

Załącznik

Kluczowe tematy z perspektywy trilogu

W następstwie już wydanych opinii i oświadczeń dotyczących reformy ochrony danych¹, Grupa Robocza chciałaby wyrazić swoje poglądy w odniesieniu do określonych problematycznych obszarów, które wymagają dalszej uwagi w perspektywie trilogu między instytucjami europejskimi.

Istotne jest, aby wyniki tych negocjacji doprowadziły do przyjęcia nowych ram regulacyjnych zapewniających poszanowanie podstawowych praw obywateli oraz biorących pod uwagę interesy innych interesariuszy. Rozporządzenie powinno być na tyle proste, skutecznie i jasne, na ile to możliwe. Wymaga to odpowiedniego wyważenia, aby zagwarantować wysoki poziom ochrony osób oraz pozwolić przedsiębiorstwom na utrzymanie innowacyjności i konkurencyjności. Ponadto w tekście rozporządzenia należy powstrzymać się od wnikania w kwestie szczegółowej implementacji. Kwestie te trzeba pozostawić Europejskiej Radzie Ochrony Danych, która ma wypracować wytyczne i zasady postępowania. Grupa Robocza byłaby wdzięczna za możliwość rozpoczęcia pracy nad wytycznymi i zasadami postępowania od daty przyjęcia rozporządzenia.

Rozdział I/ Przepisy ogólne

1/Przedmiot i cel

Rada UE zapewnia państwom członkowskim możliwość wprowadzenia “bardziej szczegółowych przepisów w celu dostosowania stosowania rozporządzenia w odniesieniu do przetwarzania danych osobowych w celu wypełnienia obowiązku prawnego lub w celu wykonania zadania realizowanego w interesie publicznym lub wykonania władzy publicznej powierzonej administratorowi lub innych określonych sytuacji przetwarzania”.

¹WP191, WP199, WP222 Dodatkowe oświadczenia w sprawie pakietu reformy z 27.02.2013 r., 11.12 2013 r. oraz 16.04.2014 r.

17 czerwca 2015 r.

Grupa Robocza podkreśla, że jeżeli przepis ten będzie utrzymany, należy go rozumieć jako zapewnioną państwom członkowskim możliwość określenia i dostosowania postanowień rozporządzenia bez obniżenia poziomu ochrony.

Uznając potrzebę lokalnego dostosowania w niektórych przypadkach, Grupa Robocza chciałaby stanowczo podkreślić, że zapewniona możliwość takiej elastyczności nie powinna obniżać poziomu ochrony przewidzianego przez rozporządzenie oraz że celem nadal pozostaje maksymalna harmonizacja.

Zakres rzeczowy

Granice między rozporządzeniem a dyrektywą

Należy unikać sytuacji, w których to samo przetwarzanie danych (tj.: przetwarzanie w celach administracyjnych) podlega różnym przepisom (tj.: rozporządzenia lub dyrektywy), które nie zapewniają potencjalnie tego samego poziomu gwarancji.

W istocie, nawet jeżeli dyrektywę należy traktować jako minimalny standard umożliwiający państwom członkowskim zapewnienie dodatkowych gwarancji, proponowane przez Radę UE rozszerzenie jej zakresu na wszelkie działania w zakresie przetwarzania w celu „ochrony przed i zapobiegania zagrożeniom dla bezpieczeństwa publicznego” - obok przetwarzania prowadzonego w celach zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, wykrywania ich lub ścigania lub wykonywania kar kryminalnych – doprowadziłoby do różnego poziomu ochrony w zależności od jej wdrożenia.

Ponadto pojęcie “zapobiegania zagrożeniom dla bezpieczeństwa publicznego” nie związane z koncepcją przestępstw jest dosyć niejasne i może otwierać drzwi do objęcia nim wszystkich operacji przetwarzania tylko dlatego, że są prowadzone przez administratorów, którzy działają w najszerszym kontekście egzekwowania prawa”.

Ponadto takie rozszerzenie objęłoby nieokreśloną liczbę organów, których zadania mogą tylko okazjonalnie być związane z tym celem w zakresie dyrektywy.

Obniżyłoby to poziom ochrony danych w sektorze publicznym w porównaniu z tym proponowanym przez rozporządzenie. Nie istnieje istotny powód do zapewnienia takiej elastyczności oraz do usunięcia działań w zakresie bezpieczeństwa publicznego z rozporządzenia.

W celu zapewnienia poziomu ochrony porównywalnego do obecnych ram, Grupa Robocza jest zdania, że działania w zakresie przetwarzania prowadzone w celach innych niż zapobieganie przestępstwom, prowadzenie dochodzeń w ich sprawie, wykrywanie ich lub ściganie lub wykonywanie kar kryminalnych powinny być wyraźnie utrzymane w zakresie rozporządzenia.

Ponadto należy zapewnić, aby “kluczowe” aspekty obu tekstów były spójne oraz jednolicie rozumiane, niezależnie od wybranego instrumentu prawnego, w celu uniknięcia nieporozumień oraz nakładania się przepisów mającego wpływ na poziom ochrony gwarantowany osobom.

Jest to szczególnie prawdziwe w przypadku definicji, zasad, obowiązków, praw osób oraz uprawnień organu nadzorczego.

Wyłączenie do celów domowych

Rada UE rozszerzyła zakres tzw. „wyłączenia do celów domowych” w art. 2(2)(d) rozporządzenia, usuwając słowa “w celach niezarobkowych” oraz “wyłącznie”, które zawarto w wersji Komisji UE, oraz przez odniesienie w motywie 15 przewidujące, że wyłączenie do celów domowych nie oznacza powiązania z działalnością zawodową lub handlową.

Grupa Robocza uznaje cel Rady UE dotyczący nieznacznego rozszerzenia zakresu wyłączenia do celów domowych, aby ograniczyć zakres rozporządzenia, ale uważa, że wszelkie wyłączenia od zasad powinny być formułowane i interpretowane zawężająco.

17 czerwca 2015 r.

Ponadto organy ochrony danych i/lub EROD (Europejska Rada Ochrony Danych) mogą wypracować dalsze szczegóły w celu określenia działań o charakterze "czysto" domowym".

Grupa Robocza popiera ograniczone i dokładnie wyważone wyłączenie do celów domowych mające zastosowanie do działań o charakterze "czysto" domowym, jak przewidziano w dyrektywie 95/46/WE oraz zinterpretowano w orzecznictwie ETS.

