



01574/12/PL

WP199

**Opinia 08/2012 przedstawiająca dalsze uwagi dotyczące dyskusji na temat reformy
ochrony danych**

Przyjęta w dniu 5 października 2012 r.

Grupa robocza została powołana 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 Komisji Europejskiej, B-1049 Bruksela, Belgia, biuro nr MO-59 02/013.

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

Wprowadzenie

Wraz z przyjęciem pakietu dotyczącego reformy ochrony danych w dniu 25 stycznia 2012 r. zarówno Rada, jak i Parlament Europejski rozpoczęły realizację odpowiednich procedur w ramach procesu legislacyjnego.

Parlament Europejski

Parlament Europejski wyznaczył komisję LIBE na główną komisję odpowiedzialną za oba wnioski oraz mianował Jana Albrechta i Dimitriosą Droutsasa sprawozdawcami. Do zaangażowanych komisji parlamentarnych należą również IMCO, ITRE, ECON, JURI i EMPL.

Pakiet dotyczący reformy przedyskutowano już kilkakrotnie w LIBE oraz z kontrsprawozdawcami (członkami innych ugrupowań politycznych zajmujących się reformą). W dniu 29 maja 2012 r. sprawozdawcy zorganizowali również spotkanie zainteresowanych podmiotów w sprawie projektu rozporządzenia. W dniach 9 i 10 października 2012 r. komisja LIBE organizuje posiedzenie międzyparlamentarne z członkami parlamentów narodowych w celu omówienia pakietu dotyczącego reformy. Komisja LIBE zamierza przedstawić projekty sprawozdań dotyczących reformy przed końcem 2012 r. W takiej sytuacji inne zaangażowane komisje musiałyby również przedstawić swoje projekty opinii przed końcem roku.

Podczas posiedzenia LIBE w czerwcu 2012 r. sprawozdawcy przedstawili pierwszy dokument roboczy, w którym uwypuklają główne elementy reformy, wnoszą o zastosowanie podejścia pakietowego („sporządzenie dwóch w pełni spójnych, harmonijnych i wysokiej jakości instrumentów prawnych dotyczących ochrony danych poprzez zastosowanie kompleksowych, zrównoważonych, skoordynowanych i równoległych procedur dla obu tekstów”) oraz identyfikują szereg obszarów, które wymagają dalszej dyskusji i wyjaśnienia:

1. rola Komisji w kwestii aktów delegowanych i aktów wykonawczych oraz w ramach mechanizmu zgodności;
2. obecne wyłączenie z zakresu reformy przepisów dotyczących ochrony danych przez instytucje i organy UE;
3. relacja między ogólnym prawem Unii a szczegółowymi krajowymi przepisami prawnymi;
4. dokładny podział ról i zadań między organami ochrony danych w sprawach transgranicznych;
5. doprecyzowanie kwestii profilowania, z uwzględnieniem interwencji ze strony człowieka oraz prawa do informacji na temat zasad przetwarzania danych, zgodnie z żądaniami Parlamentu;
6. pojęcia „uzasadnionego interesu”, „interesu publicznego” i „bezpieczeństwa publicznego”;

7. wzajemne powiązania między oboma instrumentami ustawodawczymi, szczególnie w przypadkach dostępu organów ścigania do danych osobowych przechowywanych przez podmioty prywatne;
8. wnioski o udzielenie dostępu lub nakazy udzielenia dostępu do danych osobowych przechowywanych w Unii przez organy publiczne państw trzecich, zwłaszcza w przypadkach, gdy administrator danych również ma tam swoją siedzibę;
9. silniejsze zachęty do ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej.

Rada

Odbyło się szereg posiedzeń grupy roboczej Rady (DAPIX), najpierw w ramach duńskiej prezydencji i obecnie w ramach cypryjskiej prezydencji Rady. Dyskusje prowadzone w ramach DAPIX dotyczą głównie projektu rozporządzenia i polegają na jego omawianiu artykuł po artykule.

Według Rady dyskusje na szczeblu grupy roboczej pokazują powszechny konsensus między państwami członkowskimi co do konieczności przeprowadzenia reform istniejących ram prawnych w zakresie ochrony danych oraz wzmocnienia praw osób fizycznych do ochrony swoich danych osobowych. Ponadto występuje zbieżność opinii wśród państw członkowskich odnośnie do konieczności zapewnienia większej harmonizacji i spójności w stosowaniu przepisów UE w zakresie ochrony danych. Jak wynika jednak z ujawnionego dokumentu, szereg delegacji narodowych podaje w wątpliwość wiele kluczowych pojęć w zakresie ochrony danych, które funkcjonują już od dłuższego czasu.

