W związku z tym stanowisko Rady ustala, że informacje, których udziela się tej osobie, mogą być opatrzone standardowymi znakami graficznymi. Administratorzy mogą sami zdecydować, czy ich użycie będzie przydatne dla prowadzonego przez nich przetwarzania. Znaki te powinny w widoczny, zrozumiały i czytelny sposób przedstawiać sens zamierzonego przetwarzania. Należy je zaprezentować równocześnie z samymi informacjami. Jeżeli znaki te są przedstawiane elektronicznie, muszą się nadawać do odczytu maszynowego. Aby rozpropagować standardowe znaki graficzne w UE, rozporządzenie upoważnia Komisję do przyjmowania aktów delegowanych, które określałyby, jakie informacje należy przedstawić za pomocą znaków graficznych i jakie procedury zastosować w celu ich ustanowienia. Opinię o znakach zaproponowanych przez Komisję musi wydać Europejska Rada Ochrony Danych. Możliwość przyjmowania przez Komisję aktów delegowanych nie wyklucza publikowania przez Europejską Radę Ochrony Danych wytycznych, opinii i najlepszych praktyk co do znaków graficznych.

4.5. **Prawo dostępu**

Osoba, której dane dotyczą, jest uprawniona do uzyskania od administratora potwierdzenia, czy przetwarzane są dane jej dotyczące, a jeżeli takie dane są przetwarzane – do uzyskania dostępu do informacji wymienionych w rozporządzeniu. W tym kontekście rozporządzenie wskazuje, że administrator musi bezpłatnie dostarczyć kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne żądane kopie administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Prawo do uzyskania kopii nie może niekorzystnie wpływać na prawa i wolności innych.

4.6. **Prawo do usunięcia danych („prawo do bycia zapomnianym")**

Stanowisko Rady uprawnia osoby, których dane dotyczą, do żądania, by dane osobowe ich dotyczące zostały usunięte, o ile przetwarzanie takich danych jest niezgodne z rozporządzeniem lub z prawem Unii, lub z prawem państwa członkowskiego, któremu podlega administrator.

Wzmianka o „prawie do bycia zapomnianym" wynika z potrzeby, by prawo do usunięcia danych dostosować zwłaszcza do realiów cyfrowych. Jeżeli osoba, której dane dotyczą, zażądała usunięcia danych osobowych, ale administrator wcześniej te dane upublicznił, musi on – biorąc pod uwagę dostępną technologię i koszt realizacji – podjąć rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda usunięcia łączy do nich, ich kopii lub replikacji. Europejska Rada Ochrony Danych może wydawać wytyczne, zalecenia i najlepsze praktyki co do procedur usuwania łączy, kopii lub replikacji danych osobowych z ogólnodostępnych usług łączności.

Prawo do usunięcia danych oraz spoczywający na administratorze obowiązek poinformowania innych administratorów o żądaniu usunięcia danych nie mają zastosowania, jeżeli przetwarzanie danych osobowych jest niezbędne do celów, których wyczerpująca lista znajduje się w rozporządzeniu, takich jak prawo do wolności wypowiedzi i informacji.

4.7. **Prawo do przenoszenia danych**

Stanowisko Rady przewiduje, że jeżeli przetwarzanie danych osobowych odbywa się w sposób zautomatyzowany, osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym, interoperacyjnym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, których dostarczyła administratorowi, i ma prawo przesłać te dane innemu administratorowi. Ponadto stanowisko Rady stwierdza, że osoba, której dane dotyczą, ma prawo zażądać, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe. Zwiększa to dodatkowo kontrolę osoby, której dane dotyczą, nad własnymi danymi. Stymuluje też konkurencję wśród administratorów.

Jednak prawo do przenoszenia danych nie ma zastosowania do przetwarzania, które jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi. Ponadto jeżeli w pewnych zestawach dane osobowe dotyczą więcej niż jednej osoby, prawo osoby, której dane dotyczą, do otrzymania danych osobowych pozostaje bez uszczerbku dla praw i wolności innych.

4.8. **Prawo do sprzeciwu**

Nawet jeżeli dane osobowe można przetwarzać zgodnie z prawem, gdyż przetwarzanie to jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi lub ze względu na uzasadnione interesy administratora lub strony trzeciej, każdej osobie, której dane dotyczą, przysługuje prawo do sprzeciwu wobec przetwarzania danych osobowych dotyczących jej indywidualnej sytuacji. W takim przypadku administratorowi nie wolno już przetwarzać tych danych, chyba że wykaże istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania – nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą – lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

W tym kontekście wskazano, że jeżeli dane osobowe są przetwarzane do celów marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych. Dotyczy to też profilowania, o ile wiąże się z takim marketingiem bezpośrednim. „Profilowanie" zdefiniowano jako dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów. Ponadto o prawie tym należy wyraźnie i jasno poinformować osobę, której dane dotyczą, najpóźniej przy okazji pierwszej komunikacji między administratorem a tą osobą.