Zakres terytorialny

PE przewiduje, że rozporządzenie ma zastosowanie tylko do przetwarzających spoza UE, obok administratorów spoza UE, gdzie przetwarzanie związane jest z:

- (a) oferowaniem dóbr lub usług, niezależnie od tego, czy wymagane jest dokonanie płatności przez osobę, której dane dotyczą, dla takich osób, których dane dotyczą w Unii;; lub
- (b) monitorowanie ich zachowania, o ile ich zachowanie ma miejsce w Unii Europejskiej

Rozważając wprowadzenie w rozporządzeniu kolejnej odpowiedzialności prawnej dla przetwarzających odrębnie od administratorów, wskazane byłoby, aby przepisom rozporządzenia podlegały działania w zakresie przetwarzania prowadzone przez przetwarzających nie mających siedziby w UE, gdzie przetwarzają oni dane osobowe w imieniu administratorów danych podlegających rozporządzeniu. W przeciwnym razie system prawny będzie różny, w zależności od tego, czy przetwarzający ma siedzibę poza UE czy w UE. W przypadku przetwarzających z siedzibą w UE, odpowiedzialność zostanie sformułowana w rozporządzeniu i będzie ją mogła bezpośrednio egzekwować osoba, której dane dotyczą. Przeciwnie, w przypadku przetwarzających spoza UE odpowiedzialność nadal będzie odpowiedzialnością umowną, tak jak obecnie.

Grupa Robocza chciałaby zwrócić uwagę na potrzebę objęcia przepisami rozporządzenia przetwarzających spoza UE w sytuacji, gdy działają jako administratorzy podlegający rozporządzeniu.

Definicje

Zgoda

Nie powinno być wątpliwości co do elementów składających się na zgodę oraz zamiaru wyrażenia zgody przez osobę, której dane dotyczą.

Chociaż zgoda może być wyrażona na wiele różnych sposobów, na przykład poprzez oświadczenie lub działanie afirmatywne, niezbędny wymóg jest taki, aby takie oświadczenie lub działanie wyraźnie oznaczało zgodę osoby, której dane dotyczą, na przetwarzanie dotyczących jej danych osobowych. Konieczne jest wyraźne rozróżnienie między systemem opt-in a opt-out.

W związku z tym pojęcie jednoznacznej zgody przewidziane przez Radę UE w motywie 25 może prowadzić do nieporozumień w zakresie celu proponowanego tekstu, szczególnie w Internecie, gdzie obecnie zbyt często używa się niewłaściwej zgody.

Wymóg, aby zgoda była *wyraźna* stanowi istotne wyjaśnienie, rzeczywiście umożliwiając osobom, których dane dotyczą, realizację ich praw.

Ponadto zgoda powinna być świadoma i dotyczyć określonego celu, zatem niedopuszczalna byłaby żadna 'szeroka zgoda'.

Grupa Robocza chciałaby wyrazić poparcie dla propozycji wymagających, aby zgoda była świadoma, udzielana na określony cel, dobrowolna i wyraźna.

Dane osobowe

Osobę fizyczną można uznać za możliwą do zidentyfikowania, gdy w grupie osób może ją odróżnić od innych i w rezultacie traktować inaczej. Oznacza to, że pojęcie identyfikowalności powinno obejmować wyodrębnianie osób.

Grupa Robocza chciałaby wyrazić poparcie dla motywu wyjaśniającego, że możliwość wyodrębnienia to sposób identyfikacji osoby, której dane dotyczą.

Jednak Grupa Robocza uważa, że motyw 24, jak zaproponował Parlament Europejski i Rada UE, nie jest zadowalający, ponieważ mógłby być interpretowany w taki sposób, że numery identyfikacyjne, dane lokalizacyjne, identyfikatory online lub inne szczególne czynniki nie będą konieczne uznane za dane osobowe. Prowadzi to do nadmiernie restrykcyjnej interpretacji pojęcia danych osobowych.

Grupa Robocza chciałaby powtórzyć, że adresy IP, identyfikatory online lub inne szczególne czynniki powinny być uznane, jako ogólna zasada, za dane osobowe, jak stwierdzono także w szeregu orzeczeń TSUE².

Pseudonimizacja

Techniki pseudonimizacji wykorzystywane do ukrycia tożsamości i umożliwiające gromadzenie danych dotyczących tej samej osoby bez konieczności znania jej tożsamości mogą pomóc ograniczyć zagrożenia dla osób.

W rozporządzeniu należy traktować proces pseudonimizacji jako system minimalizacji danych. Nowa kategoria "spseudonimizowanych" lub pseudonimowych danych może prowadzić do nieporozumień i stanowić konia trojańskiego dla nieuzasadnionych szczególnych odstępstw (np. domniemanie prawnie uzasadnionego interesu osoby, której dane dotyczą).

Na przykład, powinno to być uznane jako metoda mająca zastosowanie do administratorów, którzy już przetwarzają zwykłe identyfikatory (takie jak nazwisko, adres), ale później postanawiają wyodrębnić informacje i utworzyć pseudonimy. Jako narzędzie ochrony prywatności, pomaga to zminimalizować zakres przetwarzanych informacji i następnie zagrożenia (np. w sektorze naukowym, gdzie przetwarzane są „kluczowe zakodowane dane”).

² TSUE 29 stycznia 2008 Promusicae (C-275/06), TSUE 8 kwietnia 2014 Digital Rights Ireland ltd (C-293/12)

Grupa Robocza wyraża poparcie dla odniesienia się do pseudonimizacji jako środka bezpieczeństwa i jest przeciwna wprowadzeniu nowej kategorii danych z pojęciem “danych pseudonimowych”.

Rozdział II/ Zasady

Ograniczenie celu

Zasada ograniczenia celu jest jedną z kluczowych zasad ochrony danych. Powstała w celu ustalenia granic, w ramach których dane osobowe gromadzone w określonym celu mogą być przetwarzane i mogą być dalej wykorzystywane. Administrator może gromadzić dane tylko w określonych, wyraźnych i legalnych celach, a gdy dane zostaną już zgromadzone, nie mogą być dalej przetwarzane w sposób niezgodny z tymi celami.

Ograniczenie celu chroni osoby, których dane dotyczą, ustanawiając ograniczenia co do tego, jak administratorzy mogą wykorzystywać ich dane, oferując również niejaką elastyczność dla administratorów.

Grupa Robocza jest zdania, że pozwolenie administratorom na dalsze przetwarzanie danych w celach niezgodnych z pierwotnymi celami, o ile znajdą nową odpowiednią podstawę prawną, podważy tę fundamentalną zasadę.

W szczególności Grupa Robocza uważa, że umożliwiając administratorowi przetwarzanie danych w niezgodny z przepisami sposób, gdy administrator ma nadrzędny interes w zakresie przetwarzania, dalsze przetwarzanie będzie strywializowane w takim stopniu, że utoruje drogę do zakwestionowania podstawowej zasady ograniczenia celu.

Zgodnie z obecnymi ramami prawnymi przetwarzanie danych osobowych w sposób niezgodny z celami określonymi przy gromadzeniu jest sprzeczne z prawem i w związku z tym zakazane. Administrator nie może legitymizować niezgodnego przetwarzania po prostu opierając się na nowej podstawie prawnej. Nowe przepisy prawne powinny zapewnić co najmniej taki sam poziom ochrony jak oferowany przez obecną dyrektywę.

