



**00530/12/PL
WP 191**

Opinia 01/2012 o projektach reformy ochrony danych

Przyjęta w dniu 23 marca 2012 r.

Grupa robocza została ustanowiona na mocy art. 29 dyrektywy 95/46/WE. Jest ona niezależnym europejskim organem doradczym w zakresie ochrony danych i prywatności. Zadania grupy określone są w art. 30 dyrektywy 95/46/WE i art. 15 dyrektywy 2002/58/WE.

Obsługę sekretariatu zapewnia Dyrekcja C (Prawa Podstawowe i Obywatelstwo Unii Europejskiej) Dyrekcji Generalnej ds. Sprawiedliwości, Wolności i Bezpieczeństwa Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

Strona internetowa: http://ec.europa.eu/justice/data-protection/index_en.htm

Spis treści

Wprowadzenie.....	4
Uwagi ogólne	4
W kwestii rozporządzenia	6
Pozytywne aspekty	6
Rola Komisji	7
Rola europejskich organów ochrony danych w kształtowaniu polityki.....	8
Progi dla MŚP	8
Wpływ na budżet i zasoby	9
Przepisy ogólne	9
Zasada publicznego dostępu do informacji.....	12
Dalsze wykorzystywanie niezgodne z pierwotnym celem.....	12
Wyjątki wprowadzone dla organów publicznych	12
Małoletni	14
Prawo do bycia zapomnianym	14
Marketing bezpośredni.....	15
Profilowanie	15
Przedstawiciel.....	15
Rozliczalność	16
Zgłaszanie naruszeń ochrony danych.....	17
W odniesieniu do roli i funkcjonowania OOG.....	18
Jurysdykcja i kompetencje OOD (punkt kompleksowej obsługi).....	19
Wzajemna pomoc	20
Zgodność	21
„Kompleksowy punkt obsługi” dla podmiotów danych	22
Struktura instytucyjna EROD.....	23
Transfery międzynarodowe.....	23
Ujawnianie danych niedozwolone w prawie UE	24
Prawo do dochodzenia odpowiedzialności i odszkodowania	24
Grzywny	25
Sądowe środki ochrony prawnej	26
Kościoły i związki wyznaniowe.....	27

W kwestii dyrektywy	27
Wybór instrumentów	27
Spójność	28
Zakres stosowania	28
Zasady przetwarzania danych	29
Prawa podmiotów danych	30
Obowiązki administratorów danych.....	31
Transfery międzynarodowe	32
Kompetencje OOD i współpraca.....	33
Braki	34

Wprowadzenie

Grupa robocza ds. ochrony danych ustanowiona na mocy art. 29 (Grupa Robocza lub G.R.29) przyjmuje z zadowoleniem projekty przyjęte przez Komisję Europejską mające na celu wzmocnienie pozycji osób, których dotyczą dane, zwiększenie odpowiedzialności administratorów oraz wzmocnienie pozycji organów nadzorczych, zarówno na szczeblu krajowym, jak i międzynarodowym. Po wprowadzeniu dalszych ulepszeń proponowane przepisy mogą znacząco ograniczyć obecne rozdrobnienie oraz wzmocnić ochronę danych w całej Europie.

Grupa robocza wyraża szczególne zadowolenie z powodu włączenia przepisów stanowiących zachętę do podejmowania przez administratorów wysiłków na rzecz zapewnienia odpowiedniego poziomu ochrony od samego początku (takich jak ocena skutków w zakresie ochrony danych, uwzględnianie ochrony danych już w fazie projektowania oraz ochrona danych jako opcja domyślna). Projekty jasno określają odpowiedzialność i rozliczalność podmiotów przetwarzających dane osobowe przez cały „cykl życia” informacji.

Grupa Robocza podkreśla znaczenie przepisów służących wyjaśnieniu i wzmocnieniu praw osób, których dotyczą dane, zwłaszcza poprzez wyjaśnienie pojęcia zgody, wprowadzenie zasady ogólnej przejrzystości oraz udoskonalonych mechanizmów ochrony prawnej. Również bardzo pozytywnie należy ocenić wprowadzenie obowiązku zgłaszania naruszenia ochrony danych, który zapewnia spójność w skali wszystkich sektorów.

Grupa Robocza uznaje za korzystne także to, że projekty harmonizują kompetencje organów nadzorczych, by mogły one skuteczniej zapewniać, i, w razie konieczności, egzekwować przestrzeganie przepisów, zarówno indywidualnie, jak i we wzajemnej współpracy, np. dzięki możliwości nakładania sporych kar finansowych.

Mimo ogólnej pozytywnej oceny proponowanego rozporządzenia, Grupa Robocza jest zdania, że niektóre jego części wymagają wyjaśnienia i udoskonalenia. Jeżeli chodzi o dyrektywę o ochronie danych w obszarze policji i wymiaru sprawiedliwości, grupa robocza jest rozczarowana zbyt mało ambitnym podejściem Komisji oraz podkreśla potrzebę ustanowienia lepszych przepisów.

Grupa Robocza uważnie przeanalizowała oba projekty, a niniejsza opinia stanowi pierwszą reakcję na nie. W opinii uwidatniono elementy budzące wątpliwości oraz, w odpowiednich przypadkach, przedstawiono zalecenia służące ich poprawie. W razie potrzeby w przyszłości Grupa Robocza może przedstawić dalsze opinie na temat konkretnych przepisów lub aspektów projektów.

Grupa Robocza wzywa Radę i posłów Parlamentu Europejskiego do skorzystania z możliwości udoskonalenia obu projektów oraz wzmocnienia ochrony danych w Unii Europejskiej.

Uwagi ogólne

Rozporządzenie stanowi realizację ambicji opracowania tekstu odzwierciedlającego zwiększone znaczenie ochrony danych w porządku prawnym UE (art. 16 Traktatu, art. 8 Karty). Zachowuje ono i wzmacnia zasadnicze zasady ochrony danych, nakłada jasne i

jednolite obowiązki na administratorów danych i podmioty przetwarzające dane, ułatwia swobodny przepływ danych osobowych oraz zapewnia wzmocnione ramy prawne na potrzeby jednolitego stosowania przepisów przez organy ochrony danych (OOD), których kompetencje zostały zwiększone.

Grupa Robocza jest rozczarowana tym, że jej opinie na temat kompleksowości nie doprowadziły do zaproponowania jednego instrumentu prawnego. Grupa Robocza odnotowuje, że Komisja ze względu na ograniczenia polityczne zdecydowała się przedstawić odrębny wniosek dotyczący dyrektywy mającej zastosowanie w obszarze policji i wymiaru sprawiedliwości w sprawach karnych. Tym bardziej konieczne jest, aby standardy ochrony danych mające zastosowanie także w tym obszarze, były spójne i prezentowały wysoki standard. W każdym razie powinno być jasne, że nowa dyrektywa nie może doprowadzić do obniżenia przez państwa członkowskie ich obecnych standardów w zakresie ochrony danych w sektorze policji i wymiaru sprawiedliwości w sprawach karnych. Poza tym nowe ramy prawne powinny być zgodne z innymi umowami międzynarodowymi, w tym konwencją Rady Europy nr 108 o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych i jej protokołem dodatkowym. Grupa Robocza proponuje zawarcie w preambule rozporządzenia i dyrektyw wyraźnego odniesienia do konwencji nr 108 i jej protokołu dodatkowego.

W swoich poprzednich opiniach Grupa Robocza podkreślała również potrzebę osiągnięcia kompleksowości ram prawnych. Z tego punktu widzenia dyrektywa wydaje się zbyt mało ambitna w porównaniu z rozporządzeniem. Fakt, że przedstawiono dwa instrumenty prawne nie przekreśla możliwości stworzenia kompleksowych ram prawnych, tak długo jak utrzymany będzie jednolity cel – osiągnięcie wysokiego poziomu ochrony danych obywateli Europy we wszystkich sektorach – a instrumenty zawierać będą jednolite podejście, między innymi do zasad ochrony danych, prawa osób, których dotyczą dane oraz obowiązków administratorów i podmiotów przetwarzających.

Konieczne jest podjęcie przez europejskiego prawodawcę istotnych wysiłków w toku procedury legislacyjnej, by zbliżyć materialne przepisy dyrektywy do przepisów zawartych w rozporządzeniu oraz zagwarantować spójność obu tekstów.

Ponadto instytucje UE powinny być związane tymi samymi przepisami, które mają zastosowanie na szczeblu państw członkowskich. Zatem by reforma była faktycznie kompleksowa, w momencie wejścia w życie rozporządzenia ramy ochrony danych obowiązujące instytucje Unii Europejskiej, ustanowione obecnie w rozporządzeniu (WE) nr 45/2001, powinny zostać uzgodnione z tym nowym rozporządzeniem.

To samo dotyczy obecnych szczególnych przepisów dotyczących przetwarzania danych w dawnym trzecim filarze UE, np. w odniesieniu do agencji UE, takich jak Europol i Eurojust. Grupa Robocza zwraca uwagę na możliwość wystąpienia trudności praktycznych z zaproponowaniem ogólnej rewizji obecnego dorobku prawnego, równocześnie jednak uważa, że należy ostatecznie dążyć do obowiązywania takiego samego poziomu ochrony danych we wszystkich operacjach przetwarzania danych w tym obszarze, w tym dokonywanych przez organy UE.

Równocześnie Grupa Robocza zwraca uwagę na zaangażowanie Komisji zmierzające do rewizji innych instrumentów prawnych, by ustalić potrzebę uzgodnienia w okresie trzech lat. Grupa Robocza zaleca prawodawcy wyznaczenie dużo krótszego terminu oraz wzywa

Komisję do faktycznego przedłożenia takich projektów. Grupa Robocza uznaje przy tym fakt, że obecne reżimy ochrony danych w niektórych obowiązujących instrumentach oraz organach sięgają dalej niż proponowana dyrektywa. Jak wspomniano, w przypadku państw członkowskich będących w podobnej sytuacji uzgodnienie obecnych reżimów z dyrektywą nie powinno w żadnym razie prowadzić do obniżenia obecnego standardu ochrony danych.

Z innej strony, Grupa Robocza wyraża rozczarowanie faktem, że ani w rozporządzeniu ani w dyrektywie nie podjęto kwestii gromadzenia i przekazywania przez podmioty prywatne lub organy publiczne niebędące organami ścigania danych faktycznie przeznaczonych do celów ochrony porządku publicznego, jak również późniejszego wykorzystywania tych danych przez organy ścigania. Szereg przykładów w ubiegłym dziesięcioleciu (tzn. PNR, zatrzymywanie danych telekomunikacyjnych) jasno pokazało konieczność ustanowienia rygorystycznych warunków, zwłaszcza gdy takie przetwarzanie ma charakter zorganizowany. Działa to również w odwrotną stronę: niezbędne są także zasady gwarantujące ochronę danych, gdy informacje są przekazywane przez organy ścigania lub inne „właściwe” organy sektorowi prywatnemu lub innym organom publicznym.

Na koniec należy stwierdzić, w odniesieniu do obu proponowanych instrumentów, że Grupa Robocza wyraża zaniepokojenie zakresem kompetencji Komisji do przyjmowania aktów delegowanych i wykonawczych. Grupa Robocza uznaje potrzebę zagwarantowania, by niektóre kwestie mogły zostać rozstrzygnięte na bardziej szczegółowym poziomie na późniejszym etapie, uważa jednak, że nie powinno mieć to miejsca np. w odniesieniu do przepisów dotyczących zgłoszeń naruszenia ochrony danych. Aby zagwarantować pewność prawa zasadnicze elementy powinny zostać włączone do samego rozporządzenia, zgodnie z treścią art. 290 TFUE.

W kwestii rozporządzenia

Pozytywne aspekty

- W ogólnym ujęciu rozporządzenie zapewnia większą jasność dzięki bardziej precyzyjnym definicjom oraz przepisom służącym zagwarantowaniu bardziej zharmonizowanego stosowania prawa, ułatwiając tym samym swobodny przepływ danych.
- Jeżeli chodzi o osoby fizyczne, rozporządzenie wzmacnia ich prawa, w tym poprzez zapewnienie większej przejrzystości, większej kontroli nad przetwarzaniem, minimalizację danych, szczególne przepisy dotyczące przetwarzania danych osobowych dzieci, wzmocnione prawo dostępu do danych, wzmocnione prawa wniesienia sprzeciwu, prawo do przenoszenia danych, wzmocnione prawa do usunięcia danych („prawo do bycia zapomnianym”) oraz wzmocnione prawo do środków ochrony prawnej zarówno za pośrednictwem OOD, jak i sądów.
- W odniesieniu do administratorów danych rozporządzenie prowadzi do uproszczenia i większej spójności, kładzie większy nacisk na ich rozliczalność za przetwarzane dane oraz potrzebę wykazania tego poprzez ochronę danych w fazie projektowania, domyślną ochronę danych, oceny skutków w zakresie prywatności, wyznaczanie inspektora ochrony danych (IOD), obowiązki w zakresie zgłaszania naruszenia

ochrony danych oraz przyjęcie ostrożnościowego podejścia w zakresie transferów międzynarodowych. Oprócz tego wiążące reguły korporacyjne zostają wyraźnie uznane za narzędzie służące do kształtowania ram transferów międzynarodowych.

- Jeśli chodzi o obowiązki w dziedzinie bezpieczeństwa spoczywające na podmiotach przetwarzających dane, to są one oparte na przepisach, a ponadto wprowadzono obowiązek przejścia odpowiedzialności administratora w przypadku konkretnych operacji przetwarzania danych, w ramach których podmiot przetwarzający wykracza poza instrukcje administratora w odniesieniu do danej operacji przetwarzania (dotyczy to dostawców oferujących „przetwarzanie w chmurze”).
- W odniesieniu do OOD rozporządzenie przewiduje większą niezależność i szersze kompetencje, w tym możliwość nakładania grzywien administracyjnych, oraz obowiązek konsultowania z nimi środków legislacyjnych, a także przepisy mające zagwarantować zharmonizowane stosowanie i, w razie potrzeby, niezbędne egzekwowanie prawa, w szczególności poprzez „mechanizm zgodności”.