Ponadto stanowisko Rady wspomina o internetowej funkcji ochrony przed śledzeniem, stwierdzając, że w związku z korzystaniem z usług społeczeństwa informacyjnego osoba, której dane dotyczą, może wykonać prawo do sprzeciwu za pośrednictwem zautomatyzowanych środków wykorzystujących specyfikacje techniczne.

4.9. **Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach (w tym profilowanie)**

Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, ocenia jej aspekty osobowe i wywołuje wobec niej skutki prawne lub w podobny sposób istotnie na nią wpływa. Przykłady to automatyczne odrzucenie elektronicznego wniosku kredytowego oraz rekrutacja elektroniczna bez interwencji ludzkiej. Elementem takiego zautomatyzowanego przetwarzania może być profilowanie. Jednak prawo do niepodlegania zautomatyzowanemu przetwarzaniu nie ma zastosowania, jeżeli przetwarzanie:

— jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem;

— jest dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, np. monitorowanie oszustw i uchylania się od podatków; lub

— opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

— Z wyjątkiem przypadku drugiego, który dotyczy przetwarzania dozwolonego prawem Unii lub prawem państwa członkowskiego, administrator przetwarzający dane w sposób zautomatyzowany musi wdrożyć właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą. Wśród środków tych muszą się znaleźć co najmniej: prawo do uzyskania interwencji ludzkiej ze strony administratora oraz możliwość wyrażenia własnego stanowiska i zakwestionowania danej decyzji. Ponadto – aby zapewnić rzetelność i przejrzystość przetwarzania – administratorzy powinni stosować odpowiednie matematyczne i statystyczne procedury profilowania oraz środki minimalizujące potencjalne ryzyko dla interesów osób, których dane dotyczą.

Osoba, której dane dotyczą, zyskuje jeszcze więcej praw: administrator musi udzielić jej informacji – jeżeli jest to niezbędne z punktu widzenia rzetelności i przejrzystości przetwarzania – o istnieniu zautomatyzowanego podejmowania decyzji, w tym profilowania, oraz (przynajmniej w tych przypadkach) użytecznych informacji o założeniach przetwarzania oraz o znaczeniu i możliwych konsekwencjach przetwarzania wobec niej.

Zautomatyzowane podejmowanie decyzji i profilowanie oparte na szczególnych kategoriach danych osobowych jest dozwolone wyłącznie przy zachowaniu szczególnych warunków, w tym prawa osoby, której dane dotyczą, do sprzeciwu wobec takiego przetwarzania, jeżeli dane te są dalej przetwarzane do celów badań naukowych lub historycznych lub do celów statystycznych – chyba że takie przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym.

Europejska Rada Ochrony Danych może wydać wytyczne, zalecenia i najlepsze praktyki, aby doprecyzować kryteria i wymogi co do decyzji opartych na profilowaniu.

5. *Administrator i podmiot przetwarzający*

5.1. **Wprowadzenie**

Stanowisko Rady ujmuje w prawne ramy obowiązki oraz odpowiedzialność prawną za przetwarzanie danych osobowych przez administratora lub w imieniu administratora przez podmiot przetwarzający. Zgodnie z zasadą rozliczalności administrator ma obowiązek wdrożyć odpowiednie środki techniczne i organizacyjne i móc wykazać, że operacje przetwarzania są zgodne z rozporządzeniem. W tym kontekście rozporządzenie zawiera przepisy dotyczące obowiązków administratora w zakresie oceny skutków, prowadzenia rejestrów przetwarzania, naruszeń ochrony danych, wyznaczania inspektora ochrony danych, kodeksów postępowania i mechanizmów certyfikacji.

5.2. **Ocena skutków**

Administrator ma obowiązek dokonać oceny skutków dla ochrony danych, aby oszacować, kiedy przetwarzanie z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Stanowisko Rady wskazuje, kiedy ocena taka jest szczególnie wymagana, np. w niektórych operacjach przetwarzania na dużą skalę. Jeżeli ocena skutków wskaże, że operacje przetwarzania powodowałyby wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed rozpoczęciem przetwarzania musi skonsultować się z organem nadzorczym. Organ nadzorczy może wtedy udzielić administratorowi zalecenia i skorzystać z dowolnego ze swoich uprawnień.

Europejska Rada Ochrony Danych może wydawać wytyczne w sprawie operacji przetwarzania mogących powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, i może wskazywać, jakie środki wystarczą w takich przypadkach dla zaradzenia takiemu potencjalnemu ryzyku.

5.3. **Rejestrowanie czynności przetwarzania**

Aby umożliwić organowi nadzorczemu kontrolę ex post, administrator lub – gdy ma to zastosowanie – przedstawiciel administratora, lub podmiot przetwarzający muszą prowadzić rejestr czynności przetwarzania, za które odpowiadają, w tym naruszeń ochrony danych. Aby obciążenia administracyjne nie były nadmierne, obowiązek prowadzenia rejestru nie ma zastosowania do przedsiębiorców ani podmiotów zatrudniających mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje dane wrażliwe lub dane dotyczące wyroków skazujących i naruszeń prawa.