Dalsze przetwarzanie powinno być dozwolone tylko w przypadku ustalenia zgodności w wyniku dokładnej oceny biorącej pod uwagę wszelkie istotne okoliczności zarówno pierwotnych, jak i dalszych operacji przetwarzania i pod warunkiem, że administrator może znaleźć odpowiednią podstawę prawną. Nie należy mylić zgodności z legalnością.

Ustalenie, że dalsze wykorzystywanie jest zgodne z początkowym nie oznacza, że dane mogą być przetwarzane bez ważnej podstawy prawnej lub opierając się na podstawie prawnej, która legitymizowała pierwotne przetwarzanie. Zgodność i legalność to łączne wymogi, a w celu zmiany celu, który nie jest zgodny, musi być zastosowana jedna z podstaw prawnych.

Grupa Robocza stanowczo zaleca usunięcie ust. 6.4 propozycji, który przewiduje możliwość dalszego przetwarzania danych przez administratora, jeżeli cel jest niezgodny z pierwotnym.

Przetwarzanie w zgodnych celach powinno zawsze wymagać własnej podstawy prawnej.

Przetwarzanie niezbędne do celów badań archiwalnych, historycznych, statystycznych i naukowych

Ust. 6.2 jest sformułowany w sposób, który można by zinterpretować jako ustanawiający nową i niezależną podstawę prawną, na mocy której przetwarzanie dla celów badań historycznych, statystycznych, naukowych (oraz archiwalnych w wersji Rady UE) byłoby legalne bez potrzeby opierania się na innej podstawie prawnej i pod warunkiem, że warunki i zabezpieczenia art. 83 są respektowane. Należy wyraźnie określić, że ust. drugi artykułu 6 nie wyłącza konieczności zapewnienia zgodności także z ust. pierwszym artykułu 6. Wszelkiego rodzaju przetwarzanie powinno spełniać test legalności.

Ponadto wydaje się, że artykuł 9(2)i. ostatniego projektu Rady UE również legitymizuje przetwarzanie danych szczególnie chronionych w tych celach per se, bez konieczności określonej podstawy prawnej.

17 czerwca 2015 r.

Ponadto artykuł 83 Rady UE pozwala państwom członkowskim na wprowadzenie wielu odstępstw od praw osób, których dane dotyczą.

Z drugiej strony wspólne stanowisko przyjęte przez Parlament Europejski wydaje się określać niepotrzebnie restrykcyjne warunki wykorzystywania danych osobowych dotyczących zdrowia w kontekście celów badań historycznych, statystycznych lub naukowych, co będzie możliwe tylko za zgodą osób, których dane dotyczą. Mimo że ten artykuł pozwala państwom członkowskim na zapewnianie wyłączeń w odniesieniu do badań, które służą bardzo ważnemu interesowi publicznemu, to ograniczenie wyboru podstawy prawnej przetwarzania danych dotyczących zdrowia w celach badań statystycznych, historycznych lub naukowych wydaje się wykraczać ponad to, co jest konieczne do ochrony praw osoby, której dane dotyczą, oraz może ograniczyć operacje przetwarzania, które mogłyby być legalne na podstawie innych podstaw prawnych.

Dalsze przetwarzanie w celach badań archiwalnych, historycznych, statystycznych i naukowych powinno być z założenia uznane za zgodne z pierwotnym celem gromadzenia. Musi być oparte na podstawie prawnej na mocy artykułu 6.1 i spełniać wymogi artykułu 9.2. Wszelki wpływ na właściwe prawa i obowiązki powinien być określony w rozporządzeniu. Stanowisko Rady UE, aby polegać jedynie na prawie krajowym uniemożliwi harmonizację w tym obszarze, podczas gdy badania historyczne, statystyczne i naukowe muszą mieć coraz bardziej unijny międzynarodowy charakter (tj. finansowanie przez UE promuje krajowe działania w ramach UE).

Ponadto Grupa Robocza naprawdę chciałaby ostrzec przed usunięciem słowa "badania" przez Radę UE (również w art. 6). Mogłoby to potencjalnie otworzyć puszkę Pandory dla ewidentnie historycznych i/lub statystycznych celów przez sektor prywatny innych niż cele badawcze.

Grupa Robocza stanowczo popiera następujące elementy

- Dalsze przetwarzanie do celów naukowych, historycznych, statystycznych lub archiwalnych powinno być uznane za zgodne pierwotnym celem gromadzenia;

- Przetwarzanie (czy to pierwotne, czy dalsze) do celów badań naukowych, historycznych, statystycznych i archiwalnych zawsze powinno być oparte na jednej z podstaw prawnych art. 6.1. i spełniać wymogi artykułu 9.2, gdy to konieczne.

Prawnie uzasadniony interes – wykorzystanie danych pseudonimowych

Wykorzystywanie danych pseudonimowych jako sposobu zapewnienia gwarancji do zapewnienia rzetelnego przetwarzania danych osobowych może odgrywać rolę w określeniu, czy podstawa prawna w zakresie uzasadnionego interesu może być legalnie wykorzystana.

Nadal jest to jednak tylko jeden czynnik spośród wielu a test równowagi zawsze wymaga, aby oceniać również cel przetwarzania.

Grupa Robocza nie popiera przepisów, które można by interpretować jako zwolnienie z obowiązku administratora do przeprowadzenia ważnego testu równowagi w przypadku przetwarzania danych pseudonimowych.

Przetwarzanie nie pozwalające na identyfikację

Grupa Robocza ma obawy co do szerokiej interpretacji, którą mogłaby być stosowana wobec artykułu 10, jak zaproponował Parlament Europejski.

Artykuł 10 zaproponowany przez Parlament Europejski może prowadzić do zwolnienia administratorów lub przetwarzających z przestrzegania rozporządzenia przy przetwarzaniu danych pseudonimowych.

Dane pseudonimowe, zważywszy że pozwalają na wyodrębnienie i inne traktowanie osoby fizycznej, pozostają danymi osobowymi, a ich wykorzystywanie nie powinno zwalniać administratorów/przetwarzających z przestrzegania obowiązków przewidzianych przez rozporządzenie (np. kluczowe zasady, obowiązki w zakresie rozliczalności ...).

Jednak administrator nie powinien mieć możliwości bycia zobowiązanym do gromadzenia większego zakresu informacji od osoby, której dane dotyczą, w celu realizacji jej praw, jeżeli nie może bezpośrednio zidentyfikować osoby, której dane dotyczą. Od chwili, gdy osoba, której dane dotyczą, będzie mogła być uwierzytelniona, powinna być możliwa realizacja jej praw. W praktyce, jeżeli administrator wyodrębni osoby, których dane dotyczą, na podstawie identyfikatorów cyfrowych, osoba, której dane dotyczą, powinna być uprawniona do realizacji jej praw przez uwierzytelnienie się przy pomocy tych identyfikatorów cyfrowych.