Rola Komisji

Grupa Robocza ma poważne zastrzeżenia, co do zakresu kompetencji Komisji do przyjmowania aktów delegowanych i wykonawczych, co ma szczególne znaczenie w sytuacji, w której grę wchodzi jedno z praw podstawowych. Naturalnie niezbędne może okazać się pozostawienie możliwości rozstrzygania niektórych kwestii w aktach delegowanych lub wykonawczych. Jednak nie wszystkie kwestie, o których mowa w art. 86 i 87 mają jedynie charakter szczegółowy. Niektórych przepisów rozporządzenia (np. dotyczących zgłaszania naruszeń ochrony danych, wzajemnej pomocy, spójności i wyjątków od prawa do informacji i dostępu w kontekście przetwarzania danych do celów badań historycznych, statystycznych lub innych badań naukowych) nie da się stosować bez przyjęcia aktów delegowanych lub wykonawczych. Poza tym inne akty delegowane dotyczą przedmiotowego zakresu rozporządzenia, np. art. 6 ust. 1 lit. f) w związku z art. 6 ust. 5, który umożliwia Komisji zdefiniowanie „słuszných interesów” administratora w odniesieniu do konkretnych operacji przetwarzania i sektorów. Aby zagwarantować pewność prawa, zasadnicze elementy powinny zostać włączone do samego rozporządzenia, zgodnie z treścią art. 290 TFUE.

W praktyce przyjęcie aktów delegowanych lub wykonawczych na podstawie dużej liczby artykułów może zabrać wiele lat, co mogłoby doprowadzić do braku pewności prawa po stronie administratorów i podmiotów przetwarzających, którzy oczekują szybkiego wdrożenia rozporządzenia i konkretnych wytycznych. Na sam koniec Grupa Robocza wzywa Komisję do określenia, które akty delegowane i wykonawcze zamierza przyjąć w perspektywie krótko-, średnio- i długoterminowej.

Niezależnie od roli Komisji jako strażniczki Traktatów, Grupa Robocza ma także istotne zastrzeżenia odnośnie do roli przewidzianej dla Komisji w indywidualnych sprawach, rozstrzygniętych w ramach mechanizmu zgodności, ponieważ zagraża ona niezależnemu statusowi organów ochrony danych. Jeżeli sprawa rozstrzygana jest lub została rozstrzygnięta przy udziale Europejskiej Rady Ochrony Danych (EROD) w ramach mechanizmu zgodności, Komisja powinna mieć możliwość przedstawienia swojej oceny prawnej, jednak powinna powstrzymać się od dalszej ingerencji. Można byłoby przewidzieć procedurę umożliwiającą

Komisji i EROD zwrócenie się do Europejskiego Trybunału Sprawiedliwości o opinię na temat wykładni rozporządzenia.

Rola europejskich organów ochrony danych w kształtowaniu polityki

Grupa Robocza jest zdania, że istotna rola odgrywana przez nią dotychczas oraz rola, jaką Europejska Rada Ochrony Danych może odgrywać w przyszłości w zakresie kształtowania polityki (np. poprzez wydawanie wytycznych lub zaleceń) powinna znaleźć odzwierciedlenie w projektach.

W art. 66 zapisano, że EROD z własnej inicjatywy, lub na wniosek Komisji, doradza we wszelkich kwestiach związanych z ochroną danych osobowych oraz rozpatruje wszelkie pytania dotyczące zastosowania rozporządzenia. Zgodnie z interpretacją Grupy Roboczej obejmuje to również inne przepisy, dlatego zaleca ona dodanie w art. 66 ust. 1 lit. a) następującego zapisu: „oraz wszelkich dodatkowych lub szczególnych środków służących zabezpieczeniu prawa i wolności osób fizycznych w odniesieniu do przetwarzania danych osobowych oraz wszelkich zaproponowanych środków Unii wpływających na takie prawa i wolności”.

Poza tym Grupa Robocza zaleca stworzenie, nie tylko dla Komisji Europejskiej, lecz także Parlamentu Europejskiego, możliwości zapytania EROD o opinię, poprzez dodanie zapisu „i Parlamentu Europejskiego” w art. 66 ust. 1 lit. b).

Ponadto Grupa Robocza usilnie zaleca ustanowienie obowiązku konsultowania przez Komisję z EROD każdej decyzji stwierdzającej odpowiedni poziom ochrony (w art. 41) oraz standardowej klauzuli ochrony danych (w art. 42), jak również konsultowania z EROD kodeksów postępowania na szczeblu europejskim (w art. 38) i uzyskiwania zatwierdzenia ich z jej strony. W każdym zaś razie należy wprowadzić obowiązek konsultowania przez Komisję z EROD wszystkich aktów delegowanych i wykonawczych (w art. 86 i 87).

Organy krajowe powinny mieć w dalszym ciągu możliwość tworzenia wytycznych i zaleceń, które powinny zostać przekazane do mechanizmu zgodności, jeżeli mają istotny wpływ na inne państwa członkowskie. Powinny one również mieć możliwość monitorowania pieczęci i oznaczeń certyfikacyjnych mających chronić osoby fizyczne.

Progi dla MŚP

Grupa Robocza odnotowuje, że w całym rozporządzeniu wprowadzono wyjątki i progi mające ograniczyć obciążenia administracyjne i konsekwencje dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw (MŚP). Progi wprowadzono w przepisach dotyczących obowiązku wyznaczenia przedstawiciela w UE (art. 25), dokumentacji (art. 28 ust. 4) wyznaczenia IOD (art. 35 ust. 1) oraz nakładania grzywien administracyjnych (art. 79 ust. 3). Obok tego projekt przewiduje akty delegowane i wykonawcze umożliwiające Komisji uwzględnienie dodatkowych kwestii dotyczących MŚP w art. 12 ust. 6 o procedurach i mechanizmach korzystania z praw przez podmioty danych, art. 14 ust. 7 o obowiązku udzielania informacji podmiotom danych, art. 22 ust. 4 dotyczącym obowiązków dotyczących rozliczalności oraz art. 33 ust. 6 o przeprowadzaniu ocen skutków w zakresie ochrony danych.

Grupa Robocza wyraża opinię, że podmioty danych powinny korzystać z takiego samego poziomu ochrony, niezależnie od tego, czy ich dane przetwarzane są przez MMSP czy też duże przedsiębiorstwa. Równocześnie jednak uznaje fakt, że niektóre proponowane obowiązki mogą okazać się uciążliwe dla MMSP. Dlatego też, choć Grupa Robocza zasadniczo uznaje przyczyny wprowadzenia tych progów, wyraża obawę, że wprowadzone wyjątki mogą zarówno w praktyce, jak i w stosunku do ochrony danych osobowych, prowadzić do niespójnych wyników i niepożądanych rezultatów. Grupa Robocza jest zdania, że bardziej odpowiedni byłby próg uwzględniający charakter i zakres przetwarzania danych.

Wpływ na budżet i zasoby

Grupa Robocza z zadowoleniem przyjmuje fakt, że w projektach uznano istotną rolę, jaką OOG mogą odebrać w zapewnieniu zgodności poprzez zwiększenie obowiązków ciążących zarówno na OOG, jak i EDOR. Grupa Robocza ma jednak przy tym poważne wątpliwości, czy dostatecznie uwzględniono istotne konsekwencje budżetowe tych zwiększonych obowiązków. Aby odpowiednio wyposażać OOG i EDOR, by mogły skutecznie wykonywać swoje obowiązki, w tym zadania związane z wzajemną współpracą i pomocą w ramach mechanizmu zgodności, państwa członkowskie muszą być gotowe do zapewnienia odpowiednich zasobów finansowych, ludzkich i technicznych.

W tym kontekście Grupa Robocza usilnie zaleca przeprowadzenie wnikliwej oceny zwiększonych kosztów dla OOG i Europejskiego Inspektora Ochrony Danych (jako zapewniającego obsługę sekretariatu dla EDOR) w oparciu o obecne projekty. Na podstawie wyników takiej oceny należało będzie wyjaśnić co stanowi „odpowiednie zasoby ludzkie, techniczne i finansowe, pomieszczenia i infrastrukturę” dla OOG, wymienione w art. 47 ust. 5.

Grupa Robocza zamierza skontaktować się z Komisją w sprawie celów i parametrów takiej oceny skutków w odrębnym piśmie.

Przepisy ogólne

Zakres

Zgodnie z art. 3 ust. 2 rozporządzenie ma zastosowanie także do przetwarzania danych osobowych podmiotów danych mających miejsce zamieszkania w Unii przez administratora niemającego siedziby w Unii, gdy przetwarzanie wiąże się z oferowaniem towarów lub usług takim podmiotom danych w Unii lub monitorowaniem ich zachowania.

Niezależnie od prób zdefiniowania tego, co należy rozumieć przez „oferowanie towarów i usług” oraz „monitorowanie ich zachowania” w motywach, Grupa Robocza ma wrażenie, że konieczne jest dalsze wyjaśnienie tych pojęć.

Należy jednoznacznie przewidzieć, że „oferowanie towarów i usług” obejmuje także usługi darmowe (w przypadku których osoby fizyczne faktycznie płacą za usługę przekazując swoje dane osobowe). Grupa Robocza zaleca zatem dodanie zapisu o następującym brzmieniu „w tym usług świadczonych bez kosztów finansowych dla osoby fizycznej”.

Ponadto w motywie 21 sugeruje się, że „monitorowanie zachowania” wiąże się ze śledzeniem w Internecie oraz tworzeniem profili. Grupa robocza doradza zmianę tego sformułowania w celu zagwarantowania, by nawet w sytuacjach, w których administrator nie tworzy profili jako takich, operacje przetwarzania mogły być niekiedy uznawane za „monitorowanie zachowania”, jeżeli prowadzą do decyzji dotyczących podmiotów danych lub wiążą się z analizowaniem lub przewidywaniem ich osobistych preferencji, zachowań i postaw.

Podmiot danych i dane osobowe

Grupa Robocza z zadowoleniem przyjmuje definicję „podmiotu danych” w art. 4 ust. 1 proponowanego rozporządzenia, który stanowi, że „podmiot danych oznacza zidentyfikowaną osobę fizyczną lub osobę fizyczną, którą można zidentyfikować...”. Osoba fizyczna może być uznawana za możliwą do identyfikacji w grupie osób, jeżeli można ją odróżnić od innych członków grupy, a tym samym traktować inaczej. Podejście to zostało określone we wcześniej przyjętej opinii Grupy Roboczej na temat koncepcji danych osobowych (WP136). Motyw 23 należy zatem zmienić w celu doprecyzowania, że pojęcie identyfikowalności obejmuje również taki sposób wyodrębnienia.

Motyw 24 dotyczący definicji danych osobowych przewiduje, że numery identyfikacyjne, dane o lokalizacji, identyfikatory online oraz inne szczególne czynniki nie muszą być uznawane za dane osobowe we wszystkich okolicznościach. W swoim obecnym brzmieniu ostatnie zdanie może prowadzić od nienależycie restrykcyjnej wykładni pojęcia danych osobowych np. w odniesieniu do adresów IP lub identyfikatorów opartych na „cookies”. Grupa Robocza przypomina, że dane osobowe to dane dotyczące możliwej do identyfikacji osoby fizycznej. „Dane dotyczą osoby, jeżeli odnoszą się do tożsamości, cech lub zachowania danej osoby lub też jeśli informacje te determinują lub też wpływają na sposób traktowania lub ocenę danej osoby¹”. Grupa Robocza przedstawiła już w swojej opinii WP136 różne scenariusze uzasadniające, dlaczego adresy IP powinny być traktowane jako należące do identyfikowalnych osób fizycznych: „zwłaszcza w przypadkach, gdy przetwarzanie adresów IP ma na celu zidentyfikowanie użytkowników komputera (na przykład przez posiadaczy praw autorskich w celu ścigania użytkowników za pogwałcenie praw autorskich) (...)”. W tym przypadku, jak również w przypadku „cookies”, administrator przewiduje, że „sposoby, jakimi można się posłużyć” będą dostępne w celu identyfikacji osób oraz traktowania ich w określony sposób². Dlatego Grupa Robocza zaleca odpowiednią zmianę art. 24.

Dane biometryczne

Grupa Robocza z zadowoleniem przyjmuje wprowadzenie definicji danych biometrycznych w art. 4 ust. 11 rozporządzenia. Tym niemniej ma ona zastrzeżenia do obecnego sformułowania, w którym skoncentrowano się na kwestii umożliwienia identyfikacji osoby fizycznej. Dane biometryczne wykorzystywane są nie tylko do celów identyfikacyjnych, lecz również na potrzeby uwierzytelniania (w celu sprawdzenia tożsamości bez faktycznej identyfikacji osoby fizycznej). Definicja ta powinna zostać zmieniona celem położenia akcentu na tym, jakie rodzaje danych mają być uznawane za dane biometryczne, nie zaś na tym, co umożliwiają. Grupa Robocza zaleca zatem zmianę brzmienia art. 4 ust. 11 z „umożliwiają jej precyzyjną identyfikację...” na „są unikalne u każdej osoby fizycznej...”.

Główna siedziba

¹ WP136, s. 10.

² WP136, s. 16.

Sposób, w jaki ma być podejmowana decyzja o tym, gdzie wielonarodowa spółka (należąca do podmiotu z UE lub spoza niej) ma swój główny zakład, zdefiniowany w art. 4 ust. 13 oraz w motywie 27, wymaga dalszego wyjaśnienia, w tym w przypadkach, gdy spółka ta ma odrębne podmioty prawne działające w różnych sektorach. Pod uwagę można wziąć przykładowo „dominujący wpływ” jednego zakładu na operacje przetwarzania w odniesieniu do przepisów dotyczących ochrony danych.

Grupa Robocza odnotowuje fakt, że w art. 4 projektu rozporządzenia zawarte są różne definicje jednostek biznesowych, między którymi brakuje wyraźnych różnic. Pojęcia „administratora” i „głównej siedziby” odnoszą się z jednej strony do tego, gdzie podejmowane są istotne decyzje w sprawie przetwarzania danych, z drugiej zaś strony w definicjach „przedsiębiorstwa” i „grupy przedsiębiorstw” mowa jest o działalności gospodarczej i strukturze korporacyjnej.

Wprowadzono dodatkowy termin odnoszący się do podmiotów przetwarzających – główna siedziba ma być miejscem, w którym znajduje się „zarząd”. Ponadto w rozdziale VIII dotyczącym środków ochrony prawnej, odpowiedzialności i sankcji w kontekście ustalenia właściwego sądu w postępowaniu przeciwko administratorowi lub podmiotowi przetwarzającemu następuje odniesienie do jakiejkolwiek siedziby, niezależnie od tego, czy dany zakład ma coś wspólnego z przedmiotowymi operacjami przetwarzania (co więcej w sensie prawnym może być on całkowicie niezależny od innych zakładów administratora/podmiotu przetwarzającego).