5.4. **Naruszenia ochrony danych**

Naruszenie ochrony danych osobowych może skutkować uszczerbkiem fizycznym oraz szkodami majątkowymi lub niemajątkowymi, takimi 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 chronionych tajemnicą zawodową lub wszelkie inne szkody gospodarcze lub społeczne. W myśl stanowiska Rady administrator musi zgłosić naruszenie ochrony danych organowi nadzorczemu, chyba że jest mało prawdopodobne, by skutkowało ryzykiem naruszenia praw i wolności osób

fizycznych. Musi też – jeżeli naruszenie może skutkować wysokim ryzykiem – zawiadomić o nim osobę, której dane dotyczą. Zgłoszenie naruszenia organowi nadzorczemu pozwoli temu organowi w razie potrzeby zainterweniować. Ponadto zawiadomienie osoby, której dane dotyczą, pozwoli jej przedsięwziąć środki zaradcze.

Aby nie nakładać nadmiernych obciążeń administracyjnych, stanowisko Rady różnicuje wymóg zgłaszania naruszeń organowi nadzorczemu i wymóg zawiadamiania o nim osób, których dane dotyczą: próg dla zawiadomień jest wyższy niż dla zgłoszeń. Administratorzy mają obowiązek, jak tylko stwierdzą naruszenie, zgłosić je bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin – właściwemu organowi nadzorczemu. Mogą tego nie zrobić, jeżeli są w stanie wykazać, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw i wolności osób fizycznych. Poza kilkoma wyjątkami administratorzy mają obowiązek bez zbędnej zwłoki zawiadomić o naruszeniu ochrony danych osoby, których dane dotyczą, jeżeli naruszenie może skutkować wysokim ryzykiem naruszenia ich praw i wolności.

Europejska Rada Ochrony Danych może wydawać wytyczne, zalecenia i najlepsze praktyki, jak stwierdzać naruszenie, określać zbędną zwłokę po stwierdzeniu naruszenia, w jakich okolicznościach administrator musi zgłosić naruszenie oraz w jakich naruszenie może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych.

5.5. **Inspektor ochrony danych**

Aby zwiększyć przestrzeganie rozporządzenia, wyznacza się inspektora ochrony danych. Powinna to być osoba o wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych; musi ona pomagać administratorowi i podmiotowi przetwarzającemu monitorować wewnętrzne przestrzeganie rozporządzenia. Inspektor może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług. W przypadku grupy przedsiębiorstw lub administratorów lub podmiotów przetwarzających będących organami publicznymi, można wyznaczyć jednego inspektora. Stanowisko Rady przewiduje, że inspektora należy wyznaczyć zawsze wtedy, gdy:

— przetwarzania dokonuje organ publiczny, z wyjątkiem sądów lub niezależnych organów sądowych w zakresie sprawowania przez nie wymiaru sprawiedliwości;

— główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę; lub

— główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych wrażliwych oraz danych dotyczących wyroków skazujących i naruszeń prawa.

5.6. **Kodeksy postępowania i mechanizmy certyfikacji**

Stanowisko Rady zachęca do stosowania kodeksów postępowania i propaguje mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych. Tego rodzaju inicjatywy mają przyczynić się do przestrzegania przepisów o ochronie danych, a zarazem zapobiec nadmiernej nakazowości i nadmiernym wydatkom organów publicznych egzekwujących przepisy. Kodeksy postępowania mają uwzględniać specyficzny charakter przetwarzania w niektórych sektorach oraz potrzeby mikroprzedsiębiorstw oraz przedsiębiorstw małych i średnich. Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych tymczasem mają przyczynić się do przestrzegania rozporządzenia w ten sposób, że osoby, których dane dotyczą, będą mogły łatwo ocenić poziom ochrony cechujący dane wyroby lub usługi.

Stanowisko Rady zawiera rozbudowane przepisy dotyczące kodeksów postępowania i mechanizmów certyfikacji oraz znaków jakości i oznaczeń w zakresie ochrony danych, ale pozostawia pewne pole do własnej inicjatywy, przy czym chroni standardy ochrony danych, gdyż włącza w działania organy nadzorcze.

5.6.1. *Kodeksy postępowania*

Organ nadzorczy może zatwierdzać nowe, zmienione lub rozszerzone kodeksy postępowania. Jeżeli projekt kodeksu postępowania dotyczą czynności przetwarzania prowadzonych w kilku państwach członkowskich, właściwy organ nadzorczy musi przed zatwierdzeniem projektu kodeksu, zmiany lub rozszerzenia przedłożyć je do zaopiniowania Europejskiej Radzie Ochrony Danych.