Grupa Robocza popiera propozycje wyjaśniające, że jeżeli cele, w których administrator przetwarza dane osobowe, nie wymagają lub już nie wymagają bezpośredniej identyfikacji osoby, której dane dotyczą, przez administratora, administrator nie może być zobowiązany do zatrzymania lub uzyskania dodatkowych informacji ani do zaangażowania się w dodatkowe przetwarzanie jedynie w celu zgodności z artykułami 15, 16, 17, 18 z wyjątkiem sytuacji, gdy osoba, której dane dotyczą tego wymaga i przedstawia dodatkowe informacje umożliwiające jej uwierzytelnienie.

Rozdział III/ Prawa osoby, której dane dotyczą

Informacje dla osoby, której dane dotyczą

Grupa Robocza uważa, że informacje dotyczące środków bezpieczeństwa, okresu zatrzymywania, właściwych zabezpieczeń w odniesieniu do przekazywania danych do państw trzecich, oraz leżącej u podstaw logiki przetwarzania danych winny być przekazane osobom, których dane dotyczą.

Informacje mogą być przekazywane osobom, których dane dotyczą, przy wykorzystaniu warstwowych informacji o prywatności rozpowszechniających wymagane informacje w łatwo odczytywalnym formacie.

Grupa Robocza popiera propozycje określające, że informacje dotyczące dalszego przetwarzania, okresu zatrzymywania danych, zabezpieczeń wdrożonych w przypadku międzynarodowego przekazywania danych, środków bezpieczeństwa powinny być przekazywane przez administratora osobom, których dane dotyczą.

Podejście oparte na ryzyku (RBA) w prawach osoby, której dane dotyczą

Jak określono w poprzedniej opinii³, Grupa Robocza podkreśla, że prawa przyznane osobom, których dane dotyczą przez prawo UE powinny być respektowane, niezależnie od poziomu zagrożeń, które te ostatnie napotykają w związku z określonym przetwarzaniem danych (np. prawo dostępu, poprawienia, usunięcia danych oraz wyrażenia sprzeciwu, przejrzystość, prawo do bycia zapomnianym, prawo do przenoszenia danych).

W związku z tym niektóre odniesienia w stanowisku Rady UE do konieczności „wzięcia pod uwagę okoliczności” lub „brania pod uwagę celów” przy przyznawaniu praw osobom, których dane dotyczą, tworzą niepewność i potencjalne pole do interpretacji, co mogłaby prowadzić do obniżenia poziomu ochrony osób, których dane dotyczą.⁴

Możliwość przenoszenia danych

Jednym z celów prawa do przenoszenia danych jest uprawnienie obywateli do sprawowania kontroli nad swoimi danymi osobowymi.

³ Oświadczenie na temat roli podejścia opartego na ryzyku w ramach prawnych ochrony danych WP218. 30 maja 2014 r.

⁴ Patrz na przykład artykuł 16 stanowiska Rady: „Zważywszy na cele, w których przetwarzano dane, osoba, której dane dotyczą, posiada prawo do uzyskania uzupełnienia niepełnych danych (...).

17 czerwca 2015 r.

W celu zapewnienia większej skuteczności tego prawa, osoba, której dane dotyczą, powinna być w stanie przekazywać dane osobowe dotyczące jej lub osoby trzeciej od chwili, gdy je jej przekazano.

Ponadto dane powinny, na wniosek osoby, której dane dotyczą, być przekazywane bezpośrednio od administratora do innego administratora.

Powinno to mieć zastosowanie do wszystkich rodzajów przetwarzania, niezależnie od podstawy prawnej wykorzystanej do tego przetwarzania.

Grupa Robocza popiera propozycje w odniesieniu do szerokiego zakresu i treści prawa do przenoszenia danych, ale popiera utrzymanie tego prawa na mocy artykułu 18 jako odrębnego i niezależnego nowego prawa z prawa dostępu.

Prawo dostępu

Prawo dostępu dla osoby, której dane dotyczą, jest podstawowym prawem, które ma zastosowanie nawet, gdy dane osobowe osoby, której dane dotyczą, to także dane osobowe jednej lub kilku innych osób, których dane dotyczą. W takich przypadkach administrator danych musi wyważyć prawo dostępu dla wnioskującej osoby, której dane dotyczą, bez szkody dla praw i wolności innych osób, których dane dotyczą, jaką przyznanie takiego dostępu mogłoby wyrządzić.

Jest to przewidziane przez ograniczenia praw osób, których dane dotyczą, gdy są to niezbędne i proporcjonalne środki do ochrony praw i wolności innych.

Każde ogólne ograniczenie dostępu do danych osobowych, w tym także danych osobowych innej osoby, której dane dotyczą, stanowiłoby ograniczenie praw osób, których dane dotyczą, obecnie przewidzianych na mocy dyrektywy 95/46/WE.

W związku z tym propozycja Rady Unii Europejskiej ograniczająca prawo uzyskania kopii danych osobowych przy udostępnianiu danych osobowych innym osobom, których dane dotyczą, mogłaby prowadzić do ograniczenia prawa dostępu.

Grupa Robocza uważa, że ogólne ograniczenie prawa dostępu dla osoby, której dane dotyczą, do danych osobowych, w tym także do danych osobowych innych osób, których dane dotyczą, jest nieuzasadnione ze względu na ochronę prywatności i stanowiłoby ograniczenie istniejących praw osób, których dane dotyczą.

Prawo do wyrażenia sprzeciwu

Grupa Robocza ma obawy co do propozycji Rady UE, aby ograniczyć realizację prawa do wyrażenia sprzeciwu tylko do takich przypadków, gdy przetwarzanie danych jest oparte jest na prawnie uzasadnionym interesie administratora lub na interesie publicznym bądź też jego podstawą jest wykonywanie władzy publicznej powierzonej administratorowi ⁵.

Propozycja ta utoruje drogę do niedopuszczalnego obniżenia obecnego poziomu ochrony ustanowionego w dyrektywie 95/46/WE oraz w transponujących ją przepisach w państwach członkowskich.

Biorąc pod uwagę, co jest wykonalne, Grupa Robocza popiera rozszerzenia prawa osoby, której dane dotyczą, do wyrażenia sprzeciwu ponad to, co jest obecnie ustanowione na mocy artykułu 14 dyrektywy.

Ograniczenia

Rada Unii Europejskiej dodała nowe podstawy pozwalające na derogację praw osób, których dane dotyczą (art. 12 do 20 oraz 5) takie jak „ważne cele ogólnych interesów publicznych Unii lub państwa członkowskiego, , oraz wykonywanie roszczeń cywilnych.”