Zdaniem Grupy Roboczej definicje te pokrywają się wzajemnie i dlatego należy je doprecyzować. W każdym zaś razie należy wyraźnie zaznaczyć, jaki jest związek między główną siedzibą a odpowiedzialnością administratora.

Definicja głównej siedziby wydaje się służyć przede wszystkim ustalaniu, który OOD powinien przejąć funkcję wiodącą w określonej sprawie lub w odniesieniu do konkretnego przedsiębiorstwa. Jasne pojmowanie pojęcia „główna siedziba” ma zasadnicze znaczenie, ponieważ przesądza o ustaleniu organu wiodącego w rozumieniu art. 51 ust. 2, w przypadkach, w których przetwarzanie danych osobowych odbywa się w kontekście działalności zakładu administratora lub podmiotu przetwarzającego w Unii, a administrator lub podmiot przetwarzający prowadzą działalność w więcej niż jednym państwie członkowskim (zob. także na s. 25).

Pseudonimizacja

Grupa Robocza uważa, że pojęcie pseudonimizacji powinno być wprowadzone do dokumentu w sposób bardziej wyraźny (np. poprzez dodanie definicji danych poddanych pseudonimizacji, spójnej z definicją danych osobowych), ponieważ może to pomóc w osiągnięciu lepszej ochrony danych, przykładowo w kontekście ochrony danych już w fazie projektowania i ochrony danych jako opcji domyślnej. Grupa Robocza zaleca zatem wprowadzenie ogólnego obowiązku anonimizacji lub pseudonimizacji danych osobowych, tam gdzie jest to wykonalne i proporcjonalne w stosunku do celu przetwarzania. Taka zasada może być wprowadzona w art. 5 oraz w kontekście ochrony danych już w fazie projektowania i ochrony danych jako opcji domyślnej w art. 23.

Ochrona danych już w fazie projektowania i ochrona danych jako opcja domyślna

Grupa Robocza z zadowoleniem przyjmuje wprowadzenie w art. 23 zasad ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej, doradza jednak bliższe wyjaśnienie ich znaczenia w jednym z motywów, np. poprzez zaznaczenie, że elementy produktu lub usług sprzyjające prywatności powinny być aktywowane automatycznie i że należy wdrożyć odpowiednie procedury na etapie projektowania operacji przetwarzania danych lub produktu. Naturalnie to administrator powinien wykazać, że w operacjach przetwarzania uwzględniono koncepcje ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej, które stanowią odpowiednie środki w kontekście art. 22 ust. 1.

Grupa Robocza zwraca uwagę na fakt, że Komisja uprawniona jest do ustanawiania norm technicznych w tym zakresie. Grupa Robocza głęboko przekonana, że Komisja powinna włączyć do opracowywania takich norm EROD i międzynarodowe organizacje normalizacyjne oraz we właściwych przypadkach prowadzić z nimi konsultacje.

Zasada publicznego dostępu do informacji

W motywie 18 stwierdzono, że rozporządzenie pozwala na uwzględnienie zasady publicznego dostępu do dokumentów urzędowych przy stosowaniu przepisów tego rozporządzenia. Ponieważ zasada publicznego dostępu do dokumentów urzędowych to utrwalone i istotne prawo podstawowe, powinno ono zostać nie tylko wymienione w motywie, lecz także wyrażone w jednym z artykułów rozporządzenia.

Dalsze wykorzystywanie niezgodne z pierwotnym celem

Artykuł 6 ust. 4 wprowadza możliwość dalszego przetwarzania danych w celach niezgodnych z pierwotnym celem w przypadkach, w których można ku temu znaleźć inną podstawę prawną (z wyjątkiem słusznego interesu administratora). Chociaż Grupa Robocza nie kwestionuje potrzeby pozostawienia możliwości dalszego przetwarzania danych dla innych celów, obecnie proponowane przepisy otwierają możliwość dalszego wykorzystywania danych do celów niezgodnych z pierwotnym celem, które mogą, zarówno w sektorze publicznym, jak i prywatnym i zwłaszcza gdy opierają się na lit. b) – wykonanie umowy oraz lit. e) – interes publiczny, prowadzić do wysoce niepożądanych rezultatów. Zdaniem Grupy Roboczej przepis ten jest sprzeczny z ogólną zasadą celowości, która stanowi jeden z fundamentów ochrony danych w Europie, i dlatego usilnie zaleca skreślenie art. 6 ust. 4 lub nadanie mu bardziej precyzyjnego brzmienia, z odniesieniem do art. 21. W tym kontekście Grupa Robocza pragnie również zwrócić uwagę na fakt, że podda bardziej dogłębnej analizie kwestię wykorzystywania danych zgodnie z pierwotnym celem jeszcze w 2012 r., zgodnie ze swoim programem prac na lata 2012-2013.

Wyjątki wprowadzone dla organów publicznych

Jedną z przyczyn rewizji ram ochrony danych jest dążenie do zapewnienia kompleksowości. Dzięki ustanowieniu jednego zestawu przepisów do stosowania zarówno w sektorze publicznym, jak i prywatnym, ramy prawne powinny zwiększać bezpieczeństwo prawne i

pewność prawa w odniesieniu do gwarancji ochrony danych obowiązujących we wszystkich sektorach, w szczególności w odniesieniu do osób fizycznych.

Grupa Robocza już wcześniej wyraziła rozczarowanie brakiem ambicji w obszarze policji i wymiaru sprawiedliwości. Jednak również w samym rozporządzeniu sektor publiczny uzyskuje specjalny status. Grupa Robocza jest zaniepokojona faktem, że w wielu częściach rozporządzenia wprowadzono obszerne wyjątki dla organów publicznych motywując je interesem publicznym. Grupa Robocza uważa obszerne i niedookreślone wyjątki, którym nie towarzyszą odpowiednie gwarancje, za nieuzasadnione. Dlatego też sugeruje ustalenie w rozporządzeniu na tyle, na ile to możliwe, konkretnego interesu publicznego. Przyczyniłoby się to również do harmonizacji w obrębie UE.

Jak wspomniano powyżej art. 6 ust. 4 wprowadza także dla organów publicznych bardzo obszerne możliwości zmiany pierwotnego celu postępowania na inny niezgodny z nim cel. Oprócz tego art. 9 ust. 2 lit. g) umożliwia przetwarzanie danych szczególnie chronionych na potrzeby zadań realizowanych „w interesie publicznym”. To samo dotyczy wyjątków ustanowionych w art. 17 ust. 5, w szczególności w odniesieniu do interesu publicznego i interesu osób trzecich. Grupa Robocza zaleca ograniczenie tego wyjątku do „realizacji istotnego interesu publicznego”.

Ponadto art. 21 przewiduje możliwość ograniczenia obowiązywania zasad ochrony danych i praw podmiotów danych, rozszerzając tym samym możliwość wprowadzenia ograniczeń w porównaniu z obecną sytuacją, bez zapewnienia odpowiednich gwarancji, których należałoby przestrzegać przy powoływaniu się na ten artykuł. Ponadto art. 21 ust. 1 lit. c) może być przywoływany w celu zabezpieczenia otwartej kategorii „innych publicznych interesów”. Grupa Robocza uważa, że jest to zbyt szerokie ujęcie, dlatego usilnie zaleca skreślenie fragmentu „innych interesów publicznych Unii lub państwa członkowskiego...” w art. 21 ust. 1 lit. c) i rozpoczęcie go sformułowaniem „ważnego interesu gospodarczego lub finansowego...”.

Artykuł 33 ust. 5 wprowadza dla organów publicznych wyjątek od obowiązku przeprowadzania ocen skutków w zakresie ochrony danych, gdy przetwarzanie wynika z obowiązku prawnego. W opinii Grupy Roboczej jedynym wyjątkiem, który mógłby zostać uznany za uzasadniony w tym kontekście to sytuacja, w której w procesie legislacyjnym przeprowadzono już wcześniej ocenę skutków w zakresie ochrony danych.

Grupa Robocza jest głęboko przekonana, że ogólne wyjątki dla sektora publicznego są nieuzasadnione i szkodzą kompleksowości ram prawnych, dlatego zdecydowanie zaleca, by w możliwym zakresie sektor publiczny i prywatny były traktowane w ten sam sposób i by były zobowiązane do przestrzegania tego samego zestawu norm. Należy jednak także ostrzec, że nowe ramy prawne mogą prowadzić do sytuacji, w której ochrona danych już osiągnięta w państwach członkowskich w różnych dziedzinach zostanie osłabiona. Szczególnie w sektorze publicznym poziom ochrony danych jest zróżnicowany ze względu na tradycje i przemiany konstytucyjne i prawne. Nowe ramy prawne powinny zatem zapewnić zharmonizowane standardy w tym obszarze, stwarzając zarazem możliwość dalszego uszczegółowienia przez państwa członkowskie (tak jak przewidziano to już w rozdziale IX), jednak bez uszczerbku dla rozporządzenia. Oznacza to także, że mogłyby one uzupełniać rozporządzenie.

Małoletni

Grupa Robocza uznaje znaczenie zasady „najlepszego zabezpieczenia interesów dziecka” oraz pojęcie progresywnej ochrony stosownie do stopnia dojrzałości³. Chociaż rozporządzenie nie wkracza na obszar przepisów dotyczących ważności, zawierania lub skutków umów w odniesieniu do dzieci w ogólnym prawie umów państw członkowskich, Grupa Robocza z zadowoleniem przyjmuje fakt, że w kontekście oferowania usług społeczeństwa informacyjnego skierowanych do dzieci art. 8 ust. 1 stanowi, że przetwarzanie danych osobowych dziecka w wieku poniżej 13 lat jest zgodne z prawem jedynie za zgodą lub zezwoleniem rodzica lub opiekuna dziecka.

Grupa Robocza ma świadomość trudności z harmonizacją limitów wiekowych w takim instrumencie i rozumie, że w czysto krajowych przypadkach powinno mieć zastosowanie prawo państwa członkowskiego. Grupa Robocza sugeruje jednak rozszerzenie zakresu wprowadzonej w rozporządzeniu reguły minimalnej dotyczącej sposobu traktowania małoletnich na inne kwestie, poza oferowaniem usług społeczeństwa informacyjnego, ponieważ jest więcej sytuacji, w których można by przewidzieć szczególne przepisy.

Ogólnie w rozporządzeniu brakuje przepisów dotyczących sposobu wykonywania praw przez przedstawiciela, nie tylko w przypadku małoletnich, lecz także w odniesieniu do reprezentowania osób pozbawionych zdolności do czynności prawnych oraz przez zastępstwo przez adwokatów.

Prawo do bycia zapomnianym

Grupa Robocza z zadowoleniem przyjmuje specjalne włączenie do rozporządzenia prawa do bycia zapomnianym i do usunięcia danych jako metodę wzmocnienia kontroli osób fizycznych na ich danymi osobowymi. Jednak sposób w jaki prawa te zostały skonfigurowane przez rozporządzenie oraz realne funkcjonowanie internetu mogą znacząco ograniczyć ich skuteczność.

Administrator odpowiada nie tylko za usunięcie danych, lecz także za poinformowanie osób trzecich, które przetwarzają te dane za pośrednictwem linków, kopii lub replik, o żądaniu podmiotu danych. Nałożenie tego obowiązku jedynie na administratora wiąże się z ograniczeniami, ponieważ mogą zachodzić przypadki, w których administrator podjął wszelkie rozsądne kroki by poinformować osoby trzecie, jednak nie jest świadomy istnienia wszystkich kopii lub replik albo przypadki, w których nowe kopie lub repliki pojawiają się po tym, gdy administrator poinformował wszystkie osoby trzecie. Co ważniejsze żaden z przepisów rozporządzenia nie wydaje się zobowiązywać osób trzecich do spełnienia żądania podmiotu danych, chyba że on także zostanie uznany za administratorów.

Rozporządzenie nie zawiera żadnych wskazówek co do tego, w jaki sposób podmioty danych mogą wykonywać swoje prawa, jeżeli administrator przestał istnieć, zniknął, lub nie można go zidentyfikować albo nawiązać z nim kontaktu. Dlatego też należy wyjaśnić status osób trzecich przetwarzających dane w celu określenia warunków, na jakich mają one spełnić

³ Zob. opinię 2/2009 w sprawie ochrony danych osobowych dzieci (WP 160) oraz dokument roboczy 1/2008 o ochronie danych osobowych dzieci (WP 147).

żądanie podmiotu danych oraz w jakim charakterze wtedy występują, a także określić konsekwencje zignorowania tego żądania.

Z tych samych przyczyn należy rozważyć rozszerzenie prawa podmiotów danych, by umożliwić im bezpośrednie kierowanie żądania usunięcia danych do osób trzecich, w przypadku gdy nie można tego uczynić za pośrednictwem administratora.

Na koniec należy stwierdzić, że żaden mechanizm nie przewiduje usunięcia linków, kopii lub replik danych, które nie zostały usunięte zgodnie z art. 17 ust. 3, ale które same w sobie nie należą do zakresu tego artykułu. Takie linki, kopie lub repliki mogą jednak ułatwiać dostęp do oryginalnej treści, co niekoniecznie musi być uzasadnione na mocy wspomnianego artykułu. Naturalnie Grupa Robocza uznaje potrzebę wyważenia prawa do prywatności i prawa do swobody wypowiedzi. Rozporządzenie powinno wyjaśnić związek między art. 17 ust. 3 a obowiązkiem przewidzianym w art. 17 ust. 2.

Marketing bezpośredni

Niezależnie od art. 19 ust. 2 rozporządzenia, który przewiduje prawo sprzeciwienia się przetwarzaniu danych na potrzeby marketingu bezpośredniego, Grupa Robocza podkreśla, że przepisy dyrektywy 2002/58/WE mają w dalszym ciągu pełne zastosowanie, tak jak to zresztą przewidziano w art. 89 rozporządzenia. Dotyczy to w szczególności internetowej reklamy behawioralnej oraz marketingu za pośrednictwem poczty elektronicznej.