Komisja może przyjmować akty wykonawcze w celu stwierdzenia, czy nowe, zmienione lub rozszerzone kodeksy zatwierdzone przez właściwy organ nadzorczy mają powszechnie obowiązywać w Unii.

Europejska Rada Ochrony Danych powinna zachęcać do opracowywania kodeksów postępowania. Musi też gromadzić w rejestrze wszystkie zatwierdzone kodeksy podstępowania i zmiany do nich i udostępniać je opinii publicznej za pomocą odpowiednich środków.

5.6.2. *Mechanizmy certyfikacji oraz znaki jakości i oznaczenia w zakresie ochrony danych*

Stanowisko Rady przewiduje, że każde państwo członkowskie musi określić, czy podmioty certyfikujące są akredytowane przez organ nadzorczy czy krajową jednostkę akredytującą. Akredytowane podmioty certyfikujące mogą udzielić certyfikacji administratorom i podmiotom przetwarzającym na podstawie kryteriów zatwierdzonych przez właściwy organ nadzorczy lub – zgodnie z mechanizmem spójności – przez Europejską Radę Ochrony Danych. W tym drugim przypadku kryteria zatwierdzone przez Europejską Radę Ochrony Danych mogą skutkować wspólną certyfikacją: europejskim znakiem jakości ochrony danych. Certyfikacji udziela się administratorowi lub podmiotowi przetwarzającemu maksymalnie na 3 lata z możliwością przedłużenia. Podmiot certyfikujący musi przedstawić organowi nadzorczemu powody udzielenia lub cofnięcia żądanej certyfikacji. Na tej podstawie organ nadzorczy może odrzucić certyfikację lub stwierdzić jej nieważność.

Do Komisji należy przyjmowanie aktów delegowanych w celu doprecyzowania wymogów, które uwzględnia się w przypadku mechanizmów certyfikacji. Opinię o tych wymogach musi wydać Europejska Rada Ochrony Danych. Komisja może też przyjmować akty wykonawcze w sprawie technicznych standardów mechanizmów certyfikacji oraz znaków jakości i oznaczeń w dziedzinie ochrony danych, a także sposobów upowszechniania i uznawania tych mechanizmów, znaków i oznaczeń.

Ponadto Europejska Rada Ochrony danych powinna zachęcać do ustanowienia takich mechanizmów, znaków i pieczęci.

6. *Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych*

6.1. **Wprowadzenie**

Transgraniczny przepływ danych osobowych do państw spoza Unii i do organizacji międzynarodowych oraz z takich państw i z takich organizacji jest kluczowy w globalnym handlu i transgranicznej gospodarce cyfrowej. Jeżeli dane obywateli UE są przekazywane poza Unię, należy zachować stopień ich ochrony gwarantowany przez Unię.

Zasadniczo jakiekolwiek przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może mieć miejsce wyłącznie wtedy, gdy administratorzy i podmioty przetwarzające zastosują się do przepisów rozporządzenia. W stanowisku Rady w pełni uwzględniono orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej, w tym orzeczenie z dnia 6 października 2015 r. w sprawie C-362/14. Stanowisko Rady podtrzymuje różne podstawy transgranicznego przekazywania danych osobowych, a zarazem wzmacnia gwarancje poszanowania praw do ochrony danych. Podstawy przekazywania danych osobowych to: decyzja stwierdzająca odpowiedni stopień ochrony, odpowiednie zabezpieczenia oraz wyjątki.

Stanowisko Rady wyjaśnia, że wyrok sądu lub trybunału oraz decyzja organu administracyjnego państwa trzeciego wymagające od administratora lub podmiotu przetwarzającego przekazania lub ujawnienia danych osobowych mogą zostać uznane lub być egzekwowalne wyłącznie wtedy, gdy opierają się na umowie międzynarodowej obowiązującej między wzywającym państwem trzecim a Unią lub państwem członkowskim. Ponadto stanowisko Rady wyraźnie mówi, że takie umowy międzynarodowe pozostają bez uszczerbku dla innych podstaw przekazywania transgranicznego przewidzianych w rozporządzeniu.

6.2. **Decyzja stwierdzająca odpowiedni stopień ochrony**

Międzynarodowe przekazanie danych może nastąpić wtedy, gdy Komisja stwierdzi, że państwo trzecie – lub terytorium, lub określony sektor, lub określone sektory w tym państwie trzecim – lub dana organizacja międzynarodowa zapewniają stopień ochrony zasadniczo odpowiadający stopniowi gwarantowanemu przez Unię. Tym samym w całej Unii zagwarantowane zostają pewność prawa i jednorodność.