Podczas nieformalnego posiedzenia ministrów sprawiedliwości i spraw wewnętrznych w Nikozji w dniach 23–24 lipca 2012 r. ministrowie omawiali potrzebę lepszego dostosowania niektórych wymogów formalnych (obciążenie administracyjne), w szczególności w odniesieniu do mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, na podstawie ustalonych kryteriów, takich jak ryzyko związane z przetwarzaniem danych, wielkość administratora danych, ilość przetwarzanych danych osobowych lub liczba dotkniętych tym osób fizycznych (podmiotów danych). Ministrowie zgodzili się ponadto, że przepisy dotyczące sektora prywatnego i publicznego nie powinny się zasadniczo różnić, chociaż konieczny jest pewien stopień elastyczności w odniesieniu do sektora publicznego. Ministrowie uzgodnili również, że w odniesieniu do każdego z licznych proponowanych aktów delegowanych i wykonawczych przeprowadzona zostanie analiza ich konieczności, ram czasowych oraz możliwych rozwiązań alternatywnych. W tym celu państwa członkowskie otrzymały kwestionariusz (z terminem udzielenia odpowiedzi do dnia 4 października) dotyczący obciążenia administracyjnego, aktów delegowanych i wykonawczych oraz stopnia elastyczności przewidzianego w przepisach w zakresie ochrony danych uznanych za niezbędne dla sektora publicznego.

Dalsze informacje od Grupy Roboczej Art. 29

W opinii z dnia 23 marca 2012 r. Grupa Robocza Art. 29 przedstawiła swoją pierwszą ogólną reakcję na wnioski Komisji, zwracając uwagę na obszary problematyczne i przedstawiając propozycje pewnych poprawek.

Grupa Robocza Art. 29 z zadowoleniem przyjmuje tzw. podejście pakietowe przyjęte przez sprawozdawców Parlamentu Europejskiego oraz wyraża przekonanie, iż wszystkie zaangażowane komisje parlamentarne należycie uwzględnią wszystkie elementy pakietu w celu dalszego udoskonalenia obydwu wniosków Komisji.

Grupa robocza z zadowoleniem przyjmuje również kroki poczynione przez cypryjską prezydencję Rady, o których mowa powyżej, mające na celu ożywienie dyskusji w ramach grupy roboczej Rady zajmującej się reformą.

Mając na uwadze dyskusje prowadzone zarówno w Parlamencie Europejskim, jak i w Radzie, Grupa Robocza podjęła decyzję o przyjęciu niniejszej opinii dostarczającej dalszych wytycznych, w szczególności w odniesieniu do niektórych kluczowych pojęć w zakresie ochrony danych oraz poprzez analizę zapotrzebowania na proponowane akty delegowane i wykonawcze i skutków tych aktów, a także – w razie potrzeby – sugerowanie bardziej odpowiednich rozwiązań alternatywnych¹.

Grupa robocza zauważa, że niektóre z osób, które wyraziły obawy o wpływ proponowanego rozporządzenia, koncentrują się na kluczowych pojęciach danych osobowych i zgody. Grupa robocza uważa, że jest to błędne podejście. W celu zapewnienia należytej ochrony prywatności danych osobowych oraz aktualności rozporządzenia w przyszłości należy przyjąć szeroką definicję danych osobowych oraz dopilnować, aby w przypadkach, w których wymagana jest zgoda, była to zgoda udzielona według wysokich standardów. Jeżeli przyjęcie tych kluczowych pojęć prowadzi do nieproporcjonalnych wyników w stosowaniu przepisów rozporządzenia regulujących przetwarzanie i ustalanie praw indywidualnych, uwagę należy skupić na tych właśnie przepisach i wyjątkach od nich, nie zaś na samych pojęciach kluczowych.

¹ Ponadto Grupa Robocza analizuje pojęcia celowości i zamierza przyjąć opinię w tej kwestii na początku przyszłego roku. Grupa Robocza wniesie również wkład w trwającą dyskusję na temat zakresu rozporządzenia, szczególnie w odniesieniu do wyjątku dotyczącego użytku domowego i osobistego.

W sprawie definicji danych osobowych

W opinii z dnia 23 marca² Grupa Robocza z zadowoleniem przyjmuje definicję „podmiotu danych” zawartą w art. 4 ust. 1 rozporządzenia, którego dotyczy wniosek, zgodnie z którą „podmiot danych oznacza zidentyfikowaną osobę fizyczną lub osobę fizyczną, którą można zidentyfikować [...]”.

Grupa Robocza zauważa, że definicja ta nie zmienia całkowicie pojęcia danych osobowych zdefiniowanego w dyrektywie 95/46/WE, lecz jedynie przeorganizowuje różne jego elementy³. W opinii w sprawie pojęcia danych osobowych⁴ Grupa Robocza zauważyła już, że obecna definicja zapewnia wystarczającą ciągłość i elastyczność w sposobie jej zastosowania do danych w różnych kontekstach, takich jak badania farmaceutyczne czy adresy IP.

Jednym z głównych wniosków tej analizy jest to, że osobę fizyczną można uznać za możliwą do zidentyfikowania, jeżeli w grupie osób można ją odróżnić od pozostałych członków grupy i w związku z tym traktować odmiennie.