Profilowanie

Grupa Robocza popiera przepisy rozporządzenia dotyczące profilowania. Ma jednakże wątpliwości, czy przyjęte podejście wystarczy do uwzględnienia problematyki tworzenia i wykorzystywania profili, w szczególności w środowisku online. Poza tym Grupa Robocza zwraca uwagę, że pojęcie „istotnego wpływu” z art. 20 ust. 1 jest nieścisłe. Należy je sprecyzować, by obejmowało również np. stosowanie narzędzi analizujących wykorzystanie internetu, śledzenie w celu oceny naszego zachowania, tworzenie profili ruchu przez mobilne aplikacje lub tworzenie profili osobowych przez sieci społecznościowe.

Ponadto zakres tego przepisu nie powinien ograniczać się wyłącznie do całkowicie automatycznego przetwarzania, lecz powinien obejmować także metody przetwarzania częściowo zautomatyzowane. Zdaniem Grupy Roboczej należy przyjąć podejście, w którym jasno zdefiniowany zostanie cel, dla którego profile mogą być tworzone i wykorzystywane, w tym szczególne obowiązki administratorów w zakresie informowania podmiotów danych, w szczególności o prawie do sprzeciwienia się tworzeniu i wykorzystywaniu profili.

Przedstawiciel

Grupa Robocza jest zdania, że należy bliżej wyjaśnić rolę i obowiązki przedstawiciela określone w art. 25. Należy wyjaśnić, jaka jest rola przedstawiciela w stosunku do podmiotów danych, sądów i OOD, w szczególności uwzględniając fakt, że art. 79 ust. 6 lit. f) przewiduje najwyższe możliwe grzywny w przypadku braku wyznaczenia przedstawiciela. Należy sprecyzować mandat przedstawiciela w celu jasnego określenia zakresu jego misji, roli i odpowiedzialności.

Artykuł 78 ust. 2 stanowi, że w przypadku wyznaczenia przez administratora przedstawiciela, wszelkie kary mają być nakładane na przedstawiciela. Tę samą jasność należy zapewnić w przypadku kar administracyjnych orzekanych zgodnie z art. 79. Ze sformułowania „organ nadzorczy może się do niego zwracać” użytego zarówno w motywie 63, jak i w art. 4 ust. 14 nie wynika wystarczająco jasno, że na przedstawiciela można nałożyć również karę administracyjną w rozumieniu art. 79.

Należy również wyjaśnić, że posiadanie przez przedstawiciela siedziby w UE zgodnie z treścią art. 25 ust. 3, który brzmi: „ma siedzibę w jednym z państw członkowskich”, **nie** oznacza uruchomienia mechanizmu głównej siedziby przewidzianego w art. 4 ust. 13 w tym sensie, że **nie** odgrywa ona **decydującej** roli w ustaleniu wiodącego OOD z art. 51 ust. 2.

W odniesieniu do wyjątków od obowiązku wyznaczenia przedstawiciela Grupa Robocza nie widzi żadnego istotnego powodu, by wykluczyć administratora z państwa trzeciego zapewniającego odpowiedni poziom ochrony. Fakt, że państwo trzecie ma odpowiedni poziom ochrony danych nie sprawia, że mniej potrzebne staje się posiadanie punktu kontaktowego w Unii Europejskiej, dlatego Grupa Robocza zaleca skreślenie art. 25 ust. 2 lit. a).

Jeżeli mają być wprowadzone wyjątki od obowiązku wyznaczenia przedstawiciela, powinny one opierać się na charakterze i zakresie przetwarzania danych osobowych, jak również (potencjalnej) liczbie podmiotów danych w UE, których może to dotyczyć. Obecny próg liczby osób zatrudnianych przez administratora niesie ze sobą ryzyko wykluczenia małych organizacji prowadzących operacje przetwarzania stwarzające zagrożenie dla osób fizycznych. Podobnie, niezależnie od wyjaśnienia w motywie 64 sformułowania „oferowanie towarów i usług tym osobom, **stanowi działalność dodatkową do działalności głównej**” jest zbyt nieprecyzyjne i w praktyce może często prowadzić do błędnej interpretacji.

Rozliczalność

Grupa Robocza z dużym zadowoleniem przyjmuje wprowadzenie w rozporządzeniu zasady rozliczalności, szczególnie w art. 22, oraz zdecydowanie akceptuje cel wdrożenia skutecznych procedur i mechanizmów skoncentrowanych na tych operacjach przetwarzania, które mogą nieść ze sobą szczególne zagrożenia dla praw i wolności podmiotów danych. Tym niemniej Grupa Robocza ma pewne wątpliwości odnośnie do artykułów mających sprecyzować ogólną zasadę.

Po pierwsze należy zagwarantować odpowiednią skalę. Przy realizacji zasady rozliczalności powinna istnieć możliwość uwzględnienia rozmiarów administratora oraz charakteru działalności związanej z przetwarzaniem. Ponadto organy nadzoru powinny zyskać możliwość analizowania wdrożonych mechanizmów rozliczalności przy nakładaniu sankcji i grzywien.

Dodatkowo art. 28 przewiduje obowiązek prowadzenia przez administratora dokumentacji wszystkich operacji przetwarzania odbywających się pod jego nadzorem. Artykuł 28 ust. 2 określa, jakich konkretnie dokumentów to dotyczy. Obowiązek ten współgra z ogólnym zobowiązaniem do bycia rozliczanym z art. 22, na mocy którego administratorzy zobowiązani są do zapewniania *możliwości wykazania*, jakie polityki zostały przyjęte i jakie środki zostały wdrożone w celu zapewnienia zgodności. Zasadniczo każdy administrator, podmiot przetwarzający oraz ewentualny przedstawiciel administratora powinien być

zobowiązany do prowadzenia podstawowej dokumentacji wszystkich swoich operacji przetwarzania.

Chociaż Grupa Robocza z zadowoleniem przyjmuje obowiązek oceny skutków w zakresie ochrony danych przewidziany w art. 33, ma wrażenie że ocena ta powinna naturalnie zostać przeprowadzona także wtedy, gdy nie ma jasności, czy przetwarzanie może powodować konkretne zagrożenia dla praw i wolności podmiotów danych. Grupa Robocza zaleca zatem uzgodnienie art. 33 ust. 1 z motywem 70 oraz proponuje dodanie słów „mogą przypuszczalnie”, tak by pierwsze zdanie tego artykułu brzmiało „Jeśli operacje przetwarzania **mogą przypuszczalnie** stwarzać szczególne ryzyko dla praw i wolności podmiotów...”.

Grupa Robocza uważa, że wyjątki przewidziane w art. 28 ust. 4 lit. b) o dokumentacji i art. 35 ust. 1 lit. b) o wyznaczaniu OOG mogą mieć niezamierzone konsekwencje, w szczególności gdy mała organizacja zatrudniająca mniej niż 250 pracowników przetwarza dużo danych osobowych lub dane operacje przetwarzania są ze swej natury ryzykowne. Podobnie obecnie sformułowanie w sposób nieproporcjonalny obciąża duże organizacje przetwarzające ograniczą ilość danych osobowych. Grupa Robocza jest zdania, że zamiast łącznej liczby pracowników firmy, należałoby raczej wziąć pod uwagę charakter i zakres przetwarzania danych osobowych, jak również liczbę pracowników bezpośrednio zaangażowanych w przetwarzanie danych osobowych oraz liczbę podmiotów danych.

Grupa Robocza uważa, że operacje przetwarzania dotyczące kategorii danych szczególnie chronionych, takich jak dane określone w art. 9 rozporządzenia, powinny być poddawane ocenie skutków w zakresie ochrony danych. Dlatego też wszystkie elementy danych szczególnie chronionych powinny być uwzględnione w art. 33 ust. 2 lit. b).

Poza tym należy skreślić fragment mówiący o ograniczeniu operacji przetwarzania na mocy art. 33 (lit. b), c) i d)) do przetwarzania „na szeroką skalę”, ponieważ Grupa Robocza uważa, że ocena skutków w zakresie ochrony danych jest w przypadku takich operacji niezbędna nawet wtedy, gdy są one dokonywane na małą skalę.

Dotyczy to w szczególności danych biometrycznych, które zdaniem Grupy Roboczej powinny być w określonych okolicznościach uznawane za ryzykowne i dlatego powinna zostać przeprowadzona ocena skutków w zakresie ochrony danych, niezależnie od wszelkich progów przewidzianych w art. 33. Podobnie, jak wspomniano wcześniej, zwolnienie w art. 33 ust. 5 organów publicznych z obowiązku przeprowadzania oceny skutków jest nieuzasadnione, chyba że taka ocena została już przeprowadzona w procesie legislacyjnym.

Zgłaszanie naruszeń ochrony danych

Grupa Robocza z zadowoleniem przyjmuje wprowadzenie obowiązku zgłaszania naruszeń ochrony danych, który zapewnia spójność we wszystkich sektorach. Grupa ma jednak wątpliwości czy sposób, w jaki obowiązek zgłaszania został wprowadzony, zapewni zadowalające rezultaty. W szczególności zakres obowiązku dokonywania zgłoszeń do organu nadzorczego powinien być bardziej skoncentrowany i ograniczony. Należy unikać sytuacji, w których organy nadzorcze są rozprasane i nadmiernie obciążone ze względu na konieczność rozpatrzenia zgłoszeń niewielkich naruszeń ochrony danych, które prawdopodobnie nie będą miały negatywnego wpływu na prawa podmiotów danych. Ponadto należy wyjaśnić rolę OOD w przypadku zgłoszenia (i po nim).

Grupa Robocza jest świadoma faktu, że 24-godzinny termin na dokonanie zgłoszeń może okazać się w pewnych okolicznościach niemożliwy do dotrzymania. W art. 31 ust. 1 uwzględniono ten problem stwarzając możliwość dokonania zgłoszenia po upływie 24 godzin od uzyskania wiedzy o naruszeniu. Tym niemniej istotne jest szybkie dokonywanie zgłoszeń. Z tego względu Grupa Robocza proponuje przyjęcie podejścia dwufazowego, zgodnie z którym administrator musi zasadniczo dokonać zgłoszenia w terminie 24 godzin od momentu, w którym dowiedział się o naruszeniu. W przypadku gdy nie można przekazać wszystkich informacji w tym 24-godzinnym terminie, administrator będzie miał możliwość uzupełnienia zgłoszenia w drugiej fazie.

Konieczne jest dalsze sprecyzowanie kryteriów ustalania wystąpienia naruszenia ochrony danych oraz okoliczności, w jakich naruszenie musi zostać zgłoszone OOD i zainteresowanym podmiotom danych (np. gdy istnieje zagrożenie konkretnym niebezpieczeństwem lub szkodą dla podmiotów danych). Grupa Robocza uważa że EROD powinna w każdym przypadku być zaangażowana w ustalenie tych kryteriów i okoliczności.

Aby odzwierciedlić zalecenia Grupy Roboczej i ENISA, formularz zgłoszenia powinien zawierać ocenę powagi naruszenia ochrony danych opartą na obiektywnych kryteriach.

W odniesieniu do roli i funkcjonowania OOG

Niezależność

Obecny tekst stanowi, że członkowie OOD mogą być wyznaczani jedynie przez parlament lub rząd. Grupa Robocza pragnęłaby jednak umożliwić państwom członkowskim dopuszczenie możliwości wyznaczania lub mianowania członków OOD także przez inne niezależne organy, np. radę sądownictwa.

Uprawnienia

Obok możliwości prowadzenia przez OOG dochodzeń, powinny one mieć również wyraźnie określone kompetencje do prowadzenia audytów.

Budżet

W celu skutecznego wykonywania obowiązków i kompetencji OOD zwiększonych w związku z rozporządzeniem, w tym tych, które mają być wykonywane w kontekście wzajemnej pomocy, współpracy i udziału w EROD, rozporządzenie stanowi, że państwa członkowskie muszą zapewnić OOD odpowiednie zasoby ludzkie, techniczne i finansowe oraz pomieszczenia i infrastrukturę. Jak wspomniano wcześniej Grupa Robocza usilnie zaleca bardziej konkretne zaznaczenie, co należy rozumieć przez odpowiedni budżet, np. po niezależnej dogłębnej ocenie zwiększonych kosztów dla OOD w świetle obecnych propozycji.

Odpowiedni budżet mógłby opierać się na stałej kwocie mającej pokryć koszty funkcji podstawowych, które wszystkie OOD muszą wykonywać w równym stopniu, uzupełnionej o kwotę wyliczaną zgodnie ze wzorem uwzględniającym ludność państwa członkowskiego i jego PKB. Możliwe byłoby również uwzględnienie liczby wielonarodowych spółek mających siedzibę w tym państwie członkowskim. W jednym z motywów należy jednoznacznie

zachęcić państwa członkowskie do rozważenia szerokiego wachlarza opcji finansowania OOD, tak by zagwarantować spełnienie wymogu, który mówi o odpowiednim wyposażeniu organu.

Zakres swobody

By OOD mogły być skuteczne, powinny zyskać charakter selektywny. Powinny one mieć możliwość definiowania swoich własnych priorytetów i rozpoczynania działań, takich jak dochodzenia, z własnej inicjatywy, niezależnie od obowiązków dotyczących współpracy, wzajemnej pomocy i zgodności zgodnie z rozdziałem VII. OOD powinny mieć możliwość przydziału zasobów stosownie do strategicznego charakteru i złożoności danych zagadnień, np. poprzez uwzględnienie faktycznych i potencjalnych naruszeń ochrony danych, liczby zainteresowanych osób oraz wykorzystywanej technologii. Umożliwienie OOD ustalania swoich własnych priorytetów pomaga także w radzeniu sobie z ograniczeniami natury finansowej i budżetowej.

Obowiązki wynikające z art. 52 ust. 2 i 3, które stanowią, że OOD „działa na rzecz” oraz „na wniosek, doradza każdemu podmiotowi danych” wydają się zmniejszać zakres swobody potrzebnej do skutecznego działania OOD. Ponadto by zapewnić OOD swobodę, Grupa Robocza sugeruje dodanie słowa „może” w art. 34 ust. 3, co prowadzi do brzmienia „i **może** wystąpić z odpowiednimi propozycjami mającymi na celu zniwelowanie braku zgodności”.

Jurysdykcja i kompetencje OOD (punkt kompleksowej obsługi)

Artykuł 51 ust. 1 przewiduje, że OOD ma mieć kompetencje na terytorium swojego państwa członkowskiego. Tę ogólną zasadę uzupełnia art. 51 ust. 2, który stanowi, że OOD państwa członkowskiego, w którym administrator ma swoją główną siedzibę, uznawany jest za OOD właściwy do nadzoru nad operacjami przetwarzania we wszystkich państwach członkowskich.