⁵ Rada UE/ Artykuł 19.1 “Osoba, której dane dotyczą, ma prawo do wyrażenia sprzeciwu wobec przetwarzania dotyczących jej danych osobowych w każdym momencie, na podstawie jej konkretnej sytuacji, w oparciu o punkty (...) (e) lub (f) artykułu 6(1), pierwsze zdanie art. 6(4) w połączeniu z punktem (e) artykułu 6(1) lub drugie zdanie artykułu 6(4).”

Grupa Robocza zauważyła, że takie bardzo ogólne i niejasne odstępstwa idące dalej niż obecnie dozwolone podstawy prawne na podstawie dyrektywy stoją w sprzeczności wobec pewności prawnej oraz stanowią naruszenie „prawa wspólnotowego”.

Dodatkowo Grupa Robocza uważa, że środki prawne ograniczające prawa oraz obowiązki, które mają być przyjęte zgodnie z art. 21 § 1, powinny zawsze spełniać wymogi art. 8 § 2 Europejskiej Konwencji Praw Człowieka oraz odpowiednie orzecznictwo Europejskiego Trybunału Praw Człowieka oraz art. 8 Karty Praw Podstawowych Unii Europejskiej.

Odpowiednio, te środki legislacyjne muszą zawierać, jako zasady a nie tylko „tam gdzie to odpowiednie” (jak zaproponowała Rada UE), cele przetwarzania lub kategorie celów przetwarzania, kategorie danych osobowych, wprowadzony zakres ograniczeń, opis administratora lub kategorii administratorów oraz właściwe środki ochronne biorąc pod uwagę charakter, zakres oraz cele przetwarzania oraz zagrożenia dla praw oraz wolności osób, których dane dotyczą.

Profilowanie

Profilowanie znalazło drogę do wielu obszarów życia (np. profile konsumentów, profile ruchu, profile użytkowników oraz profile społeczne). W związku z szeroką dostępnością oraz możliwością łączenia danych w Internecie, osoby, których dane dotyczą mogą być przedmiotem niewystarczającej przejrzystości i z tego powodu mogą mieć poczucie, że nie są w stanie wykonywać wystarczającej kontroli nad przetwarzaniem ich danych osobowych.

W swojej poprzedniej Opinii⁶, Grupa Robocza podkreśliła konieczność zapewnienia większej pewności prawnej oraz większej ochrony dla osób w odniesieniu do przetwarzania danych w kontekście profilowania. Zidentyfikowała potrzebę wprowadzenia jasnej definicji profilowania w następstwie podejścia Rady Europy.⁷

⁶ Dokument na temat kluczowych elementów definicji oraz przepisów o profilowaniu w ogólnym rozporządzeniu o ochronie danych / 13 maja 2013 r.

⁷ Zalecenie CM/Rec(2010)13 Komitetu Ministrów do państw członkowskich w sprawie ochrony osób w związku z automatycznym przetwarzaniem danych osobowych w kontekście profilowania.

Grupa Robocza ocenia, że propozycje Rady UE⁸ są niejasne oraz nie przewidują wystarczających środków ochronnych, które powinny być zastosowane.

Grupa Robocza ponawia swój apel o przepisy dające osobie, której dane dotyczą maksimum kontroli oraz autonomii przy przetwarzaniu danych w związku z profilowaniem.

Przepisy powinny jasno zdefiniować cele, dla których mogą być tworzone oraz wykorzystywane profile, w tym szczególne obowiązki administratorów informowania osoby, której dane dotyczą, w szczególności o ich prawach do wyrażenia sprzeciwu wobec utworzenia oraz wykorzystania profilów.

Grupa Robocza zaleca modyfikację art. 20 poprzez dodanie przepisów dotyczących celów, dla których profile mogą być tworzone oraz wykorzystywane oraz szczególnych obowiązków administratorów do poinformowania osoby, której dane dotyczą.

⁸ Art. 20.1b Obowiązek administratora "wdrożenia odpowiednich środków w celu zabezpieczenia praw oraz wolności oraz uzasadnionych interesów osoby, której dane dotyczą, takich jak prawo do uzyskania ludzkiej interwencji od administratora danych w celu wyrażenia swojego punktu widzenia i sprzeciwienia się decyzji".

Rozdział IV/ Obowiązki administratorów danych oraz podmiotów przetwarzających

Podejście oparte na ryzyku/Rozliczalność

Grupa Robocza uważa, że rozliczalność jest podstawową zasadą praktyk prywatności, która nie może być pozbawiona swojej istoty poprzez nieodpowiednie zastosowanie podejścia opartego na ryzyku.

Administratorzy oraz podmioty przetwarzające powinny być rozliczalne, co powinno być zasadą przy zachowaniu zgodności z wymogami ochrony danych, włączając w to wykazanie zgodności w odniesieniu do jakiegokolwiek przetwarzania danych, niezależnie od charakteru, zakresu, kontekstu, celów przetwarzania oraz możliwych zagrożeń dla osób, których dane dotyczą.

Grupa Robocza byłaby za dodaniem motywu wyjaśniającego, że rozliczalność jest fundamentalną zasadą, która znajduje zastosowanie do wszystkich operacji przetwarzania.

Przedstawiciele administratorów nie posiadających siedziby w Unii

Wyłączenie administratorów nie posiadających siedziby na terytorium UE spod obowiązku wyznaczania przedstawiciela, jeżeli przetwarzanie jest „rzadkie oraz mało prawdopodobne, że przetwarzanie będzie skutkowało zagrożeniem dla praw oraz wolności osób, których dane dotyczą, tak jak to zaproponowała Rada, jest zbyt niejasne⁹, i może ograniczyć skuteczność rozporządzenia. Każdy wyjątek powinien być oparty na obiektywnych kryteriach, takich jak charakter, regularność i skala czynności przetwarzania danych ukeirunkowanych na UE, co pomoże dokonać pomiaru zagrożeń. Ponadto przedstawiciele powinni posiadać osobowość prawną, tak aby schemat odpowiedzialności był operacyjny oraz efektywny.

⁹ Art. 25

Dokumentacja

Dokumentacja jest ważnym narzędziem dla administratorów w należyтым zarządzaniu ich obowiązkami ochrony danych. Administratorzy nie mogą zapewnić zgodności bez wiedzy na temat tego, jakie dane osobowe przetwarzają oraz jak je przetwarzają.

Co więcej, utrzymywanie właściwej dokumentacji jest niezbędnym elementem rozliczalności, pomaga umożliwić wykonanie praw przez osoby, których dane dotyczą oraz wspiera następce postępowania organów ochrony danych. Podczas gdy wymóg wobec administratora lub przetwarzającego utrzymywania dokumentacji musi być skalowalny oraz proporcjonalny wobec ryzyka jakie stanowi przetwarzanie oraz charakter przechowywanych danych osobowych, nie powinien on być przedmiotem całkowitych wyłączeń.