Proponuje się zatem sprecyzowanie w motywie 23 oraz w art. 4, że pojęcie identyfikowalności obejmuje również odróżnienie osoby w taki sposób.

Motyw 23: „Zasady ochrony należy stosować do wszelkich informacji dotyczących zidentyfikowanych lub możliwych do zidentyfikowania osób **oraz wszelkich informacji pozwalających wyróżnić osobę fizyczną i traktować ją w odmienny sposób**. Aby ustalić, czy można zidentyfikować daną osobę fizyczną, należy wziąć pod uwagę wszystkie sposoby, jakimi mogą posłużyć się administrator lub inna osoba w celu zidentyfikowania tej osoby. Zasady ochrony nie powinny być stosowane do danych zanonimizowanych w taki sposób, że podmiot danych nie może być już zidentyfikowany”⁵.

Artykuł 4 ust. 1: „«podmiot danych» oznacza zidentyfikowaną osobę fizyczną lub osobę fizyczną, którą można zidentyfikować, bezpośrednio lub pośrednio, **lub wyróżnić i traktować w odmienny sposób**, za pomocą wszelkich środków, które z rozsądnym prawdopodobieństwem mogą być użyte przez administratora lub inną osobę fizyczną bądź prawną, szczególnie przez odniesienie do numeru identyfikacyjnego, danych dotyczących lokalizacji, identyfikatora online lub przynajmniej jednego czynnika charakterystycznego dla

² Opinia 1/2012 o projektach reformy ochrony danych (WP 191).

³ Art. 2 lit. a) dyrektywy 95/46/WE stanowi obecnie, że „dane osobowe” oznaczają „wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej („osoby, której dane dotyczą”); osoba możliwa do zidentyfikowania to osoba, której tożsamość można ustalić bezpośrednio lub pośrednio, szczególnie przez powołanie się na numer identyfikacyjny lub jeden bądź kilka szczególnych czynników określających jej fizyczną, fizjologiczną, umysłową, ekonomiczną, kulturową lub społeczną tożsamość”. Motyw 26 obecnie stanowi, że „w celu ustalenia, czy daną osobę można zidentyfikować, należy wziąć pod uwagę wszystkie sposoby, jakimi może posłużyć się administrator lub inna osoba w celu zidentyfikowania owej osoby”. Rozporządzenie, którego dotyczy wniosek, wprowadza zatem jedynie definicję „podmiotu danych” na podstawie istniejących elementów.

⁴ Opinia 4/2007 w sprawie pojęcia danych osobowych (WP 136).

⁵ **Pogrubiona czcionka** oznacza tekst dodany. Zaleca się skreślić tekst podany w [...].

fizycznej, fizjologicznej, genetycznej, umysłowej, ekonomicznej, kulturowej lub społecznej tożsamości tej osoby”.

Ponadto w motywie 24 odnoszącym się do definicji danych osobowych przewiduje się, że numery identyfikacyjne, dane dotyczące lokalizacji, identyfikatory internetowe lub inne szczególne czynniki jako takie niekonieczne muszą być uważane za dane osobowe w każdych okolicznościach. W obecnym kształcie ostatnie zdanie mogłoby doprowadzić do niesłusznie restrykcyjnej interpretacji pojęcia danych osobowych w odniesieniu do np. adresów IP lub identyfikatorów plików cookie. Grupa Robocza przypomina, że dane osobowe są to wszelkie dane odnoszące się do możliwej do zidentyfikowania osoby. „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 osoby”.

Już w opinii 4/2007 Grupa Robocza opracowała różne scenariusze, które uzasadniają, dlaczego adresy IP należy uważać za dotyczące osób możliwych do zidentyfikowania „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, podobnie jak w przypadku plików cookie, administrator danych przewiduje, że „sposoby, jakimi można się posłużyć” będą dostępne w celu zidentyfikowania danej osoby i traktowania jej w sposób szczególny⁶.

Dlatego też grupa robocza sugeruje odpowiednią zmianę motywu 24.

Motyw 24: „Osoby fizyczne korzystające z usług internetowych można identyfikować na podstawie identyfikatorów internetowych, które znajdują się w urządzeniach, aplikacjach, narzędziach i protokołach, takich jak adresy IP lub identyfikatory plików cookie. Mogą one zostawiać ślady, które w połączeniu z unikatowymi identyfikatorami i innymi informacjami uzyskanymi przez serwery, mogą być wykorzystywane do tworzenia profili poszczególnych osób, ich identyfikacji **lub wyróżnienia**. W wyniku tego numery identyfikacyjne, dane dotyczące lokalizacji, identyfikatory internetowe lub inne szczególne czynniki jako takie **muszą być z zasady uważane za** [skreślić: niekonieczne muszą być uważane za] dane osobowe [skreślić: w każdych okolicznościach].

⁶ Zob. także wstępne sprawozdanie służb Federalnej Komisji Handlu (FTC) „Protecting Consumer Privacy in an Era of Rapid Change” z grudnia 2010 r. oraz sprawozdanie FTC „Protecting Consumer Privacy in an Era of Rapid Change” z marca 2012 r.