Komisja może zdecydować, wcześniej informując o tym państwo trzecie lub organizację międzynarodową i przedstawiając mu kompletne uzasadnienie, o cofnięciu takiej decyzji. Decyzję stwierdzającą odpowiedni stopień ochrony i decyzję o cofnięciu takiej decyzji Komisja przyjmuje jako akty wykonawcze. W aktach takich musi zostać przewidziany mechanizm okresowego przeglądu – przynajmniej raz na cztery lata. Komisja musi monitorować zmiany w państwach trzecich i organizacjach międzynarodowych mogące wpłynąć na obowiązywanie jej decyzji. Monitorując i dokonując okresowego przeglądu, Komisja powinna uwzględniać stanowisko i wnioski Parlamentu Europejskiego i Rady, a także innych odpowiednich organów i źródeł. W kontekście oceny i przeglądu rozporządzenia Komisja musi także regularnie przedstawiać sprawozdania Radzie i Parlamentowi Europejskiemu. Ponadto Europejska Rada Ochrony Danych musi wydawać na potrzeby Komisji opinie pozwalające ocenić odpowiedniość stopnia ochrony w państwie trzecim lub organizacji międzynarodowej, w tym ocenić, czy stopień ten nadal jest zapewniany.

Decyzje przyjęte przez Komisję na mocy art. 25 ust. 6 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia decyzją Komisji. Także zezwolenia udzielone przez państwo członkowskie lub organ nadzorczy na mocy art. 26 ust. 2 dyrektywy 95/46/WE oraz decyzje przyjęte przez Komisję na mocy art. 26 ust. 4 dyrektywy 95/46/WE pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia w razie potrzeby odpowiednio przez organ nadzorczy lub decyzją Komisji. Zapewniając ciągłość, stanowisko Rady gwarantuje pewność prawa.

6.3. **Odpowiednie zabezpieczenia**

Transgraniczne przekazywanie danych może się odbywać nie tylko na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, lecz także na podstawie odpowiednich zabezpieczeń ze strony administratora lub podmiotu przetwarzającego kompensujących brak ochrony danych w państwie trzecim lub organizacji międzynarodowej. Takie zabezpieczenia mogą mieć formę prawnie wiążących i egzekwowalnych instrumentów między organami lub podmiotami publicznymi, wiążących reguł korporacyjnych lub też standardowych klauzul ochrony danych przyjętych przez Komisję, standardowych klauzul ochrony danych przyjętych przez organ nadzorczy lub klauzul umownych dopuszczonych przez organ nadzorczy. Odpowiednie zabezpieczenia na potrzeby przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych mogą też zapewnić administratorzy lub podmioty przetwarzające w państwie trzecim. Mogą to uczynić poprzez zatwierdzone kodeksy postępowania wraz z wiążącymi i egzekwowalnymi zobowiązaniami do stosowania odpowiednich zabezpieczeń w drodze umownych lub innych prawnie wiążących instrumentów, w tym w odniesieniu do praw osób, których dane dotyczą. Może im do tego posłużyć również mechanizm certyfikacji zatwierdzony przez organ nadzorczy wraz z wiążącymi i egzekwowalnymi zobowiązaniami administratora lub podmiotu przetwarzającego w państwie trzecim do stosowania odpowiednich zabezpieczeń, w tym w odniesieniu do praw osób, których dane dotyczą.

6.4. **Wyjątki**

W razie braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń jednorazowe lub wielokrotne przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej może nastąpić na podstawie wyjątków, których pełna lista znajduje się w rozporządzeniu. Jednym z nich są prawnie uzasadnione interesy realizowane przez administratora, o ile charakteru nadrzędnego wobec nich nie mają interesy ani prawa i wolności osoby, której dane dotyczą. Aby zabezpieczenia przy transgranicznym przekazywaniu danych osobowych były dostateczne, prawnie uzasadnione interesy administratora są ściśle ograniczone i mogą być wykorzystywane tylko w ostateczności. Aby zapewnić spójne stosowanie rozporządzenia, Europejska Rada Ochrony Danych musi z własnej inicjatywy lub na wniosek Komisji opracować i weryfikować wytyczne, zalecenia i najlepsze praktyki w celu doprecyzowania kryteriów i wymogów przekazywania danych w przypadku braku decyzji stwierdzającej odpowiedni stopień ochrony lub braku odpowiednich zabezpieczeń.

7. ***Organy nadzorcze***

7.1. **Niezależność**

Aby chronić podstawowe prawa i wolności osób fizycznych w związku z przetwarzaniem ich danych osobowych oraz ułatwiać swobodny przepływ danych osobowych w Unii, każde państwo członkowskie musi zapewnić, by za monitorowanie stosowania rozporządzenia na jego terytorium odpowiadał co najmniej jeden niezależny organ publiczny. Każdy organ nadzorczy i jego członkowie muszą działać w sposób w pełni niezależny i uczciwy podczas wypełniania powierzonych im zadań i wykonywania powierzonych im uprawnień.

Każdy organ nadzorczy musi przyczyniać się do spójnego stosowania rozporządzenia w całej Unii. W tym celu organy nadzorcze muszą współpracować ze sobą, z Europejską Radą Ochrony Danych i z Komisją. Spójnemu stosowaniu rozporządzenia służy ponadto określenie właściwości organów nadzorczych oraz ich minimalnych zadań i uprawnień naprawczych, doradczych, w zakresie prowadzonych postępowań, i w zakresie wydawania zezwoleń.