Grupa Robocza Art. 29 opowiada się za stworzeniem koncepcji organu wiodącego oraz nałożeniem na OOD wyraźnego obowiązku współpracy jak również korzystania z mechanizmu zgodności, w przypadku gdy dane operacje przetwarzania mogą mieć wpływ na podmioty danych w wielu państwach członkowskich, ponieważ doprowadzi to do spójnej wykładni i stosowania ram prawnych UE, zapewniając tym samym pewność prawa. Jednakże, jak wspomniano powyżej, by mechanizm ten mógł funkcjonować, należy wyjaśnić definicję głównej siedziby oraz konsekwencje dla kompetencji innych OOD. Wątpliwości budzi również sposób zaproponowania mechanizmu zgodności.

Należy w każdym przypadku jasno stwierdzić, że kompetencje wiodącego OOD nie są wyłączne. Kompetencje wiodącego OOD wykonywane są z zastrzeżeniem obowiązku współpracy, świadczenia i przyjmowania wzajemnej pomocy oraz korzystania z mechanizmu zgodności – zgodnie z treścią rozdziału VII o zgodności i współpracy – jak również działania w porozumieniu z innymi zaangażowanymi OOD.

Ponadto Grupa Robocza podkreśla, że zasada kompleksowego punktu obsługi zapisana w art. 51 ust. 2 ma zastosowanie tylko do sytuacji, w której administrator i podmiot przetwarzający mają więcej niż jedną siedzibę na terytorium UE, nie zaś do sytuacji, w której nie ma żadnej siedziby UE i gdy operacje przetwarzania związane są z oferowaniem towarów i usług podmiotom danych w Unii lub monitorowaniem ich zachowania, zgodnie z art. 3 ust. 2. W

związku z tym, w takim przypadku każdy OOD, na którego państwo członkowskie operacje przetwarzania mają wpływ, jest właściwy zgodnie z art. 51 ust. 1, jednak w rozporządzeniu brakuje reguł pozwalających ustalić, który OOD powinien w takich przypadkach być tym „wiodącym”. Grupa Robocza uważa, że współpraca i spójność mają w takich przypadkach szczególnie istotne znaczenie.

Ze względu na to, że obecne elementy definicji głównej siedziby w art. 4 ust. 13 są, jak wyjaśniono wcześniej, niezadowalające i dlatego brakuje jasności co do ustanowienia wiodących OOD w sprawach transgranicznych, Grupa Robocza proponuje rozważenie:

1. akceptacji podejścia, zgodnie z którym wiodący OOD nie będzie miał wyłącznych kompetencji, lecz będzie zobowiązany do współpracy, świadczenia i przyjmowania wzajemnej pomocy oraz korzystania z mechanizmu zgodności, zgodnie z treścią rozdziału VII o zgodności i współpracy; oraz
2. w przypadkach, w których nie ma siedziby w UE (lub brakuje jasności co do tego, gdzie znajduje się główna siedziba) kryteriów ustalania wiodącego OOD, które powinny obejmować:
 - państwo członkowskie, w którym odbywają się główne przedmiotowe operacje przetwarzania;
 - państwo członkowskie, w którym znajdują się osoby fizyczne, na które operacje te mają wpływ;
 - państwo członkowskie, w którym osoby fizyczne złożyły skargi na dane operacje lub zgłosiły swoje wątpliwości OOD, zgodnie z art. 73 ust. 1.

Jasne jest, że zastosowanie powyższych kryteriów może prowadzić do wyłonienia wielu państw członkowskich. Jednakże na bazie tych kryteriów właściwe OOD powinny uzgodnić między sobą, który z nich powinien objąć rolę wiodącą. W przypadkach, gdy nie jest to oczywiste, lub w braku porozumienia decyzję powinna podejmować EROD, na bazie tych samych kryteriów.

Wzajemna pomoc

Grupa Robocza zaleca kompleksową koncepcję wiodącego OOD i współpracy. W każdym przypadku, w którym, w rozumieniu art. 56 „operacje przetwarzania będą miały prawdopodobny wpływ na podmioty danych w wielu państwach członkowskich” należy ustanowić ogólny obowiązek współpracy dla odpowiednich OOD, ponieważ operacje te mają wpływ na ich obywateli. Współpraca ta powinna obejmować ocenę prawną, jak również szczególne środki nadzorcze, które należy podjąć.

Zgodnie z art. 55 ust. 1 Grupa Robocza uważa, że OOD powinny wzajemnie przekazywać sobie właściwe informacje, także w przypadkach, w których nie podjęto jeszcze środka o którym mowa w art. 58 ust. 1 (np. w przypadku naruszenia bezpieczeństwa). Obok tego OOD powinny informować się wzajemnie o pozytywnych decyzjach podjętych w sprawie ocen skutków w zakresie ochrony danych.

Grupa Robocza zaleca wyjaśnienie w art. 55 i 56, że w każdym przypadku, w którym podjęta musi zostać decyzja, w którą zaangażowany jest wiodący OOD oraz inny zainteresowany OOD zgodnie z art. 51 ust. 1, wiodący OOD i krajowy „miejscowy” OOD powinny działać *w porozumieniu* jeżeli chodzi o ocenę sprawy i środków, które należy podjąć. Jeżeli zainteresowane OOD nie osiągną porozumienia co do oceny sprawy lub środków, które należy podjąć na poziomie dwustronnym lub wielostronnym, sprawa powinna zostać skierowana do mechanizmu zgodności jak w art. 57.

Grupa Robocza z zadowoleniem przyjmuje zaproponowane środki mające zagwarantować OOD możliwość współpracy oraz zwraca uwagę na fakt, że – jak omówiono powyżej – kompetencje wiodącego OOD nie są wyłączne. Grupa Robocza podkreśla jednak, że potrzebnych jest więcej elementów dla zagwarantowania wzajemnej współpracy – dotyczy to budżetu OOD, jak wspomniano powyżej, lecz także uwzględnienia istotnych szczegółowych elementów w zakresie praktycznego wdrażania wzajemnej współpracy. Wykorzystywane języki, terminy, ilość i charakter wnioskowanych informacji, jak również środki techniczne, formaty i procedury wymiany informacji, wszystkie te kwestie w praktyce mają zasadnicze znaczenie dla zapewnienia skutecznej współpracy między OOD i dlatego są centralnym elementem zasady „kompleksowego punktu obsługi”.

Zgodność

Grupa Robocza z zadowoleniem odnotowuje, że jej propozycja dotycząca mechanizmu współpracy i koordynacji, który ma zapewnić spójne stosowanie przepisów o ochronie danych, została uwzględniona w art. 57 i 58 projektu.

Grupa Robocza uważa jednak, że taki mechanizm powinien zagwarantować spójność jedynie w tych sprawach, w których jest to potrzebne, i nie powinien ograniczać niezależności krajowych organów nadzorczych a także nie powinien ingerować w kompetencje różnych podmiotów.

Ze względu na szeroki zakres art. 58 ust. 2 lit. a), rozciągający się na przetwarzanie danych w kontekście jakiegokolwiek rodzaju transgranicznego oferowania towarów lub usług na terytorium UE, Grupa Robocza sugeruje, by mechanizmowi zgodności w ramach EROD podlegały jedynie te przypadki, w których właściwe OOD zgodnie z art. 51 nie osiągnęły porozumienia w sprawie oceny tych przypadków oraz środków, które należy podjąć na poziomie dwustronnym lub wielostronnym. W każdym przypadku EROD powinna być informowana o przypadkach mających ogólne znaczenie dla ochrony danych oraz swobodnego przepływu danych osobowych w UE.

Aby uniknąć sytuacji, w której duża liczba spraw mogłaby trafiać do mechanizmu ze względu na jego szeroki zakres (zgodnie z art. 58 ust. 3, który stanowi, że **każdy** organ może zażądać, aby jakakolwiek sprawa została załatwiona w ramach mechanizmu zgodności), Grupa Robocza zaleca poddawanie wniosków złożonych na mocy art. 58 ust. 3 pod głosowanie w EROD.

Niezależnie od roli Komisji jako strażniczki Traktatów, Grupa Robocza ma istotne zastrzeżenia odnośnie do roli przewidzianej dla Komisji w indywidualnych sprawach, rozstrzygniętych w ramach mechanizmu zgodności, ponieważ zagraża ona niezależnemu statusowi OOD i EROD. Jeżeli sprawa rozstrzygana jest lub została rozstrzygnięta przy udziale Europejskiej Rady Ochrony Danych (EROD) w ramach mechanizmu zgodności, Komisja powinna mieć możliwość przedstawienia swojej oceny prawnej, ale powinna powstrzymać się od dalszej ingerencji. Dotyczy to w szczególności przypadków zawieszenia środka, zgodnie z treścią art. 60 ust. 1, art. 62 ust. 1 lit. a) oraz art. 62 ust. 2. Ponadto „poważne wątpliwości” nie wystarczają do tego, by interweniowała Komisja.

Grupa Robocza podkreśla, że to do samej EROD należy dopilnowanie, by jej opinie były respektowane i stosowane w jednolity sposób przez wszystkie właściwe OOD.

Aby zwiększyć skuteczność opinii EROD, można by wprowadzić „mechanizm potwierdzenia” w przypadkach, w których co najmniej jeden OOD zamierza dokonać odstępstwa od treści opinii przyjętej przez EROD w ramach mechanizmu zgodności stosownie do art. 58 ust. 7. EROD powinien mieć w takich przypadkach możliwość ponownego potwierdzenia swojej opinii kwalifikowaną większością głosów, podkreślając tym samym znaczenie wspólnego podejścia w przypadkach mających ogólne znaczenie dla ochrony danych w UE. Inny wariant polegałby na umożliwieniu OOD zgłaszania stanowisk mniejszości. Stanowiska te byłyby umotywowane i ogłaszane publicznie.

Oprócz tego można by przewidzieć procedurę umożliwiającą EROD i Komisji występowanie do Europejskiego Trybunału Sprawiedliwości o opinię w sprawie wykładni rozporządzenia, jeżeli OOD nie zamierza postąpić zgodnie z określoną opinią, którą EROD ponownie potwierdziła większością kwalifikowaną.

Stosowanie prawa krajowego (rozdział IX)

Gdy państwa członkowskie przyjmują przepisy szczególne na mocy art. 80-83, przepisy te są powiązane z przepisami dotyczącymi kompetencji OOD oraz systemem wiodącego OOD.

W obecnym brzmieniu tekst nie rozwiązuje problemu spraw wynikających z równoległe obowiązujących przepisów krajowych, np. w kontekście zatrudnienia, w odniesieniu do zakresu kompetencji OOD głównej siedziby administratora. Pojawia się w związku z tym pytanie, czy np. niemiecki OOD musiałby interpretować i stosować hiszpańskie prawo pracy w przypadku zagadnienia dotyczącego pracownika spółki zależnej w Hiszpanii podlegającej spółce mającej główną siedzibę w Niemczech. Należy zatem wyjaśnić, że w drodze wyjątku od art. 51 ust. 2, w sprawach, które zależą od stosowania prawa krajowego zgodnie z rozdziałem IX rozporządzenia, właściwy krajowy OOD powinien zawsze (naturalnie przy współdziałaniu z wiodącym OOD) być właściwym organem do stosowania równoległe obowiązującego prawa krajowego w danej sprawie (w powyższym przykładzie hiszpański OOD byłby właściwy do stosowania szczególnej hiszpańskiej ustawy o ochronie danych w kontekście zatrudnienia).

Ogólnie Grupa Robocza podkreśla potrzebę wyjaśnienia zakresu stosowania przepisów krajowych przyjętych na mocy rozdziału IX.

Terminy

Grupa Robocza podziela zdanie, że istotne jest terminowe wydawanie przez EDOR opinii, o które występuje się za pośrednictwem mechanizmu zgodności. Terminy wyznaczone na osiągnięcie rezultatów powinny być jednak na tyle długie, by zagwarantować doradztwo dobrej jakości. Aby zagwarantować faktyczne przewodnictwo i wsparcie na miejscu oraz zagwarantować porady, które mogą zostać obronione w toku postępowań sądowych, należy w każdym przypadku rozszerzyć rygorystyczne ramy czasowe.

„Kompleksowy punkt obsługi” dla podmiotów danych

Podobnie jak administratorzy danych, także podmioty danych w jurysdykcji unijnych OOD powinny posiadać „kompleksowy punkt obsługi”. W rozporządzeniu istnieje szereg możliwości wykonywania przez podmioty danych ich praw i dochodzenia sprawiedliwości. Podmioty danych mogą złożyć skargę w OOD we wszystkich państwach członkowskich (w

swoim krajowym OOD, OOD państwa członkowskiego, gdzie administrator ma swoją główną siedzibę, lub innym OOD w Unii). Podmioty danych mogą również wszcząć postępowanie przed swoim sądem krajowym oraz przed sądem państwa, w którym administrator danych ma siedzibę.

Chociaż możliwości te wydają się zwiększać prawa podmiotów danych, mogą one również prowadzić do nieporozumień i niepewności co do tego, kto ostatecznie odpowiadał będzie za udzielenie odpowiedzi podmiotowi danych.

Niezależnie od prawa do sądowego środka ochrony prawnej, Grupa Robocza zaleca doprecyzowanie, że podmioty danych powinny zasadniczo zwracać się do OOD w jurysdykcji, w której mają miejsce zamieszkania lub OOD, w którego jurysdykcji administrator danych lub podmiot przetwarzający dane mają siedzibę. Aby umożliwić udzielenie odpowiedzi podmiotowi danych, OOD w tym państwie członkowskim, do którego zwrócono się z wnioskiem, musiałby współpracować z OOD głównej siedziby administratora (wiodącym OOD), aby uzgodnić niezbędne środki w celu przeprowadzenia dochodzenia oraz, w określonych przypadkach, podjęcia działań egzekucyjnych. Jednak niezależnie od okoliczności, to OOD do którego pierwotnie zwrócono się z wnioskiem, pozostaje odpowiedzialny za udzielenie odpowiedzi podmiotowi danych.

Struktura instytucyjna EROD

Grupa Robocza odnotowuje, że zostanie zastąpiona Europejską Radą Ochrony Danych (EROD), która została ustanowiona w art. 64.

Grupa Robocza uważa, że powinna ona mieć możliwość demokratycznego wyboru swojego przewodniczącego i wiceprzewodniczących. Zdaniem Grupy Roboczej nie przedstawiono przekonujących powodów za tym, by EIOD pełnił funkcję stałego wiceprzewodniczącego.