Oдноśnie do pojęcia zgody

Zgoda podmiotu danych stanowi pierwszą podstawę prawną w art. 6 ust. 1 w zakresie przetwarzania danych osobowych z zastrzeżeniem spełnienia określonych warunków. Warunki te określono w art. 4 pkt 8 i art. 7 rozporządzenia, którego dotyczy wniosek.

Zgoda odgrywa ważną rolę, co nie wyklucza jednak możliwości – w zależności od kontekstu – zastosowania innych podstaw prawnych w celu uzasadnienia przetwarzania danych osobowych.

W niedawno wydanej opinii w sprawie definicji zgody⁷ Grupa Robocza Art. 29 nalega na konieczność zapewnienia wykorzystania zgody we właściwym kontekście i nienadużywania jej. W przypadku wykorzystania zgody powinna być ona wystarczająco jasna. Zgodę można wyrazić na różne sposoby, na przykład poprzez oświadczenie lub działanie potwierdzające, ponieważ pojęcie zgody jest wystarczająco elastyczne. Zgodnie z zasadniczym wymogiem takie oświadczenie lub działanie potwierdzające musi jednoznacznie oznaczać zgodę podmiotu danych na przetwarzanie odnoszących się do niego danych osobowych.

Bazując na opinii grupy roboczej, w art. 7 projektu rozporządzenia wprowadza się nowe i pozytywne elementy polegające w szczególności na nałożeniu ciężaru udowodnienia zgody na administratora danych, wprowadzeniu zabezpieczeń w kontekście pisemnego oświadczenia oraz wykluczeniu ważności zgody w sytuacji poważnej nierówności między podmiotem danych a administratorem. Grupa robocza z dużym zadowoleniem przyjmuje te istotne wyjaśnienia i wzmocnienie praw osób fizycznych.

Grupa robocza zdaje sobie sprawę, że zgłoszono wątpliwości co do praktycznych trudności wynikających ze słowa „wyraźne” w kontekście zgody w art. 4 pkt 8. Grupa robocza jest jednak zdania, że dodanie słowa „wyraźne” jest ważnym elementem doprecyzującym tekst, który jest niezbędne, aby naprawdę umożliwić podmiotom danych korzystanie z przysługujących im praw, zwłaszcza w internecie, gdzie obecnie zgoda jest zbyt często niewłaściwie stosowana. Usunięcie tego istotnego doprecyzowania z treści rozporządzenia byłoby działaniem wysoce niepożądanym.

Ponadto grupa robocza podkreśla, że pojęcie zgody ma znaczenie ogólne w szerokim wachlarzu sytuacji. Warunki przedstawione w art. 4 pkt 8 i art. 7 są jej zdaniem w pełni wystarczające, aby zapewnić właściwe wykorzystanie zgody we wszystkich tych sytuacjach. W odniesieniu do szczególnego przypadku plików cookie grupa robocza zwróciła niedawno uwagę na dodatkową elastyczność zapewnioną w tym kontekście⁸.

⁷ Opinia 15/2011 w sprawie definicji zgody (WP187).

⁸ Opinia 4/2012 w sprawie wyjątków w zakresie pozyskiwania zgody na zapisywanie plików cookie (WP 194).

Odniesienie do proponowanych aktów delegowanych

We wniosku Komisji dotyczącym nowego rozporządzenia w sprawie ochrony danych przewiduje się znaczną liczbę aktów delegowanych i wykonawczych. Chociaż w niektórych przypadkach takie kolejne akty mogą być cennym instrumentem zapewniającym dalszą harmonizację i wytyczne, Grupa Robocza Art. 29 ma pewne zastrzeżenia co do zakresu, w jakim Komisja byłaby uprawniona do przyjmowania takich aktów, o czym wspomniano również w opinii o projektach reformy ochrony danych (WP191). Jak wspomniano powyżej, zarówno komisja LIBE Parlamentu Europejskiego, jak i Rada wyraziły podobne obawy i ogłosiły, że przeanalizują proponowane akty delegowane i wykonawcze artykuł po artykule, aby ustalić, czy rzeczywiście są one konieczne.

Grupa robocza wskazała w swojej opinii o projektach reformy ochrony danych, że przy opracowywaniu projektów aktów delegowanych lub aktów wykonawczych należy w każdym przypadku konsultować się z Europejską Radą Ochrony Danych (EROD), która zastąpi grupę roboczą. Ponadto jednym z podstawowych zadań grupy roboczej jest obecnie dostarczanie wytycznych interpretacyjnych. Wytyczne dostarczone w ubiegłych latach, głównie w formie opinii, potwierdziły swoją wartość dodaną. W przyszłości przygotowywanie takich wytycznych interpretacyjnych przez Europejską Radę Ochrony Danych będzie jeszcze ważniejsze. Ponieważ w skład Europejskiej Rady Ochrony Danych wchodzi wszystkie krajowe organy ochrony danych UE, w niektórych sytuacjach może być ona lepiej predysponowana do udzielania wytycznych.