7.2. **Tajemnica służbowa**

Stanowisko Rady zawiera przepisy o obowiązku zachowania tajemnicy służbowej przez organy nadzorcze i ich członków. Przede wszystkim członek lub członkowie oraz personel każdego z organów nadzorczych muszą podlegać zgodnie z prawem Unii lub prawem państwa członkowskiego obowiązkowi zachowania tajemnicy służbowej – w trakcie kadencji oraz po jej zakończeniu – w odniesieniu do wszelkich poufnych informacji, które uzyskali w toku wypełniania zadań lub wykonywania swoich uprawnień. Ponadto obowiązek zachowania tajemnicy służbowej w trakcie kadencji dotyczy zwłaszcza sytuacji, w których osoby fizyczne zgłaszają naruszenia rozporządzenia. Europejska Rada Ochrony Danych ma za zadanie wydawać wytyczne, zalecenia i najlepsze praktyki co do określania wspólnych procedur postępowania w przypadkach zgłaszania przez osoby fizyczne naruszeń rozporządzenia.

8. ***Współpraca i spójność***

8.1. **Europejska Rada Ochrony Danych**

Aby zapewnić poprawne i spójne stosowanie rozporządzenia, stanowisko Rady ustanawia Europejską Radę Ochrony Danych jako organ Unii mający osobowość prawną. Jej zadania polegają zwłaszcza na wydawaniu opinii, przyjmowaniu wiążących decyzji w ramach rozstrzygania sporów pomiędzy organami nadzorczymi czy wydawaniu wytycznych we wszelkich sprawach dotyczących stosowania rozporządzenia, aby zapewnić jego spójne egzekwowanie.

Do Europejskiej Rady Ochrony Danych należą: przewodniczący jednego organu nadzorczego każdego państwa członkowskiego i Europejski Inspektor Ochrony Danych lub ich przedstawiciele. Komisja ma prawo uczestnictwa w działaniach i posiedzeniach Europejskiej Rady Ochrony Danych, nie ma jednak prawa głosowania. Dyskusje Europejskiej Rady Ochrony Danych są poufne, jeżeli taką konieczność stwierdzi ona zgodnie ze swoim regulaminem wewnętrznym.

Jeżeli Europejska Rada Ochrony Danych przyjmuje wiążącą decyzję w ramach rozstrzygania sporu, Europejski Inspektor Ochrony Danych ma prawo głosowania wyłącznie względem decyzji co do zasad i przepisów, które mają zastosowanie do instytucji, organów i jednostek organizacyjnych Unii i merytorycznie odpowiadają przepisom rozporządzenia.

8.2. **Mechanizm spójności**

W przypadku transgranicznego przetwarzania danych osobowych, które dotyczy więcej niż jednego organu nadzorczego, mechanizm spójności gwarantuje, że podjęta zostanie jedna decyzja do zastosowania w całej Unii Europejskiej, a jednocześnie uwzględniona zostanie opinia organów nadzorczych, których sprawa dotyczy. W tym celu mechanizm „zmniejsza odległość" pomiędzy osobami, których dane dotyczą, a podejmującym decyzję organem nadzorczym, angażując w proces podejmowania decyzji lokalne organy nadzorcze. Ponadto w razie sporów między organami nadzorczymi z różnych państw członkowskich umocowana do podjęcia wiążących decyzji jest Europejska Rada Ochrony Danych.

Przepisy o mechanizmie spójności nie mają zastosowania, gdy przetwarzania dokonują organy publiczne lub podmioty prywatne działające w interesie publicznym. W takich przypadkach jedynym właściwym organem nadzorczym jest organ nadzorczy państwa członkowskiego, w którym organ publiczny lub podmiot prywatny mają jednostkę organizacyjną.

Stanowisko Rady przewiduje, że stosowanie mechanizmu współpracy i spójności przeanalizowane zostanie przy okazji przeprowadzanej przez Komisję oceny rozporządzenia.

9. ***Środki ochrony prawnej, odpowiedzialność i sankcje***

Stanowisko Rady zawiera szereg szczegółowych przepisów dających osobie, której dane dotyczą, kilka możliwości zastosowania środków ochrony prawnej, w tym dochodzenia odszkodowania, w razie gdyby w wyniku naruszenia rozporządzenia poniosła szkodę.

9.1. **Prawo do wniesienia skargi oraz prawo do środka ochrony prawnej przed sądem**

Stanowisko Rady przewiduje, że każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących nie jest zgodne z rozporządzeniem. Ponadto osoba taka ma prawo do skutecznego środka ochrony prawnej przed sądem przeciwko dotyczącej jej wiążącej decyzji organu nadzorczego. Ma też prawo do skutecznego środka ochrony, jeżeli organ nadzorczy nie rozpatrzył skargi lub nie poinformował jej o postępach lub efektach rozpatrywania skargi.