Oprócz tego pożądanym byłoby posiadanie w pełni niezależnego sekretariatu. Równocześnie jednak Grupa Robocza odnotowuje, że usługi sekretariatu EDOR zapewniane mają być już nie przez Komisję, a przez EIOD. Należy poddać dalszej analizie, w jaki sposób można to osiągnąć pod względami praktycznymi i względami podległości służbowej, w szczególności biorąc pod uwagę potrzebę zapewnienia niezależności członków sekretariatu oraz prawne i instytucjonalne konsekwencje powierzenia obsługi sekretariatu EROD jednemu z jej członków.

Transfery międzynarodowe

W rozporządzeniu słusznie podkreślono odpowiedzialność administratorów danych za dopilnowanie, by dane osobowe pozostały chronione, gdy są przekazywane poza Europejski Obszar Gospodarczy (EOG). Rozporządzenie ułatwia to zadanie administratorom, zapewniając różnego rodzaju „bezpieczne przystanie” w formie decyzji stwierdzających odpowiedni poziom ochrony, uproszczony system wiążących reguł korporacyjnych dla wielonarodowych spółek, zatwierdzone klauzule kontraktowe oraz indywidualne zatwierdzanie przez OOD. Przewiduje ono również różne odstępstwa w art. 44.

Jednakże zakres tych odstępstw, w szczególności w art. 44 ust. 1 lit. h), pozostaje bardzo szeroki i możliwy do zastosowania w wielu sytuacjach. Zgodnie z poprzednią opinią Grupy

Roboczej (WP 114), takie odstępstwa powinny mieć zastosowanie wyłącznie w przypadkach, w których przetwarzanie nie ma charakteru masowego, powtarzalnego ani zorganizowanego.

Obok tego art. 42 wprowadza możliwość wykorzystywania niewiążących instrumentów do kształtowania ram transferów międzynarodowych, przy czym instrumenty te wymagają zezwolenia ze strony OOD. Tym niemniej wiążący charakter był zawsze uważany za istotny wymóg w przypadku obowiązujących narzędzi kształtujących ramy transferów międzynarodowych (np. umowy zbiorowe, wiążące reguły korporacyjne, bezpieczna przystań, stwierdzenie zapewniania odpowiedniego poziomu ochrony przez państwa trzecie). Dlatego też proponuje się skreślenie art. 42 ust. 5, z wyjątkiem ostatniego zdania. W konsekwencji należy odpowiednio dostosować odniesienie w art. 34.

W odniesieniu do art. 41 ust. 6 należy wyjaśnić, czy wyrażenie „bez uszczerbku dla przepisów art. 42-44” oznacza, że w przypadku wydania przez Komisję decyzji stwierdzającej brak odpowiedniego poziomu ochrony w państwie trzecim, transfery danych do tego państwa będą jednak możliwe na bazie wszystkich tych artykułów.

Ponadto w przypadkach, w których Komisja zdecydowała o tym, że państwo trzecie lub terytorium albo sektor przetwarzania w tym państwie trzecim lub dana organizacja międzynarodowa zapewniają odpowiedni poziom ochrony (art. 41), takie transfery nie wymagają dalszego zezwolenia. Jednakże, jak już wspomniano wcześniej, Grupa Robocza usilnie zaleca włączenie obowiązku konsultowania przez Komisję decyzji o stwierdzeniu odpowiedniego poziomu ochrony z EDOR.

Ujawnianie danych niedozwolone w prawie UE

Grupa Robocza podkreśla potrzebę włączenia do rozporządzenia obowiązku korzystania z umów o wzajemnej pomocy prawnej (UoWPP) w przypadku ujawnienia danych niedozwolonego prawem Unii ani państwa członkowskiego. Grupa Robocza uważa, że brak przepisu o obligatoryjnym korzystaniu z takich umów tam gdzie one obowiązują umożliwi między innymi szeroko zakrojone transfery danych osobowych w oparciu o szeroką i nieograniczoną kategorię „istotnego interesu publicznego” zgodnie z art. 44 ust. 1 lit. d), w tym w przypadkach, gdy takie transfery mają charakter masowy, częsty i zorganizowany. Jeżeli na podstawie orzeczenia sądu lub decyzji organu administracyjnego państwa trzeciego administrator lub podmiot przetwarzający zostaną wezwani do przekazania danych z UE do państwa trzeciego i gdy między wzywającym państwem trzecim a Unią lub państwem albo państwami członkowskimi nie obowiązuje UoWPP ani inna umowa międzynarodowa, transfer takich danych powinien być zakazany. Grupa Robocza podkreśla, że w przypadku gdy obowiązuje UoWPP organem właściwym na podstawie takiej umowy (lub porównywalnej umowy międzynarodowej) będzie organ rozpatrujący wniosek, który powinien, w razie potrzeby, skonsultować się z OOD.

Prawo do dochodzenia odpowiedzialności i odszkodowania

Grupa Robocza z zadowoleniem przyjmuje przepisy wprowadzone w art. 77 ust. 1 służące zagwarantowaniu, by każda osoba, która poniosła szkodę w wyniku bezprawnej operacji przetwarzania lub działania niezgodnego z rozporządzeniem, miała prawo otrzymania ze strony administratora lub podmiotu przetwarzającego odszkodowania za poniesione szkody. Grupa Robocza przyjmuje również z zadowoleniem fakt, że art. 77 ust. 2 gwarantuje, by podmioty danych nie ponosiły obciążeń związanych ze zwracaniem się do odpowiedzialnego

administratora, w przypadku gdy w przetwarzaniu danych bierze udział więcej niż jeden administrator lub podmiot przetwarzający. Grupa Robocza uważa jednak przy tym, że niezbędne jest wyjaśnienie (w jednym z motywów), że słowo „szkoda” nie oznacza wyłącznie szkody materialnej, lecz obejmuje również szkody niematerialne.

Jeżeli inny OOD (np. OOD głównej siedziby) podjął decyzję wpływającą na podmiot danych lub powodującą dla niego szkodę, podmiot danych powinien mieć możliwość zaskarżenia decyzji przed sądami administracyjnymi swojego państwa zamieszkania.

Rozwiązanie proponowane przez Komisję, by podmiot danych lub OOD składał pozew przeciwko innemu OOD na terytorium tego OOD, jest dalekie od zadowalającego. Grupa Robocza wzywa do ustanowienia systemu umożliwiającego podmiotom danych zaskarżenie decyzji administracyjnej przed sądem administracyjnym swojego państwa zamieszkania.

Grzywny

Grupa Robocza z zadowoleniem przyjmuje wprowadzenie wysokich grzywien, ponieważ umożliwią one odgrywanie przez OOD ich roli organów egzekucyjnych oraz mogą, dzięki efektowi odstraszania, przyczynić się do większego przestrzegania prawa przez administratorów danych.

Artykuł 79 ust. 1 przewiduje, że każdy organ nadzoru „jest uprawniony” do nakładania sankcji administracyjnych. Na poparcie tego w motywie 120 stwierdzono, że organ nadzorczy „powinien być uprawniony” do karania wykroczeń. Jednakże w art. 79 ust. 4-6 stwierdzono, że w opisanych tam sytuacjach organ nadzorczy „nakłada grzywnę”. Grupa Robocza jest zdania, że OOD powinien mieć pewien zakres swobody w decydowaniu, kiedy nałożyć grzywnę, ponieważ na charakter naruszenia wpływa wiele czynników, które powinny być uwzględnione przy podejmowaniu decyzji o grzywnie. Dlatego też Grupa zaleca odpowiednią zmianę brzmienia art. 79 ust. 4-6.

Grupa Robocza docenia harmonizujące skutki art. 79, który reguluje jakie naruszenia prowadzą do maksymalnej grzywny, ponieważ doprowadzi to do większej spójności w nakładaniu grzywien w Unii Europejskiej. Niezależnie od tego Grupa Robocza sugeruje wyraźne przewidzenie w art. 58 ust. 2 możliwości wykorzystania mechanizmu zgodności z sekcji 2 w rozdziale VII w zakresie niezgodności w stosowaniu sankcji administracyjnych, o czym mówi także motyw 120.

Grupa Robocza rozumie ponadto, że gdy właściwych jest wiele OOD, są one także wszystkie uprawnione do nakładania grzywny zgodnie z art. 79 rozporządzenia. Rodzi to wątpliwości związane z zasadą *ne bis in idem*.

Grupa Robocza uważa, że próg wprowadzony w przypadku pierwszego i nieumyślnego naruszenia w praktyce wyłączyłby wielu administratorów z jego zakresu, dlatego opowiada się za usunięciem tego progu. Gdyby jakiś próg miał jednak obowiązywać, należałoby raczej uwzględnić liczbę podmiotów danych, na których dane operacje miały (negatywny) wpływ, a nie – liczbę pracowników administratora.

Sądowe środki ochrony prawnej

Grupa Robocza z zadowoleniem przyjmuje wprowadzenie kompleksowego zestawu przepisów dotyczących sądowych środków ochrony prawnej dla podmiotów danych, w tym możliwości wykonywania przez organizacje i stowarzyszenia praw podmiotów danych w stosunku do administratorów danych i podmiotów przetwarzających dane. Równocześnie jednak zdaniem Grupy Roboczej szereg aspektów rozdziału VIII wymaga dalszego wyjaśnienia.

Ze względu na obszerny zakres art. 73 ust. 1, zgodnie z którym każdy podmiot danych ma prawo złożenia skargi do OOD w **dowolnym** państwie członkowskim, Grupa Robocza uważa, że podmiot danych powinien zasadniczo kierować się do OOD w jurysdykcji, w której zamieszkuje, lub OOD w jurysdykcji, w której administrator lub podmiot przetwarzający ma siedzibę, tak jak w kontekście wyżej wspomnianego kompleksowego punktu obsługi dla podmiotów danych.

Ponadto gdy OOD otrzymujący skargę wydaje się nie być właściwy do rozpatrzenia istotnych elementów sprawy, zdaniem Grupy Roboczej powinien istnieć obowiązek współpracy przez ten organ z OOD stanowiącym kompleksowy punkt obsługi dla podmiotu danych oraz OOD, w którego jurysdykcji ma siedzibę administrator. W takim przypadku OOD, do którego skierowano skargę, powinien być zobowiązany do informowania podmiotu danych o postępach w rozpatrywaniu sprawy, niezależnie od tego, czy jest właściwy do zajęcia się jej istotnymi elementami. Wynika to z potrzeby zapewnienia kompleksowego punktu obsługi dla podmiotów danych (zob. wyżej).

W odniesieniu do art. 74 ust. 2 Grupa Robocza stoi na stanowisku, że należy wyjaśnić, który OOD powinien być właściwy do „do podjęcia działania w sprawie skargi w przypadku braku decyzji chroniącej jego prawa”. W przypadku wiodącego OOD, zgodnie z art. 51 ust. 2 byłby to OOD państwa członkowskiego, w którym podmiot przetwarzający/administrator ma swoją główną siedzibę, a w każdym innym przypadku byłby to właściwy organ zgodnie z art. 51 ust. 1. Należy zatem sprecyzować w art. 74 ust. 2, że obowiązek podjęcia działania dotyczy właściwego organu nadzorczego „w rozumieniu art. 51 ust. 1 lub 2”.

Obok tego art. 74 ust. 4 przewiduje, że podmiot danych, którego dotyczy decyzja OOD w innym państwie członkowskim, w którym ma ona swoje miejsce zwykłego pobytu, może wystąpić do OOD państwa członkowskiego, w którym ma swoje miejsce zwykłego pobytu, o wszczęcie postępowania przeciwko OOD w innym państwie członkowskim. Chociaż Grupa Robocza docenia motywy wprowadzenia takiego przepisu, by zagwarantować podmiotom danych możliwość wykonywania swoich praw wobec OOD w innym państwie członkowskim, uważa jednakże, że jest on sprzeczny z ogólnym obowiązkiem wzajemnej współpracy między OOD oraz świadczenia wzajemnej pomocy w sprawach transgranicznych, zgodnie z art. 55 i 56, jak również z tym, że w przypadkach braku porozumienia między OOD, sprawa powinna zostać przedłożona EROD. Dlatego też Grupa Robocza podkreśla potrzebę uważnego przeanalizowania alternatywnych możliwości uzyskania przez podmioty danych przed decyzją OOD, która ich dotyczy, sądowych środków ochrony prawnej spójnych z zasadami rozporządzenia.

Artykuł 75 ust. 2 przewiduje możliwość pozwania przed podmioty danych administratora lub podmiot przetwarzający do sądu państwa członkowskiego, w którym administrator lub podmiot przetwarzający mają siedzibę. Postępowanie takie może też zostać wszczęte przed

sądem państwa członkowskiego, w którym podmiot danych ma miejsce zwykłego pobytu. Grupa Robocza uważa, że możliwość wszczęcia postępowania przed sądem w **dowolnym** państwie członkowskim, w którym administrator lub podmiot przetwarzający mają siedzibę, niezależnie od tego, czy jest to główna siedziba lub też siedziba, w której podejmowane są istotne decyzje w sprawie przetwarzania danych, może okazać się problematyczna.

Mimo art. 75 ust. 4, który stwierdza, że państwa członkowskie wykonują prawomocne orzeczenia innych sądów, należy wątpić, czy orzeczenie sądu w państwie członkowskim, w którym administrator lub podmiot przetwarzający nie mają swojej głównej siedziby jest faktycznie wykonalne. Kwestię tę trzeba wyjaśnić.

Ponadto nawet jeśli Grupa Robocza z zadowoleniem przyjmuje wprowadzenie w art. 75 ust. 2 możliwości wszczęcia postępowania przeciwko administratorowi danych przed sądem państwa członkowskiego, w którym podmiot danych ma miejsce zwykłego pobytu, co jest zbliżone do koncepcji ochrony konsumenta zgodnie z rozporządzeniem Bruksela I i zmierza do wzmocnienia pozycji podmiotów danych, nie jest jasne w jaki sposób orzeczenie sądu w państwie członkowskim, w którym podmiot danych ma swoje miejsce zwykłego pobytu zostanie wykonane, jeżeli administrator lub podmiot przetwarzający mają siedzibę w innym państwie członkowskim.