Różnice między aktami delegowanymi a aktami wykonawczymi

Od czasu wejścia w życie traktatu lizbońskiego Komisja może być uprawniona do przyjmowania aktów delegowanych i aktów wykonawczych. Akty delegowane opierają się na art. 290 TFUE i można je przyjmować w celu uzupełnienia lub zmiany innych niż zasadnicze części aktu prawnego (w tym przypadku rozporządzenia, którego dotyczy wniosek). Akty wykonawcze opierają się na art. 291 TFUE i można je stosować, jeżeli konieczne są jednolite warunki wykonywania prawnie wiążących aktów Unii, takich jak dyrektywa lub rozporządzenie.

W odniesieniu do aktów delegowanych proponowane przekazanie uprawnień oznacza, że znaczna część przepisów nie będzie częścią proponowanego rozporządzenia i nie zostanie przyjęta w drodze zwykłej procedury ustawodawczej. Nie oznacza to jednak, że Parlament Europejski i Rada nie będą uczestniczyły w przyjmowaniu aktu delegowanego. Akty delegowane wejdą w życie, tylko jeśli Parlament Europejski lub Rada nie wyrażą sprzeciwu w terminie dwóch miesięcy od przekazania tego aktu, jak wynika również z art. 86 proponowanego rozporządzenia.

Jeżeli Parlament Europejski lub Rada wyrażą sprzeciw, oznacza to, że akt delegowany nie wejdzie w życie. Komisja może wówczas podjąć decyzję o zaproponowaniu nowego aktu

delegowanego, uwzględniając zastrzeżenia, lub może opracować projekt nowych przepisów, jeżeli zastrzeżenie dotyczyło przekroczenia przekazanych uprawnień. Komisja może również zrezygnować z proponowania jakichkolwiek dalszych aktów lub przepisów.

W art. 290 TFUE nie przewiduje się możliwości proponowania zmian przez Parlament Europejski lub Radę; organy te mogą jedynie sprzeciwiać się wejściu w życie aktu delegowanego.

Artykuły 290 i 291 TFUE nie zapewniają jasnych kryteriów wyboru między aktem delegowanym a aktem wykonawczym. Z rozporządzenia, którego dotyczy wniosek, wynika wyraźnie, że Komisja rozważa przyjęcie aktów wykonawczych w celu zagwarantowania jednolitych, bardziej technicznych warunków wdrażania tego rozporządzenia, takich jak standardowe formularze i standardowe procedury.

Powierzenie Komisji uprawnień do przyjmowania aktów delegowanych i aktów wykonawczych nie musi oznaczać, że Komisja jest zobowiązana do przyjęcia wszystkich aktów proponowanych w rozporządzeniu. Większość aktów zostanie przyjęta wyłącznie wówczas, gdy zajdzie taka potrzeba.

Grupa Robocza podkreśla, że przyjmowanie aktów delegowanych i wykonawczych powinno być możliwe tylko w przypadkach, gdy Komisja może uzasadnić, że są one faktycznie konieczne. Sam fakt, że takiej oceny nie można przeprowadzić we wszystkich przypadkach w momencie przyjęcia rozporządzenia, nie zapewnia wystarczającego uzasadnienia, aby z góry przyznać Komisji (na wszelki wypadek) uprawnienia do przyjmowania aktów delegowanych lub wykonawczych.

Z powyższego wynika, że istnieje kilka sposobów regulowania ochrony danych na poziomie UE:

- w samym rozporządzeniu, którego dotyczy wniosek;
- w akcie delegowanym;
- w akcie wykonawczym;
- w motywach rozporządzenia.

Spójne i zharmonizowane podejście na szczeblu UE można jednak w niektórych przypadkach lepiej osiągnąć poprzez stosowanie wytycznych interpretacyjnych wydanych przez Europejską Radę Ochrony Danych (które mogą obejmować zatwierdzenie kodeksu postępowania).

Ponieważ wydaje się, że Komisja rozważa zastosowanie aktów wykonawczych głównie w celu zapewnienia jednolitych, bardziej technicznych warunków wdrażania rozporządzenia, takich jak standardowe formularze i standardowe procedury, a nie na potrzeby dalszego

wdrażania i stosowania (istotnych) norm, akty te na chwilę obecną wyłączono z poniższej oceny. Niewykluczone jednak, że ich analiza również będzie konieczna.

Ocena proponowanych aktów delegowanych

Komisja od samego początku jasno stwierdziła, że celem reformy jest zapewnienie harmonizacji oraz neutralności instrumentu pod względem technologicznym. Dlatego też cel ten uwzględniono podczas analizy proponowanych aktów delegowanych.

Kolejnym wyraźnym kryterium (wynikającym z art. 290 TFUE) jest fakt, że zasadnicze elementy należy uwzględnić w akcie podstawowym, tj. w treści proponowanego rozporządzenia, a nie w akcie delegowanym. Grupa Robocza Art. 29 oraz Europejski Inspektor Ochrony Danych (EIOD) wskazali w proponowanym rozporządzeniu szereg przepisów, w których przekazuje się Komisji uprawnienia dotyczące zasadniczych elementów⁹.