Każda osoba, której dane dotyczą, ma także prawo do skutecznego środka ochrony prawnej przed sądem, jeżeli uzna, że prawa przysługujące jej na mocy rozporządzenia zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem rozporządzenia.

„Bliska odległość" między osobą, której dane dotyczą, a sądem krajowym jest gwarantowana w ten sposób, że osoba ta ma prawo, by decyzja jej organu ochrony danych podlegała zaskarżeniu do jej sądu krajowego, niezależnie od tego, w którym państwie członkowskim jednostkę organizacyjną mają administrator lub podmiot przetwarzający. Postępowanie przeciwko administratorowi lub podmiotowi przetwarzającemu musi zostać wszczęte przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający mają jednostkę organizacyjną. Ewentualnie postępowanie takie może zostać wszczęte przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

Ponadto każda osoba fizyczna lub prawna ma prawo wnieść do Trybunału Sprawiedliwości Unii Europejskiej skargę o unieważnienie decyzji Europejskiej Rady Ochrony Danych na warunkach przewidzianych w art. 263 TFUE.

9.2. **Reprezentowanie osób, których dane dotyczą**

Osoba, której dane dotyczą, ma prawo umocować podmiot, organizację lub zrzeszenie, które spełniają szczegółowe kryteria, zwłaszcza działają na zasadzie non-profit w dziedzinie ochrony danych, do wniesienia w jej imieniu skargi oraz wykonywania w jej imieniu praw do środka ochrony prawnej przed sądem oraz do żądania w jej imieniu odszkodowania, jeżeli przewiduje to prawo państwa członkowskiego. Kryteria te mają zapobiec upowszechnieniu się zjawiska roszczeń handlowych w dziedzinie ochrony danych. Państwa członkowskie mogą również przewidzieć, że taki podmiot, organizacja lub zrzeszenie mają w tym państwie członkowskim prawo – niezależnie od upoważnienia otrzymanego od osoby, której dane dotyczą – wnieść skargę do właściwego organu nadzorczego oraz wykonać prawa do środka ochrony prawnej przed sądem, jeżeli uznają, że w wyniku przetwarzania danych osobowych z naruszeniem rozporządzenia naruszone zostały prawa osoby, której dane dotyczą.

9.3. **Zawieszenie postępowania**

Aby zapobiec temu, by ta sama sprawa przetwarzania danych przez tego samego administratora lub ten sam podmiot przetwarzający podlegała kontroli sądowej różnych sądów, każdy właściwy sąd inny niż sąd, przed którym jako pierwszym wszczęto postępowanie, może zawiesić swoje postępowanie lub – na wniosek jednej ze stron – stwierdzić brak swojej jurysdykcji.

9.4. **Prawo do odszkodowania i odpowiedzialność**

Stanowisko Rady przewiduje, że każda osoba, której dane dotyczą i która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo otrzymać od administratora lub podmiotu przetwarzającego odszkodowanie. Aby dać osobom, których dane dotyczą, możliwość dochodzenia odszkodowania w razie poniesienia szkody, a jednocześnie zagwarantować administratorom i podmiotom przetwarzającym pewność prawa, rozporządzenie określa ich odpowiedzialność. Każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody przez siebie spowodowane. Podmiot przetwarzający odpowiada wyłącznie wtedy, gdy nie dopełnił obowiązków, które rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom. Jednak administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

Jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczą w nim i administrator, i podmiot przetwarzający i odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni odpowiedzialność solidarną za całą szkodę, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania. Jeżeli jednak administrator lub podmiot przetwarzający zapłacili odszkodowanie za całą wyrządzoną szkodę, mają prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność.

9.5. **Sankcje**

Aby zapewnić przestrzeganie rozporządzenia, stanowisko Rady przewiduje, że ograny nadzorcze mogą nakładać administracyjne kary pieniężne. Muszą one być skuteczne, proporcjonalne i odstraszające. Państwa członkowskie mogą ustalić, czy i w jakim zakresie administracyjne kary pieniężne można nakładać na organy i podmioty publiczne ustanowione w tym państwie członkowskim. Poza nakładaniem administracyjnych kar pieniężnych organy nadzorcze mogą też wykonywać inne uprawnienia naprawcze, takie jak ostrzeżenia czy upomnienia. Dla większej harmonizacji Europejska Rada Ochrony Danych musi sporządzić wytyczne dla organów nadzorczych w sprawie wykonywania uprawnień naprawczych oraz ustalania administracyjnych kar pieniężnych.