Grupa Robocza uważa, że co do zasady, administratorzy oraz przetwarzający powinni proporcjonalnie dokumentować swoje czynności przetwarzania, aby zapewnić rozliczalność oraz przejrzystość.

Zgłoszenie naruszenia bezpieczeństwa

Grupa Robocza wskazał już w swojej Opinii 1/2009, że powody dwóch rodzajów powiadomień są różne i przypadki w których organy ochrony danych oraz osoby, których dane dotyczą muszą być poinformowane również powinny się różnić. Konieczne jest zapewnienie gwarancji zapewniających, że naruszenia danych nie będą ukrywane, że ocena naruszenia będzie prawidłowo przeprowadzona oraz że osoby, których dane dotyczą będą powiadamiane, gdy będzie to wymagane. Organy nie powinny być powiadamiane w większej liczbie przypadków niż osoby, których dane dotyczą, zatem mogą być w stanie realizować nadzór nad procesem powiadamiania osób, których dane dotyczą. W tym względzie pojęcie wysokiego ryzyka dla praw, wolności i interesów osób, których dane dotyczą, koniecznie nie może być jedynym czynnikiem, który wywołuje powiadomienie organów ochrony danych.

Dodatkowo propozycja Rady UE przewiduje, że administrator, który podjął następne środki w celu zapewnienia, że nie będzie już dłużej prawdopodobne, aby te wysokie zagrożenia dla osoby, której dane dotyczą zmaterializowały się, jest zwolniony obowiązku zawiadomienia osoby, której dane dotyczą oraz organów ochrony danych.

Takie odstępstwo jest zbyt szerokie i może mieć taki efekt, że dla większości administratorów podstawą do nieinformowania zainteresowanych interesariuszy.

Ponadto powiadomienie osób, których dane dotyczą, nie powinno być obowiązkowe, gdy „istnieje prawdopodobieństwo, że rezultatem będzie wysokie ryzyko..”, ale raczej gdy, w znacznym zakresie, „istnieje prawdopodobieństwo, że naruszenie danych osobowych negatywnie wpłynie na dane osobowe lub prywatność” osoby, której dane dotyczą. Pozwoliłoby to na dostosowanie kryteriów do dyrektywy o prywatności i łączności elektronicznej oraz na oparcie się o wytyczne już opublikowane przez Grupę Roboczą lub ENISA.

Grupa Robocza popiera różne progi powiadamiania o naruszeniach ochrony danych osobowych organu lub osób.

Jeżeli chodzi o powiadamianie osób, których dane dotyczą, Grupa Robocza popiera również dostosowanie brzmienia użytego w dyrektywie o prywatności i łączności elektronicznej (powiadomienie osób, których dane dotyczą, gdy „istnieje prawdopodobieństwo, że naruszenie danych osobowych negatywnie wpłynie na dane osobowe lub prywatność osoby, której dane dotyczą...”)

Ocena wpływu na ochronę danych (DPIA)

Zgodnie z tekstem Parlamentu Europejskiego, DPIA staje się drugim krokiem po wstępnej analizie ryzyka, która ma być przeprowadzona przez wszystkich administratorów (oraz tam gdzie to odpowiednie przetwarzających). DPIA byłaby wymagana, jeżeli zidentyfikowano by określone ryzyko, tj. w przypadku gdy przetwarzanie znajduje się na liście „ryzykownych” operacji ustanowionych w art. 32 a) oraz musiałyby być regularnie odnawiana. Chociaż to dwustopniowe podejście ocenne wydaje się bardzo kompletne,

wymagałoby prawdopodobnie dużo pracy, zasobów oraz inwestycji przedsiębiorstw, w szczególności małych i średnich.

Grupa Robocza z zadowoleniem przyjmuje podejście do DPIA, które bierze pod uwagę szerszą perspektywę wpływu na prawa oraz wolności osób, których dane dotyczą, a nie skupia się wyłącznie na ochronie danych osobowych. Ocena wpływu, który niezgodny z prawem przetwarzanie danych osobowych może mieć na szerszy zestaw praw oraz wolności powinno również spajać proponowaną metodologię. Odniesienie do całego cyklu życia przetwarzania danych osobowych jako kontekstu oceny oraz krótki opis kluczowych elementów treści byłyby szczególnie wartościowe.

Dodatkowo Grupa Robocza nie widzi powodu, dlaczego miano by wyłączyć instytucje publiczne z wykonywania oceny wpływu na prywatność, chyba że przetwarzanie wynika z obowiązku prawnego (prawa UE lub państwa członkowskiego) a organ ochrony danych został już skonsultowany.

Grupa Robocza chciałaby wyrazić swoje wsparcie dla podejścia oceny wpływu na prywatność, które bierze pod uwagę szerszy wpływ na prawa oraz wolności osób, których dane dotyczą a nie wyłącznie wpływ na ochronę danych osobowych. Odniesienie do całego cyklu życia przetwarzania danych osobowych byłoby szczególnie pożądane.

Konsultacje z organem ochrony danych

Grupa robocza przywołuje, że administrator oraz przetwarzający są odpowiedzialni za zapewnienie zgodności z rozporządzeniem. Podejście do obowiązkowej konsultacji z organem ochrony danych powinno być zgodne oraz spójne z zasadą rozliczalności.

Grupa robocza uważa, że uprzednia konsultacja z organami ochrony danych powinna być ograniczona do sytuacji, w których ich interwencja jest szczególnie niezbędna do zabezpieczenia praw i wolności osób, których dane dotyczą.

Grupa robocza uważa, że podejście do obowiązkowych konsultacji z organami ochrony danych powinno być spójne z zasadą rozliczalności.

Inspektor Ochrony Danych (Data Protection Officer – DPO)

Inspektor ochrony danych jest kluczowym elementem rozliczalności oraz realnym narzędziem konkurencyjności dla przedsiębiorstw. Mający za zadanie wdrożenie narzędzi rozliczalności (np. dokumentacji, oceny wpływu na prywatność, itd...), powinni być uznawani za “dyrygenta zgodności” oraz pośrednika pomiędzy wszystkimi odpowiednimi interesariuszami (np. Organy nadzorcze, osoby, których dane dotyczą, partnerzy biznesowi).

Grupa robocza uważa, że odwołanie do prawa krajowego, tak jak zaproponowała Rada UE¹⁰, zwiększy ryzyko fragmentacji pomiędzy państwami członkowskimi oraz zmniejszy użyteczność inspektora ochrony danych.

Grupa robocza popiera powołanie inspektora ochrony danych jako obowiązek, przy zachowaniu obiektywnych kryteriów, takich jak rodzaj, ilość danych lub charakter działalności zainteresowanego podmiotu, co pomoże w pomiarze ryzyka.

¹⁰ Art. 35 : Administrator oraz przetwarzający mogą, lub gdy to wymagane przez prawo państwa członkowskiego lub Unii maja wyznaczyć inspektora ochrony danych.