Ponadto w niektórych przypadkach ważne jest zapewnienie pewności prawa. Ustanawianie norm w wiążących instrumentach UE zapewnia pewność prawa, jak również równe warunki działania w UE. Istnieją sytuacje, w których wiążący instrument UE określający przepis rozporządzenia będzie najwłaściwszym sposobem stworzenia pewności prawa, ochrony podmiotu danych oraz uniknięcia rozbieżności między państwami członkowskimi prowadzących do wypaczeń.

W innych sytuacjach bardziej właściwe może być jednak podejście elastyczne oraz uwzględnienie różnic kulturowych w celu zapewnienia stosowania zasad w praktyce. W takich przypadkach bardziej odpowiednie może być udzielenie wskazówek za pomocą wytycznych Europejskiej Rady Ochrony Danych, która uznaje potrzebę elastyczności i popiera wprowadzenie zasady rozliczalności. Ostateczne zdanie w tej kwestii mają Trybunał Sprawiedliwości oraz sądy krajowe.

Decyzję w sprawie wyboru jednego lub kilku wyżej wymienionych instrumentów w celu rozwiązania specyficznej kwestii ochrony danych należy podjąć na podstawie czytelnych kryteriów.

Ocenę przeprowadza się na podstawie następujących kryteriów:

- czy kwestia dotyczy zasadniczej części rozporządzenia;
- czy kwestią należy zająć się na szczeblu europejskim czy krajowym (tj. czy istnieje potrzeba harmonizacji);
- czy konieczny jest prawnie wiążący, czy też bardziej elastyczny instrument;
- czy instrument jest zgodny z wymogiem neutralności pod względem technologicznym;
- czy w ogóle istnieje konieczność zapewniania dalszych wytycznych (tj. czy to administrator ma konkretyzować zasady zgodnie ze szczególnymi okolicznościami

⁹ Opinia 1/2012 (WP191), s. 7 oraz opinia EIOD, pkt 74.

danego przypadku, zawsze z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej).

W załączniku do niniejszej opinii zidentyfikowano i przeanalizowano artykuły, w których proponuje się akty delegowane, oraz oceniono, czy akt delegowany rzeczywiście jest najwłaściwszym rozwiązaniem w odniesieniu do danej kwestii lub danych kwestii. Poza aktem delegowanym rozważa się następujące możliwości zapewnienia dalszych wytycznych:

- uwzględnienie kwestii w treści rozporządzenia;

Zamiast dopuszczać możliwość przyjęcia aktów delegowanych, pewne kwestie można lub należy włączyć do treści samego rozporządzenia. Doprecyzowanie niektórych kwestii w treści rozporządzenia doprowadziłoby do harmonizacji, ponieważ rozporządzenie ma bezpośrednie zastosowanie w całej UE. Wiązałoby się to jednak z ryzykiem zbyt małej elastyczności, aby móc uwzględnić wszystkie możliwe sytuacje, jak również niezachowania neutralności pod względem technologicznym. Ponadto próba włączenia do treści rozporządzenia większej liczby zasad może stwarzać ryzyko spowolnienia procesu reform.

- uwzględnienie kwestii w jednym z motywów rozporządzenia;

Niektóre kwestie można uwzględnić w motywach rozporządzenia zamiast w akcie delegowanym. Motyw może do pewnego stopnia zawierać pomocne, ogólne wytyczne dotyczące celu i *uzasadnienia* przepisu szczegółowego. Próba włączenia większej liczby przykładów do motywów rozporządzenia może jednak stwarzać ryzyko spowolnienia procesu reform lub przyczynić się do powstania złego prawa motywowanego konkretnymi interesami, a nie zasadami ogólnymi.

- uregulowanie tej kwestii w prawie krajowym;

Aby uwzględnić różnice (kulturowe, prawne i historyczne) między państwami członkowskimi, doprecyzowanie mogłoby się również znaleźć w prawie krajowym. Mogłoby to jednak zagrozić realizacji celu polegającego na zapewnieniu harmonizacji i funkcjonowania rynku wewnętrznego.

- wytyczne Europejskiej Rady Ochrony Danych;

Wytyczne Europejskiej Rady Ochrony Danych mogą być w szczególnych okolicznościach dobrą alternatywą dla aktu delegowanego. Wytyczne Grupy Roboczej Art. 29 nie są nowym instrumentem. Już obecnie Grupa Robocza Art. 29 wydaje opinie i zalecenia we wszystkich sprawach dotyczących ochrony osób w odniesieniu do przetwarzania danych osobowych zgodnie z art. 30 obecnej dyrektywy 95/46. Wydając wspólne opinie, obecna Grupa Robocza Art. 29 przyczynia się do zharmonizowanego stosowania obecnych ram prawnych. Mimo że opinie te jako takie nie są prawnie wiążące, są one poważane i dowiodły swej wartości dodanej. Wytyczne Europejskiej Rady Ochrony Danych są elastycznym instrumentem, który można stosunkowo łatwo

dostosowywać oraz zmieniać lub aktualizować, na przykład w reakcji na postęp techniczny.