Zarówno art. 74 ust. 5, jak i art. 75 ust. 4 stanowią, że państwa członkowskie wykonują prawomocne orzeczenia sądów, o których mowa w tych artykułach. Przepisy te są porównywalne z podobnymi obowiązkami zapisanymi w art. 111 konwencji wykonawczej do układu z Schengen. Jak wspomniano niejasne wydaje się, zgodnie z jakimi regułami proceduralnymi i przez które organy krajowe egzekwowane będą orzeczenia sądów jednego państwa członkowskiego w innym państwie członkowskim. Ponadto w odniesieniu do tego, co stanowi „prawomocne” orzeczenie, może zachodzić także potrzeba dalszej harmonizacji (System Informacyjny Schengen – sprawa pomiędzy Austrią i Francją).

Kościoły i związki wyznaniowe

Grupa Robocza rozumie, że art. 85 zobowiązuje kościoły i organizacje wyznaniowe, które obecnie mają odrębne reżymy prawne do uzgodnienia ich z rozporządzeniem. W każdym razie rozporządzenie nie daje kościołom i organizacjom wyznaniowym możliwości przyjmowania odrębnych reżymów prawnych niezgodnych z rozporządzeniem w tych państwach członkowskich, w których nie zezwalają na to regulacje konstytucyjne.

W kwestii dyrektywy

Wybór instrumentów

Grupa Robocza odnotowuje, że Komisja Europejska wyraźnie nie zdecydowała się przedstawić pojedynczego, uniwersalnego instrumentu ochrony danych, zamiast tego prezentując dyrektywę jako instrument mający uregulować ochronę danych w obszarze policji i wymiaru sprawiedliwości w sprawach karnych w sposób zapewniający wysoki, spójny poziom ochrony danych, do którego zmierza Komisja. Grupa Robocza odnotowuje również, że obecny projekt doprowadziłby do obniżenia standardów ochrony danych w wielu państwach członkowskich. Grupa Robocza uważa to za niedopuszczalne i dlatego wzywa

Europejskiego prawodawcę do zagwarantowania, by obecne, większe gwarancje ochrony danych w Unii Europejskiej uznawane były za absolutne minimum w kontekście proponowanej dyrektywy. Dyrektywa nie powinna być tak zaprojektowana, by usprawiedliwiać usunięcie dodatkowych gwarancji ochrony danych z obecnego prawodawstwa państw członkowskich.

Spójność

Pomimo różnych zaproponowanych instrumentów „zasadnicze” aspekty przepisów powinny być ze sobą spójne, w szczególności w odniesieniu do zasad, zobowiązań i obowiązków, indywidualnych praw i kompetencji oraz narzędzi, którymi dysponują organy nadzorcze. Poza tym, że względu na newralgiczny charakter danych, których przetwarzanie objęte jest zakresem dyrektywy, niedopuszczalne byłoby obniżenie standardów obowiązujących w tej dziedzinie. Oczywiście konieczne jest ustanowienie ograniczeń i wyjątków, zwłaszcza dotyczących praw podmiotów danych, należy jednak jasno postawić, że są to jedynie wyjątki, i że „zasadnicze” aspekty są takie same.

Zakres stosowania

Grupa Robocza odnotowuje i przyjmuje z zadowoleniem fakt zarzucenia w dyrektywie rozróżnienia pomiędzy przetwarzaniem danych osobowych w sprawach krajowych i transgranicznych, które było przewidziane w decyzji ramowej 2008/977/WSiSW. Grupa krytykowała w przeszłości ograniczenie stosowania europejskich przepisów do spraw o charakterze ściśle transgranicznym.

Zakres zastosowania dyrektywy powinien być możliwie najbardziej jasny. Tymczasem proponowany tekst rodzi szereg pytań; niektóre z nich omówiono poniżej.

Grupa Robocza odnotowuje trudności z oddzieleniem zakresu stosowania dyrektywy od zakresu stosowania rozporządzenia. Dyrektywa ma zastosowanie, jeżeli właściwe organy przetwarzają dane osobowe do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania albo do wykonywania kar kryminalnych. We wszystkich innych okolicznościach obowiązuje rozporządzenie, jako ogólny instrument ochrony danych osobowych. Należy jednak również uwzględnić zróżnicowane tradycje w państwach członkowskich, jeżeli chodzi o określanie działalności ich organów jako związanej z ochroną porządku publicznego lub też zwykłej działalności administracyjnej (np. w obszarze celnym, imigracji, ochrony środowiska). W rezultacie oba instrumenty, dyrektywa i rozporządzenie, mogą mieć zastosowanie do tej samej instytucji. Należy unikać sytuacji, w których ta sama operacja przetwarzania danych – np. operacja związana z ochroną porządku publicznego – w jednym państwie objęta jest zakresem rozporządzenia, natomiast w drugim przepisami przyjętymi na podstawie dyrektywy. Jest to szczególnie kłopotliwe w sytuacji, gdy oba instrumenty są niespójne, tak jak ma to miejsce w tym przypadku. Z tego punktu widzenia konieczne jest zapewnienie większej spójności między oboma instrumentami oraz większa jasność co do definicji „właściwych organów”. Grupa Robocza uważa, że musi być jasne, do których rodzajów działalności powierzonych prawem właściwym organom ma zastosowanie dyrektywa.

Grupa Robocza jest zdania, że należy jeszcze sprecyzować, w jakim zakresie dyrektywa ma zastosowanie do obszaru postępowania karnego. Grupa zwraca uwagę na fakt, że dyrektywa

ma zastosowanie do przetwarzania danych na potrzeby ścigania przestępstw (art. 1). Równocześnie Grupa Robocza rozumie, że art. 17 (i motyw 82) oznaczają, że państwa członkowskie mogą zdecydować o tym, że nie uzgodnią przepisów swojego postępowania karnego z prawami przewidzianymi w art. 11-16, przynajmniej w przypadkach dotyczących procedur sądowych. Różnice w krajowych procedurach karnych utrudniają jednakże ustalenie, o który etap postępowania karnego chodzi w dyrektywie, w której art. 17 mowa jest o „krajowych przepisach postępowania karnego, jeżeli dane osobowe zawarte są w orzeczeniu lub protokole sądowym przetwarzanym w toku dochodzenia i postępowania karnego”. Grupa Robocza zwraca się do europejskiego prawodawcy o dopilnowanie, by nie mogło być wątpliwości co do tego, że dyrektywa ma zastosowanie do postępowania karnego i ścigania przestępstw, także w celu uniknięcia sytuacji, w których nie zapewniałoby żadnej ochrony danych, gdy tylko prokurator lub sędzia śledczy zostanie zaangażowany w operację prowadzoną w ramach ochrony porządku publicznego lub dochodzenie, zgodnie z konwencją nr 108 Rady Europy.

Ponadto Grupa Robocza uważa, że w art. 44 ust. 2 należy uściślić znaczenie słów „wykonywanie funkcji sądowych” oraz motywy ich umieszczenia. Należy wyjaśnić, jaki powinien być stosunek OOD do sądów oraz w jakich okolicznościach można wykonywać działania nadzorcze.

Zasady przetwarzania danych

W odniesieniu do zasad – w dyrektywie nie zamieszczono istotnych elementów dotyczących zatrzymywania danych osobowych (w tym okresów zatrzymania), przejrzystości wobec osób fizycznych, aktualizowania danych osobowych oraz zapewniania, by były one odpowiednie, istotne i nie nadmierne. Brakuje również przepisów dotyczących rozliczalności, wymagających od administratora danych wykazywania zgodności. Treść art. 4 należy uzgodnić z treścią rozporządzenia (art. 5).

Grupa Robocza sugeruje ponadto włączenie przepisów ograniczających dostęp do danych do należycie upoważnionego personelu właściwych organów, który potrzebuje ich do wykonywania swoich zadań.

Oprócz uwag poczynionych powyżej, dotyczących braku spójności z rozporządzeniem, Grupa Robocza z zadowoleniem przyjmuje proponowane rozróżnienie szeregu kategorii podmiotów, których dane mają być przetwarzane. W szczególności odnotowuje rozróżnienie między danymi dotyczącymi podejrzanych, pokrzywdzonych, świadków itd. Podobnie z zadowoleniem przyjmuje fakt, że ma być dokonywane rozróżnienie ze względu na jakość i poprawność danych przetwarzanych przez organy ścigania. Równocześnie jednak Grupa Robocza krytycznie ocenia fakt ograniczenia tego rozróżnienia poprzez dodanie słów „w możliwym zakresie” w art. 5 i 6 i proponuje ich skreślenie. Jej troskę budzi również szeroki zakres tzw. kategorii „osób różnych” (art. 5 ust. 1 lit. e)), których dane mogą być przetwarzane. Grupa Robocza zaleca odmienne sformułowanie zapisu odnoszącego się do tej kategorii w celu zagwarantowania, by dane osób nienależących do grona podejrzanych mogły być przetwarzane tylko przez bardzo ograniczony czas i na ściśle określonych warunkach. Dyrektywa powinna jasno stwierdzać, że do grup podmiotów danych, o których mowa w art. 5 ust. 1 lit. b)-e), muszą obowiązywać bardziej rygorystyczne przepisy o terminach i kontroli.

W odniesieniu do zgodności z prawem przetwarzania (art. 7), jest niejasne, dlaczego dodano przepisy zawarte w lit. b), c) i d). Wydają się one być sprzeczne z art. 1 ust. 1 określającym cel dyrektywy. Grupa Robocza uważa, że nie powinno dochodzić do przetwarzania danych,

gdy jest ono niezgodne z ogólnym celem dyrektywy. Należy zatem albo skreślić przepisy lit. b), c) i d), albo też dostosować art. 1 ust. 1, by umożliwić takie przetwarzanie.

Grupa Robocza uważa, że należy wprowadzić szczególne przepisy dotyczące przetwarzania danych osobowych dzieci, zgodnie z treścią rozporządzenia. W szczególności państwa członkowskie powinny zostać zobowiązane do ustanowienia progów wiekowych, poniżej których dane nie powinny być przetwarzane na potrzeby zapobiegania przestępstwom kryminalnym, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania bez należytego uzasadnienia, w szczególności gdy gromadzone mają być specjalne kategorie danych. Obok tego państwa członkowskie powinny przewidzieć krótsze okresy przechowywania danych dotyczących dzieci w aktach policyjnych i sądowych.

Przepis dotyczący kategorii specjalnych (art. 8) jest nieco szerszy niż w decyzji ramowej (2008/977/WSiSW). Grupa Robocza ma wątpliwości co do konsekwencji tego rozwiązania, w szczególności czy odstępstwa z ust. 2 mogą doprowadzić do ustanowienia w prawie krajowym ogólnej klauzuli stwierdzającej, że przetwarzane mogą być wszystkie dane szczególnie chronione. W takim przypadku ogólny zakaz niczemu nie służy. W dodatku mimo włączenia danych genetycznych, brakuje osobnego motywu lub artykułu dotyczącego postępowania z tym rodzajem danych. Tymczasem przepis ten stanowiłby istotną gwarancję w kontekście wykorzystywania danych genetycznych i okresów ich zatrzymania.

Biorąc pod uwagę odstępstwo w art. 8 ust. 2, istnieje realne zagrożenie dopuszczenia na mocy dyrektywy do zróżnicowanego poziomu ochrony danych należących do specjalnych kategorii (szczególnie chronionych). Dlatego też Grupa Robocza sugeruje europejskiemu prawodawcy zmianę tego artykułu, by zapewnić zharmonizowane wdrażanie poprzez bliższe określenie wymaganych odpowiednich gwarancji. Poza tym Grupa Robocza doradza dodanie w ust. 2 zapisu stanowiącego, że wyjątki mogą być stosowane jedynie na warunkach określonych w art. 4.

Prawa podmiotów danych

Grupa Robocza odnotowuje i przyjmuje z zadowoleniem to, że w oparciu o art. 11 ust. 1 i art. 13 ust. 1, przynajmniej w niektórych państwach członkowskich, podmioty danych mogą otrzymywać więcej informacji. Uzyskanie informacji o tym, jakie dane są przetwarzane i z jakiej przyczyny, jest jednym z kluczowych aspektów prawa do ochrony danych. Należy jednakże również odnotować, że ograniczenia obowiązku informowania podmiotów danych oraz prawa dostępu przewidziane w art. 11 ust. 5 i art. 13 ust. 2 są problematyczne. Grupa Robocza uznaje te ograniczenia i wyjątki za zbyt szerokie oraz zbyt ogólne, ponieważ umożliwiają one państwom członkowskim wyłączenie całych kategorii danych z udzielanych informacji. Doprowadziłoby to do drastycznego ograniczenia praw podmiotów danych (a nie tylko zaszkodziłoby ich interesom określonym w rozdziale II). Dyrektywa powinna zatem wyraźnie stwierdzać, że ograniczenie praw podmiotu danych może być uzasadnione jedynie w indywidualnych przypadkach, przy należytym uwzględnieniu okoliczności danej sprawy oraz że każde z tych ograniczeń (a nie tylko pominięć) musi być w pełni udokumentowane. Dlatego też Grupa Robocza uważa, że ograniczenie prawa dostępu i prawa do informacji powinno również oznaczać, że w określonych przypadkach podmioty danych mogą mimo to być częściowo informowane o przetwarzaniu ich danych osobowych.

W odniesieniu do ograniczeń praw, należy przewidzieć, że administrator powinien przeprowadzać indywidualną ocenę, czy powinno się ograniczyć prawa, oraz że wszelkie ograniczenia muszą być zgodne z Kartą praw podstawowych Unii Europejskiej oraz Konwencją o ochronie praw człowieka i podstawowych wolności, a także z orzecznictwem Europejskiego Trybunału Sprawiedliwości i Europejskiego Trybunału Praw Człowieka, a w szczególności respektować istotę tych praw i wolności. Grupa Robocza sugeruje włączenie tego sformułowania do art. 13.

Dyrektywa wydaje się być spójna z rozporządzeniem jeżeli chodzi o prawo do poprawienia danych, prawo do złożenia skargi oraz prawo do sądowego środka ochrony prawnej wobec krajowego OOD, administratora danych i podmiotu przetwarzającego dane, a także prawa do odszkodowania i dochodzenia odpowiedzialności.

Dyrektywa nie przewiduje jednakże prawa sprzeciwienia się przetwarzaniu danych osobowych. Może dochodzić do sytuacji, gdy przykładowo podmioty danych, pokrzywdzeni lub świadkowie powinni mieć możliwość oznaczenia ich danych w celu ograniczenia przetwarzania po zakończeniu postępowań prawnych.