Rozdział V - Przekazywanie

Zasada odpowiedniości

Zasada odpowiedniości, która jest jedną z kluczowych zasad obecnych ram regulacyjnych UE (artykuł 25 dyrektywy UE) powinna być odzwierciedlona oraz jasno wyrażona w rozporządzeniu. Nawet jeżeli zasada odpowiedniości jest umieszczona w częściach rozporządzenia poświęconych decyzjom Komisji w sprawie odpowiedniego poziomu ochrony oraz innych instrumentom przekazywania danych, GR Art. 29 nalega na potrzebę potwierdzenia ogólnej zasady odpowiedniości jako podstawy ram regulacyjnych UE.

Grupa robocza popiera zapewnienie, że rozporządzenie zawiera zasadę odpowiedniości tak jak obecnie art. 25 dyrektywy 95/46.

Odstępstwo na podstawie uzasadnionego interesu

Grupa robocza kilkakrotnie wyraziła obawy odnośnie dodania tak szerokiego odstępstwa na mocy w art. 44 h powalającego na przekazanie do państwa spoza UE ze względu na uzasadniony interes administratora w oparciu o ocenę odpowiednich środków ochronnych. Grupa Robocza Art. 29 zauważa, że do tych obaw odniesiono się w propozycji Parlamentu Europejskiego usuwając ten przepis. Jeżeli ten przepis ma być utrzymany, powinien być co najmniej być stosowany wyjątkowo i tylko w odniesieniu do nie masowego, nie powtarzającego się i nie zorganizowanego przekazywania.

Grupa robocza popiera fakt, że jeżeli art. 44 h) ma być utrzymany, może być wykorzystywany tylko wyjątkowo i tylko w odniesieniu do nie masowego, nie powtarzającego się i nie zorganizowanego przekazywania, podlegając gwarancjom, a w szczególności określonym obowiązkom informacyjnym wobec osób, których dane dotyczą.

Przetwarzający i podprzetwarzający

Rozporządzenie zapewnia powiększoną rolę dla przetwarzających poprzez zapewnienie odpowiedniej ochrony danych w odniesieniu do ram ich własnych przekazywanych danych i również przez uznanie wprowadzenia zasady rozliczalności.

BCR dla przetwarzających są oparte na zasadzie rozliczalności oraz stanowią wartościowe narzędzie dla wykazania zgodności z wymogami ochrony danych. Są również użytecznymi środkami do zapewnienia, tak dalece jak to możliwe, dobrego poziomu ochrony przy przekazywaniu danych.

Ponadto Grupa robocza przyjmuje z zadowoleniem propozycje Rady UE w ust. 1A i 2A art. 26 dotyczące zawarcia zasad dotyczących czynności podprzetwarzania (już wypracowanych w BCR dla przetwarzających) w ramach UE.

Możliwość dla przetwarzających pod-powierzenia części ich działań jest coraz bardziej wykorzystywana w praktyce, w szczególności w kontekście rozwoju przetwarzania w chmurze oraz jest ważne, aby rozporządzenie zajmowało się tym rozwojem.

Stanowisko Rady ma na celu uniknięcie jakiegokolwiek pomylenia ról przetwarzających oraz administratorów¹¹, tak aby zapewnić pewność prawną¹² zostawiając jednak pewną elastyczność dla umawiających się stron.¹³ Warunki zaproponowane na podstawie tych ust. jasno odzwierciedlają stanowisko, które zostało już zajęte przez Grupę Roboczą i z tego powodu są przyjmowane z zadowoleniem.¹⁴

Grupa robocza jest zaniepokojona usunięciem możliwości wykorzystania WRK dla przetwarzających (BCR-P) i uważa za zasadniczą kwestię ich przywrócenie.

¹¹ Poprzez nałożenie obowiązku przejrzystości na administratora oraz jego uprzedniego upoważnienia, co pozwoli mu zachować kontrolę.

¹² Poprzez nałożenie obowiązku, aby na podprzetwarzającego zostały umownie nałożone takie same obowiązki, jakie spoczywają na głównym przetwarzającym oraz zapewnienie, że główny przetwarzający będzie odpowiedzialny za jakiegokolwiek naruszenie spowodowane przez jego pod-przetwarzającego.

¹³ Przez danie możliwości wyboru administratorowi konkretnego lub ogólnego upoważnienia połączonego z mechanizmem opt-out.

¹⁴ WP196 w sprawie przetwarzania w chmurze oraz WP195 w sprawie wiążących reguł korporacyjnych (BCR) dla przetwarzających.

Jednak Grupa Robocza popiera propozycje ustanawiające jasne warunki prawne możliwości przetwarzających do powierzenia części swoich działań, a w szczególności w kontekście rozwoju przetwarzania w chmurze. Warunki prawne powinny zapewnić, aby administratorzy utrzymali kontrole, mieli pełną przejrzystość co do czynności podprzetwarzania i aby zachowany został poziom ochrony podczas całego cyklu przetwarzania.

Dostęp instytucji publicznych

Grupa Robocza przyjmuje z zadowoleniem wprowadzenie do rozporządzenia zasady zgodnie z którą ujawnienie danych osobowych jakiejkolwiek instytucji z państwa trzeciego (sądowi, trybunałowi, instytucji administracyjnej) powinno mieć miejsce jedynie po notyfikowaniu wniosku oraz przed zgodą właściwego organu nadzorczego, bez uszczerbku dla traktatu o wzajemnej pomocy prawnej lub obowiązującej umowy międzynarodowej pomiędzy wnioskującym krajem trzecim a Unią lub państwem członkowskim. Przyjmuje również z zadowoleniem, że zgody udzielane przez organ nadzorczy powinny być oparte na ocenie zgodności wniosku z ogólnym rozporządzeniem o ochronie danych, oraz, że odpowiedni krajowy organ ds. egzekwowania prawa powinien być poinformowany o tym wniosku.

Grupa robocza uważa, że zakres przepisu powinien być szerszy niż wyroki zagranicznych sądów lub trybunałów, lub decyzje instytucji administracyjnych i powinien obejmować jakikolwiek dostęp w imieniu instytucji publicznych lub organów rządowych państw trzecich.

W tym aspekcie, dla wniosków organów ds. egzekwowania prawa, bardziej przejrzyste ramy prawne, takie jak wykorzystanie wzajemnych traktatów o pomocy prawnej (MLAT) lub istniejących umów międzynarodowych w przypadku ujawnień bez zgody na gruncie prawa Unii lub państwa członkowskiego powinny pozostać zasadą. Grupa robocza wierzy ponadto, że w przypadku gdy MLAT (lub porównywalna umowa międzynarodowa) jest przyjęty, odpowiednią instytucją zgodnie z MLAT (lub porównywalną umową międzynarodową) powinna być instytucja zajmująca się wnioskiem a nie organ ochrony danych. Naturalnie tam

17 czerwca 2015 r.

gdzie to konieczne, organ właściwy zgodnie z MLAT powinien skonsultować się z organem ochrony danych tam gdzie to odpowiednie.