- rezygnacja z opracowywania jakichkolwiek dalszych wytycznych lub przepisów;

W niektórych przypadkach można zaproponować rezygnację z opracowywania jakichkolwiek dalszych wytycznych lub przepisów, ponieważ przepisy rozporządzenia są wystarczająco jasne dla wszystkich właściwych zainteresowanych podmiotów, a administratorzy sami powinni zapewniać zgodność z rozporządzeniem, zawsze z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

ZAŁACZNIK

Artykuł 6 ust. 5 – w celu doprecyzowania warunków, o których mowa w art. 6 ust. 1 lit. f), dla różnych sektorów i sytuacji, w których przetwarza się dane, w tym jeśli chodzi o przetwarzanie danych osobowych dotyczących dziecka.

Artykuł 6 dotyczy zgodności z prawem przetwarzania; w art. 6 lit. a)–f) określa się sześć alternatywnych podstaw prawnych operacji przetwarzania, z których *przynajmniej jedna* musi zostać zastosowana na pewnym etapie.

Ustęp 1 lit. f) stanowi, że przetwarzanie danych osobowych jest zgodne z prawem jedynie wtedy, gdy jest konieczne dla celów wynikających ze słuszných interesów realizowanych przez administratora, z wyjątkiem sytuacji, kiedy nadrzędny charakter ma interes podstawowych praw i wolności podmiotu danych, które wymagają ochrony danych osobowych, w szczególności gdy podmiotem danych jest dziecko. Przepisu tego nie stosuje się do przetwarzania realizowanego przez organy publiczne w wykonaniu ich zadań.

Zgodnie z art. 6 ust. 1 lit. f) słuszny interes może stanowić podstawę prawną przetwarzania danych osobowych, o ile – i w zakresie, w jakim – spełniono określone warunki dotyczące wymogu przeprowadzenia testu równowagi w świetle okoliczności każdego przypadku.

Zgodnie z zasadą rozliczalności (omówioną w art. 22 proponowanego rozporządzenia) do administratora danych należy decyzja, czy istnieje słuszny interes uzasadniający określone przetwarzanie danych czy też nadrzędny charakter wobec słusznego interesu mają interesy lub podstawowe prawa i wolności podmiotu danych. Podjęcie takiej decyzji odbędzie się z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

Ponieważ jednak dotyczy to jednej z podstaw prawnych przetwarzania, niezbędne jest przedstawienie dalszych wytycznych, aby zapewnić wspólną interpretację przepisu. Dalsze wytyczne dotyczące wspólnych kryteriów lub przykładów pojęcia słusznego interesu byłyby przydatne w celu zapewnienia spójności stosowania i wdrażania.

Biorąc pod uwagę wszelkie różne (obecne i przyszłe) sytuacje, w których może wystąpić słuszny interes i w których nadrzędny charakter wobec słusznego interesu mają interesy lub podstawowe prawa i wolności podmiotu danych, wydaje się, że właściwszy będzie instrument bardziej elastyczny niż instrument wiążący.

Ponadto wątpliwe jest, czy akt delegowany byłby właściwym instrumentem do uregulowania tego zasadniczego elementu rozporządzenia.

Pozostawienie dalszych regulacji w gestii ustawodawcy krajowego doprowadziłoby do wysoce niepożądanych różnic w wykładni i stosowaniu. Administratorzy danych mogliby wówczas przetwarzać dane na tej podstawie w jednym państwie członkowskim, a w innym

potencjalnie nie. Dlatego też, aby zapewnić spójną interpretację i stosowanie niniejszej podstawy prawnej przetwarzania danych, należy przedstawić wytyczne na szczeblu europejskim.

Wydaje się, że zamiast uregulować tę kwestię w akcie delegowanym właściwszym rozwiązaniem zapewniającym niezbędną elastyczność będą wskazówki wydawane przez EROD dotyczące tego, w jakich okolicznościach można powoływać się na „słuszny interes” oraz w jaki sposób ocenić, czy nadrzędny charakter w stosunku do takiego interesu mają interesy lub podstawowe prawa i wolności podmiotu danych, między innymi poprzez podanie konkretnych przykładów.

Artykuł 8 ust. 3 – w celu doprecyzowania kryteriów i wymogów dotyczących sposobów uzyskania możliwej do zweryfikowania zgody, o której mowa w ust. 1. W tym celu Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Artykuł 8 ust. 1 stanowi, że do celów omawianego rozporządzenia, w odniesieniu do oferowania usług społeczeństwa informacyjnego bezpośrednio dziecku, przetwarzanie danych osobowych dziecka w wieku poniżej 13 lat jest zgodne z prawem, o ile zgodę na nie wydał lub pozwolił na nie rodzic lub opiekun dziecka. Administrator podejmuje racjonalne starania w celu uzyskania możliwej do zweryfikowania zgody, uwzględniając dostępną technologię.