Stanowisko Rady zawiera wykaz kryteriów, którymi mają się posługiwać organy nadzorcze, decydując, czy nakładać administracyjne kary pieniężne, a jeżeli tak – w jakiej wysokości. Kryteria te to m.in. charakter, waga i czas trwania naruszenia rozporządzenia lub umyślny lub nieumyślny charakter naruszenia. Rozporządzenie wymienia zarówno naruszenia, jak i odpowiadające im maksymalne administracyjne kary pieniężne. W ramach tych pułapów organ nadzorczy musi określić właściwą kwotę, zależnie od okoliczności naruszenia. Aby zagwarantować administratorom i podmiotom przetwarzającym pewność prawa i bardziej zharmonizować administracyjne kary pieniężne w Unii, a zarazem dać organom nadzorczym pewien margines swobody, naruszenia podzielono na trzy kategorie. Naruszenia pierwszej kategorii dotyczą obowiązków administratora i podmiotu przetwarzającego i podlegają administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR lub w przypadku przedsiębiorstwa – do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego (zastosowanie ma kwota wyższa). Naruszenia drugiej kategorii dotyczą praw osoby, której dane dotyczą, i podstawowych zasad przetwarzania i podlegają karze w wysokości maksymalnie 20 000 000 EUR lub 4% obrotu. Naruszenia trzeciej kategorii dotyczą nakazu orzeczonego przez organ nadzorczy i również podlegają karze w wysokości maksymalnie 20 000 000 EUR lub 4% obrotu.

10. ***Szczególne sytuacje związane z przetwarzaniem danych***

10.1. **Przetwarzanie danych osobowych a wolność wypowiedzi i informacji**

Państwa członkowskie muszą przewidzieć przepisy pozwalające pogodzić prawo do ochrony danych osobowych z prawem do wolności wypowiedzi i informacji, w tym do przetwarzania danych osobowych dla potrzeb dziennikarskich oraz do celów wypowiedzi akademickiej, artystycznej lub literackiej. Aby sposób wywiązywania się z tego obowiązku był przejrzysty, każde państwo członkowskie musi zawiadomić Komisję o stosownych przepisach, zmianach do nich oraz o wszelkich nowych przepisach.

10.2. **Przetwarzanie w kontekście zatrudnienia**

Państwa członkowskie mogą zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej szczegółowe przepisy mające zapewnić ochronę praw i wolności w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem.

Wśród przepisów tych muszą się znaleźć odpowiednie szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych. Każde państwo musi zawiadomić Komisję o stosownych przepisach, zmianach do nich oraz o wszelkich nowych przepisach.

10.3. **Zabezpieczenia i wyjątki mające zastosowanie do przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych**

Stanowisko Rady zawiera szczegółowe przepisy o przetwarzaniu danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych. Przepisy te mają godzić z jednej strony interes, którym jest udostępnianie danych osobowych na potrzeby archiwów, statystyki i badań naukowych, a z drugiej – ochronę danych.

Przetwarzanie danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych musi podlegać odpowiednim zabezpieczeniom dla praw i wolności osoby, której dane dotyczą, zgodnie z rozporządzeniem. Państwa członkowskie mają prawo przewidzieć – pod szczegółowymi warunkami i z zastrzeżeniem odpowiednich zabezpieczeń dla osób, których dane dotyczą – specyfikacje i wyjątki odnośnie do wymogów informacyjnych oraz prawa do sprostowania, usunięcia, bycia zapomnianym,

ograniczenia przetwarzania, przenoszenia danych oraz sprzeciwu, jeżeli przetwarzanie danych osobowych służy do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

Stanowisko Rady w przypadku przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych dopuszcza także wyjątek od zakazu przetwarzania danych wrażliwych. Taki wyjątek jest możliwy, o ile przetwarzanie jest oparte na prawie Unii lub prawie państwa członkowskiego, które muszą być proporcjonalne do wyznaczonego celu, przestrzegać istoty prawa do ochrony danych i przewidywać odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

11. ***Uprzednio zawarte umowy***

Stanowisko Rady precyzuje, że umowy międzynarodowe, które przewidują przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych i które zostały zawarte przez państwa członkowskie przed wejściem rozporządzenia w życie, i które są zgodne z prawem Unii mającym zastosowanie przed wejściem rozporządzenia w życie, pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia. Daje to administratorom pewność prawa, a państwom członkowskim zaoszczędza obciążeń administracyjnych. Bierze też pod uwagę, że w kwestii zmiany obowiązujących umów państwa członkowskie są po części zależne od państw trzecich czy organizacji międzynarodowych.

IV. **PODSUMOWANIE**

Stanowisko Rady w pierwszym czytaniu odzwierciedla kompromis wypracowany w nieformalnych negocjacjach między Radą a Parlamentem Europejskim przy udziale Komisji. Rada zwraca się do Parlamentu Europejskiego, by formalnie zatwierdził jej stanowisko bez poprawek, tak by można było ustanowić nowe unijne prawne ramy ochrony danych, zwiększające prawa do ochrony danych, a jednocześnie ułatwiające przepływ danych osobowych na rynku cyfrowym.