W przypadkach gdy kanały współpracy nie istnieją oraz gdy trudno jest zidentyfikować tzw. "organ właściwy" lub gdy takiego nie ma, administrator lub przetwarzający powinni zawiadomić odpowiedni organ ochrony danych.

Grupa robocza uważa kwestię udostępniania danych osobowych instytucji z państwa trzeciego (sąd, trybunał, organ administracyjny) za bardzo ważną kwestię i przyjmuje z zadowoleniem zasadę zawiadamiania organów ochrony danych o takim wniosku.

Grupa robocza uważa ponadto, że w przypadku gdy MLAT (lub porównywalna umowa międzynarodowa) jest przyjęty, odpowiednią instytucją zgodnie z MLAT (lub porównywalną umową międzynarodową) powinna być instytucja zajmująca się wnioskiem a nie organ ochrony danych. W przypadkach gdy kanały współpracy nie istnieją oraz gdy trudno jest zidentyfikować tzw. "organ właściwy" lub gdy takiego nie ma, administrator lub przetwarzający powinni zawiadomić odpowiedni organ ochrony danych.

Rozdziały VI, VII, VII Zarządzanie

Punkt kompleksowej obsługi

Grupa robocza z zadowoleniem przyjmuje usprawnienia poczynione przez obie instytucje w tej kluczowej kwestii oraz które odzwierciedlają obawy uprzednio wyrażone w dokumentach GR Art. 29¹⁵. Bardziej szczegółowo obie instytucje przewidują, że:

- Wszystkie organy nadzorcze pozostaną właściwe na terytoriach swoich państw członkowskich,

¹⁵ Oświadczenie GR29 – główne punkty dla punktu kompleksowej obsługi oraz mechanizmu spójności dla działalności biznesowej oraz jednostek – 16 kwietnia 2014 r.

- Współpraca musi odbywać się pomiędzy wszystkimi organami ochrony danych, których sprawa dotyczy oraz wyznaczonym wiodącym organem ochrony danych w sprawach międzygranicznych,
- Europejska Rada Ochrony Danych wydaje wiążące decyzje tam gdzie to konieczne.

Dodatkowo by zapewnić bliskość obywateli, Rada UE dodała wartościowe elementy:

- Organ ochrony danych jest właściwy jeżeli osoby na jego terytorium są dotknięte przetwarzaniem danych przez administratorów i przetwarzających z siedzibą w lub poza UE.
- Przypadki czysto krajowe lub o niewielkim związku z międzygranicznością są pozostawione organowi ochrony danych.
- Obywatele mają możliwość szukania odwołania w sądach w ich własnym państwie członkowskim.

Grupa robocza chciałaby wyrazić poparcie dla rozwiązania, które zapewnia bliskość wobec obywateli oraz jednakową odpowiedź wobec przedsiębiorstw.

Grupa robocza przywołuje fakt, że proces współpracy powinien być prosty, jasny oraz skuteczny dla wszystkich interesariuszy, aby zapewnić skuteczny nadzór w każdym okolicznościach. Dalsze szczegóły wdrażania powinny pozostawione Europejskiej Radzie Ochrony Danych i należy je wypracować a nie tylko określić w rozporządzeniu.

Uprawnienia organów ochrony danych/sankcje

W celu bycia skutecznym, rozporządzenie powinno zapewnić skuteczne narzędzia dla organów ochrony danych. Uprawnienie do zawieszenia przetwarzania danych, do zapewnienia zgodności operacji przetwarzania danych w określony sposób oraz nałożenia kar, które są wystarczająco odstraszające, srogię oraz proporcjonalne jest kluczowe do zapewnienia zgodności. Grupa Robocza przypomina, że cały zakres uprawnień organów ochrony danych, włączając w to kary powinien być stosowany niezależnie czy administrator jest jednostką publiczną czy prywatną.

Grupa robocza z zadowoleniem przyjmuje wprowadzenie znaczących kar pozwalających organom ochrony danych na podjęcie ich roli jako organów wdrażających i które mogą przyczynić się do wyższego poziomu zgodności administratorów danych zarówno w sektorze publicznym jak i prywatnym. Ponadto organy ochrony danych muszą mieć prawo do ustalenia priorytetów dotyczących przebiegu ich pracy oraz do skoncentrowania się na kwestiach, które mają znaczący wpływ na prawa i wolności osób, których dane dotyczą.

Rada UE nie przewiduje kar administracyjnych w przypadku gdy administrator lub przetwarzający nie zapewniają zgodności ze swoimi obowiązkami na podstawie art. 53 ust. 1¹⁶ – uprawnienia dotyczące postępowań organów ochrony danych. Dla codziennej działalności nadzoru ochrony danych, w szczególności przy przeprowadzeniu inspekcji, uprawnienia do prowadzenia postępowań organów ochrony danych są kluczowym elementem skutecznego nadzoru nad ochroną danych. W rzeczywistości organy ochrony danych mogą zostać skonfrontowane z sytuacją, w której administratorzy/przetwarzający nie zapewniają zgodności z ich obowiązkami poddania się tym postępowaniom. Ma to zastosowanie w szczególności gdy administrator lub przetwarzający odmawia odpowiedzi na wnioski organów ochrony danych.

Grupa robocza uważa za konieczne wprowadzenie kar administracyjnych w przypadkach gdy administrator lub przetwarzający nie zapewniają zgodności ze swoimi obowiązkami na podstawie art. 53 ust. 1.

Reprezentowanie osoby, której dane dotyczą/ prawo do wniesienia skargi

Grupa robocza z zadowoleniem przyjmuje artykuł 76, ponieważ dąży do ułatwienia dostępu osób, których dane dotyczą, do środków prawnych.

¹⁶ Zgodnie ze stanowiskiem Komisji jak i propozycją Parlamentu obowiązki współpracy są określone w art. 29, który zostały usunięte przez Radę.

17 czerwca 2015 r.

Rada UE przewiduje możliwość dla organu, organizacji lub zrzeszenia, złożenia skargi do organu nadzorczego niezależnie od uprawnienia osoby, której dane dotyczą lub skargi (art. 76.2).

Jednakże ta możliwość powinna respektować interes osób, których dane dotyczą, i nie powinna prowadzić do naruszenia praw osoby, której dane dotyczą, lub wywierania jakiegokolwiek presji lub wpływu na organy nadzorcze.

Grupa robocza uważa, że możliwość złożenia skargi przez publiczne lub prywatne organizacje do organu nadzorczego bez upoważnienia osoby, której dane dotyczą powinna respektować interes jakichkolwiek dotkniętych osób, których dane dotyczą.