Podobnie w dyrektywie nakłada się na administratorów danych obowiązek odpowiedzi na wnioski osób fizycznych korzystających z prawa do dostępu, poprawienia i usunięcia „bez nieuzasadnionej zwłoki”. Nie jest jasne, dlaczego nie mogą tutaj obowiązywać terminy wymagane na mocy rozporządzenia. Ponadto tryb, w jakim osoby fizyczne mogą korzystać ze swoich praw, powinien być w większym stopniu uzgodniony z procedurami opisanymi w rozporządzeniu.

Obowiązki administratorów danych

Obowiązki administratorów danych są spójne z obowiązkami wynikającymi z rozporządzenia jeżeli chodzi o podmioty przetwarzające, ustalenia ze współadministratorami, obowiązek współpracy z krajowym OOD oraz zadania inspektora ochrony danych (IOD). Jednakże na mocy dyrektywy administrator danych nie ma obowiązku informowania osoby fizycznej o tym, czy zamierza przekazać dane osobowe do państwa trzeciego, nie jest też jasne, dlaczego doszło do tego wyłączenia, w szczególności w świetle tego, że państwa członkowskie mogą w określonych okolicznościach ograniczyć prawa osób fizycznych.

W dodatku treść dyrektywy nie jest zgodna z rozporządzeniem jeżeli chodzi o ochronę danych już w fazie projektowania oraz ochronę danych jako opcji domyślnej, a Grupa Robocza nie widzi powodu dla takiej rozbieżności. Jednym z aspektów ochrony prywatności już na etapie projektowania jest ustalenie ryzyk na wczesnym etapie całego procesu i posiadanie możliwości ich ograniczenia. Dlatego też Grupa Robocza wzywa do zamieszczenia w dyrektywie przepisów nakładających wymóg przeprowadzenia ocen skutków w zakresie ochrony danych, w tym w toku procedury legislacyjnej. Grupa uważa, że oceny te są szczególnie istotne w obszarze przetwarzania danych osobowych przez organy ścigania, ze względu na zwiększone ryzyko dla osób fizycznych wynikające z tego przetwarzania. Także obowiązki dotyczące dokumentacji zostały sformułowane mniej szczegółowo niż w rozporządzeniu. Jako minimum, właściwe organy objęte zakresem dyrektywy powinny mieć również obowiązek przechowywania informacji o swoim OOD i okresach zatrzymania.

Grupa Robocza odnotowuje, że wymogi dotyczące bezpieczeństwa danych nie zostały przedstawione w sposób mało szczegółowy, a zatem są raczej niskie w porównaniu z obecnymi standardami. Przykładowo przepisy dotyczące obowiązku zagwarantowania bezpieczeństwa nie obejmują ochronę przed przypadkową utratą lub uszkodzeniem, co przewidziano w rozporządzeniu. Grupa Robocza wzywa europejskiego prawodawcę do zamieszczenia tego elementu w dyrektywie, w szczególności dlatego, że aspekt ten jest obecny zarówno w obecnej dyrektywie (95/46/WE), jak i decyzji ramowej o ochronie danych (2008/977/WSiSW).

Również przepisy dotyczące zawiadomienia o naruszeniu powinny być spójne w obu instrumentach, tymczasem Grupa Robocza stwierdza różnice w sektorze ochrony porządku publicznego jeżeli chodzi o powiadamianie osób fizycznych. Przykładowo nie zawsze może być możliwe poinformowanie osób fizycznych o naruszeniu w określonym terminie, ponieważ zaszkodziłoby to dochodzeniom lub innym operacjom realizowanym przez organy ścigania. OOD może mieć również szczególną rolę w ocenie potrzeby zawiadomienia osoby fizycznej oraz ustaleniu właściwego momentu do zawiadomienia, biorąc również pod uwagę stosowność technologicznych środków ochrony.

Na koniec należy stwierdzić, że przepisy o profilowaniu i automatycznym przetwarzaniu (art. 9) są niespójne z rozporządzeniem, ponieważ sformułowanie zawarte w dyrektywie nie obejmuje właściwych elementów, takich jak ocena zachowania.

Transfery międzynarodowe

Ogólne zasady przekazywania i dalszego przekazywania danych

Artykuł 33 zawiera przepisy dotyczące zarówno pierwotnego, jak i dalszego przekazywania danych osobowych do państw trzecich lub organizacji międzynarodowych. Grupa Robocza jest zdania, że potrzebne jest wyraźne rozróżnienie tych sytuacji, co umożliwiłoby dodatkowe ograniczenie dalszego przekazywania, np. uwzględniając wyraźne powiązanie z celem, dla którego dane zostały pierwotnie zgromadzone oraz wcześniejszą zgodę przesyłającego organu. Ponadto odbiorcą danych musi być właściwy organ w rozumieniu dyrektywy.

Negatywne decyzje w sprawie odpowiedniego poziomu ochrony

Grupa Robocza uważa, że nie ma jasności co do celu decyzji o braku odpowiedniej ochrony oraz w jaki sposób funkcjonowałyby one w praktyce. Z treści dyrektywy wynika, że taka decyzja prowadziłaby do blokady wszystkich transferów międzynarodowych do określonego państwa trzeciego, organizacji międzynarodowej lub sektora przetwarzania. Artykuły 34 ust. 6 i art. 35 ust. 1 można jednak także interpretować w taki sposób, że umożliwiają one przekazywanie danych do państw uznanych za niezapewniające odpowiedniej ochrony tak długo jak samoocena adekwatności ochrony przeprowadzona przez administratora lub podmiot przetwarzający przynosi zadowalające rezultaty oraz uzgodniono odpowiednie gwarancje. Dlatego też wzywa się europejskiego prawodawcę do dostosowania przepisów w taki sposób, by było jasne, jakie są konsekwencje decyzji stwierdzającej brak odpowiedniej ochrony oraz w jaki sposób decyzje takie mają funkcjonować w praktyce.

Operacje przekazywania dzięki odpowiednim gwarancjom

Dyrektywa przewiduje w art. 35 możliwość przekazania danych osobowych do państw trzecich lub organizacji międzynarodowych w sytuacjach, w których Komisja nie podjęła

decyzji stwierdzającej odpowiedni poziom ochrony. Grupa Robocza uważa, że jeśli takie transfery dokonywane są na podstawie samooceny, właściwy organ musi dopilnować ustanowienia odpowiednich gwarancji w prawnie wiążącym instrumencie. Ponadto zdaniem Grupy Roboczej powinny zostać wprowadzone elementy określone w art. 26 ust. 2 dyrektywy 95/46/WE, które powinny stanowić minimum aspektów uwzględnianych przy samoocenie. Proces prowadzący do samooceny musi zostać w pełni udokumentowany i udostępniony OOD na żądanie.

Odstępstwa

Grupa Robocza wyraża zaniepokojenie odstępstwami, zgodnie z którymi możliwe jest przekazywanie danych osobowych bez wydania decyzji o stwierdzeniu odpowiedniego poziomu ochrony lub bez odpowiednich gwarancji (art. 36), w szczególności odstępstw na mocy lit. c), d) i e) tego artykułu. Wyjątki te stworzyłyby możliwość dokonywania wielu międzynarodowych transferów w indywidualnych przypadkach, o ile tylko uznane one zostałyby za „konieczne”. Należy jasno określić, że wszelkie odstępstwa muszą być interpretowane zawężająco, tak by transfery dokonywane na ich podstawie były raczej wyjątkiem niż normą. Należy również unikać przepisów, których treść wskazywałaby na możliwość, by zwykłe oświadczenie o tym, że dany transfer uznawany jest za konieczny, bez bliższych wyjaśnień, wystarczyło do powołania się na te odstępstwa, a tym samym umożliwiało dokonywanie szeroko zakrojonych transferów międzynarodowych w indywidualnych przypadkach bez istnienia na miejscu jakichkolwiek gwarancji ochrony danych osobowych osoby zainteresowanej. Dlatego też Grupa Robocza uważa, że treść art. 36 lit. c), d) i e) powinna ograniczać możliwość transferów międzynarodowych w indywidualnych przypadkach.

Grupa odnotowuje ponadto, że nie wprowadzono żadnego obowiązku dopilnowania, by korzystanie z wyjątków przewidzianych w art. 36 było dokumentowane. Utrudniłoby to, lub nawet uniemożliwiło sprawdzenie przez organ nadzorczy, czy administrator lub podmiot przetwarzający spełnił warunki odstępstwa. Dlatego też proponujemy wprowadzenie takiego obowiązku poprzez dodanie poniższego ustępu: „2. Wykorzystanie tych odstępstw musi być dokumentowane, a dokumentacja musi być udostępniana na wniosek organowi nadzorczemu.”.

Grupa Robocza uważa wreszcie, że co do zasady w przypadku transferów międzynarodowych, w sytuacji, w której nie ma decyzji stwierdzającej odpowiedni poziom ochrony, państwa członkowskie powinny mieć możliwość decydowania czy i w jakim zakresie OOD będą zaangażowane w transfery międzynarodowe.

Kompetencje OOD i współpraca

Grupa Robocza z ubolewaniem przyjmuje fakt, że przepisy dotyczące kompetencji OOD nie są bardzo szczegółowe, ani zgodne z przepisami zawartymi w rozporządzeniu. Konkretnie dyrektywa nie zawiera przepisów dotyczących dostępu do pomieszczeń, tak jak to przewiduje rozporządzenie. Możliwość uzyskiwana przez organ regulacyjny w razie potrzeby dostępu do pomieszczeń administratora danych powinna istnieć we wszystkich sektorach.

Dyrektywa przewiduje wzajemną pomoc OOD, nie zawiera jednak terminów zapisanych w rozporządzeniu. Grozi to brakiem spójności, zatem wskazówki dotyczące terminów wynikające z rozporządzenia powinny być uwzględnione w obu instrumentach. Podobnie, w

celu zagwarantowania spójności w obu instrumentach dyrektywa powinna obejmować możliwość uczestniczenia przez OOD we wspólnych operacjach.

Braki

Grupa Robocza z ubolewaniem przyjmuje fakt, że dyrektywa nie zawiera przepisów dotyczących ustanowienia terminów, kontroli i innych gwarancji, takich jak ograniczenie wykorzystywania danych do przypadków ścigania poważnych przestępstw itd. Grupa Robocza odnotowuje treść art. 37, który przewiduje obowiązek informowania przez administratora odbiorcę danych o wszelkich ograniczeniach przetwarzania oraz podjęcia wszystkich racjonalnych kroków na rzecz zagwarantowania, by były one przestrzegane. Artykuł 37 ma jednak zastosowanie jedynie do państw trzecich. Nie podano uzasadnienia, dlaczego dyrektywa nie zawiera podobnego przepisu, gdy dane osobowe przekazywane są między państwami członkowskimi Unii. W takich przypadkach także otrzymujące państwa członkowskie powinno być zobowiązane do przestrzegania wszelkich ograniczeń przetwarzania nałożonych przez przekazujące państwo członkowskie. Grupa Robocza z zaskoczeniem przyjmuje fakt, że dyrektywa stanowi w tym kontekście krok w tył w porównaniu z decyzją ramową 2008/977/WSiSW.

Grupa Robocza zwraca uwagę na fakt, że właściwe organy, które przekazały dane, nie zostały zobowiązane do poinformowania odbiorcy, że przekazane dane były niepoprawne lub zostały przekazane niezgodnie z prawem. Taki obowiązek ma zasadnicze znaczenie w warunkach swobodnego przepływu informacji w obszarze ochrony porządku publicznego. Artykuł 39 ust. 2 przewiduje możliwość zdecydowania przez państwa członkowskie, by OOD odpowiedzialnym za nadzorowanie przestrzegania rozporządzenia i dyrektywy był ten sam organ. Biorąc pod uwagę specyfikę krajową, zwłaszcza w państwach, w których istnieją OOD na szczeblu niższym niż krajowy, Grupa Robocza istotnie wolałaby, by za nadzór nad przestrzeganiem obu instrumentów odpowiadał jeden OOD. Zagwarantowałoby to spójność w stosowaniu przepisów.

Na koniec Grupa Robocza wyraża ubolewanie, że dyrektywa nie zawiera przepisu dotyczącego przekazywania podmiotom prywatnym lub innym organom niebędącym właściwymi organami na mocy dyrektywy. Dlatego też Grupa Robocza wzywa europejskiego prawodawcę do dodania przepisu umożliwiającego transfer danych z obszaru ochrony porządku publicznego podmiotom prywatnym wyłącznie w ściśle opisanych okolicznościach określonych prawem.

Sporządzono w Brukseli dnia 23 marca 2012 r.

*W imieniu Grupy Roboczej
Przewodniczący
Jacob KOHNSTAMM*

Belgijski organ ochrony danych oraz rumuński organ ochrony danych zdecydowały się wstrzymać od głosowania wyłącznie z tej przyczyny, że nie popierają wyboru rozporządzenia jako odpowiedniego instrumentu prawnego.

Również organ ochrony danych Republiki Czeskiej wstrzymał się od głosowania.

Estoński organ ochrony danych głosował przeciwko opinii, ponieważ ma wątpliwości, czy proponowany pakiet reform odpowiada zadeklarowanym celom. Organ ten dostrzega zbyt wiele zasadniczych niepokojących aspektów w pakiecie, takich jak:

- 1) brak odpowiedniej oceny skutków (negatywna opinia Rady ds. Oceny Skutków);
- 2) forma bezpośrednio stosowanego rozporządzenia dla przepisów ramowych;
- 3) większe obciążenia administracyjne;
- 4) zakres delegacji do stanowienia przepisów;
- 5) osłabienie krajowych OOD, ochrona praw do prywatności, w których aspekt czasowy ma krytyczne znaczenie, zostaje osłabiona, przedłużenie środków ochrony;
- 6) problem kompetencji w odniesieniu do projektu dyrektywy o ochronie danych w obszarze policji i wymiaru sprawiedliwości w sprawach karnych;
- 7) zaprzeczenie zasadzie pomocniczości;

Dlatego też estoński organ ochrony danych nie zgadza się z głównymi konkluzjami:

- 1) projekt rozporządzenia jest zbyt słaby, by mieć „ogólnie pozytywne podejście”;
- 2) nie uważamy, że projekt dyrektywy w obszarze policji i wymiaru sprawiedliwości jest zbyt skromny. Uważamy, że jest on zbyt daleko idący ze względu na brak kompetencji do stanowienia prawa w obszarze krajowego prawa procesowego.