Zgodnie z zasadą rozliczalności administrator danych powinien odpowiadać za uzyskanie możliwej do zweryfikowania zgody, uwzględniając dostępną technologię.

Określenie kryteriów i wymogów dotyczących metod uzyskania możliwej do zweryfikowania zgody w dokumencie prawnym również stwarzałoby poważne ryzyko zbyt małej elastyczności i może również w sposób niewystarczający spełniać wymogi dotyczące zachowania neutralności pod względem technologicznym.

Ponadto dopuszczenie uregulowania tej kwestii w prawie krajowym doprowadziłoby do różnic między obowiązkami nałożonymi na administratorów danych, co byłoby sprzeczne z celem polegającym na zapewnieniu harmonizacji i stworzeniu równych warunków działania oraz nie zapewniłoby wymaganej elastyczności.

Podsumowując, na administratorze danych spoczywa już wyraźny obowiązek podjęcia racjonalnych starań w celu uzyskania możliwej do zweryfikowania zgody, uwzględniając dostępne technologie. Dlatego też wydaje się, że zapewnianie dalszych wytycznych w akcie delegowanym nie jest konieczne.

Jeżeli chodzi o szczególne traktowanie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, wydaje się, że brakuje przesłanek, by uznać to za konieczne. Ponieważ powodem wprowadzenia tego artykułu jest fakt, że dzieci są szczególnie zagrożone, tym bardziej dziwne wydawałoby się wykluczenie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców z obowiązku uzyskania możliwej do zweryfikowania zgody na wypadek, gdyby dotyczyła ona danych osobowych dzieci. Ponadto w akcie delegowanym nie można nigdy wprowadzać wyłączeń dla MŚP, których nie przewidziano już w treści samego rozporządzenia.

Artykuł 9 ust. 3 – w celu doprecyzowania kryteriów, warunków i odpowiednich gwarancji przetwarzania szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, oraz wyjątków określonych w art. 9 ust. 2.

Artykuł 9 dotyczy szczególnych kategorii danych osobowych i zakazuje się w nim przetwarzania danych z wymienionych kategorii, z wyjątkiem 10 wyłączeń ustanowionych w ust. 2.

Artykuł przypomina sposób, w jaki kwestię szczególnych kategorii danych rozwiązuje się w obowiązującej dyrektywie, w której wyraźnie zakazuje się przetwarzania szczególnych kategorii danych osobowych, przewidując jednak równocześnie pewne wyjątki. Jeżeli chodzi o „kryteria i warunki”, wydaje się, że obecna sytuacja nie powoduje wielu problemów, w związku z czym doprecyzowanie kryteriów i warunków przetwarzania szczególnych kategorii danych osobowych nie wydaje się konieczne.

Ponieważ ust. 1 i ust. 2 lit. a)–f) omawianego artykułu są już jasno sformułowane, gdyż wprowadza się w nich ogólny zakaz przetwarzania wspomnianych szczególnych kategorii danych osobowych z wyjątkiem określonych okoliczności, wydaje się, że dalsze doprecyzowanie kryteriów i warunków nie jest konieczne.

Jak wynika jednak z wcześniejszych doświadczeń, w niektórych sytuacjach przydałyby się dalsze wytyczne dotyczące tego, co stanowi odpowiednie gwarancje.

Ponieważ ustalenia tego, co stanowi właściwe gwarancje, można dokonać jedynie na podstawie indywidualnych przypadków, zapewnienie dalszych wytycznych w prawnie wiążącym dokumencie byłoby niemożliwe. Dlatego też najwłaściwszym rozwiązaniem w celu zapewnienia dalszych wytycznych dotyczących tego, co może stanowić odpowiednie gwarancje byłby bardziej elastyczny instrument.

EROD mogłaby zatem wydać wytyczne w tej kwestii. W miarę możliwości można by również przedstawić niewyczerpujący zestaw przykładów w jednym z motywów rozporządzenia.

Jeżeli chodzi o ust. 2 lit. g), rozporządzenie zawiera wyłączenia od ogólnego zakazu w odniesieniu do zadań wykonywanych w interesie publicznym. Wskazane byłoby, aby administrator decydował o możliwości zastosowania wyłączenia, zawsze z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej. W kontekście tego wyłączenia zalecane byłyby jednak dalsze wytyczne w celu zapewnienia harmonizacji w stosowaniu i spójności na szczeblu europejskim.

Z uwagi na mnogość sytuacji, w których przetwarzanie danych może być dopuszczalne na podstawie wyłączenia w odniesieniu do zadań wykonywanych w interesie publicznym,

wyduje się, że akt delegowany nie jest właściwym instrumentem. Bardziej elastyczny instrument byłby bardziej przydatny do dostarczania administratorowi wytycznych odnośnie do sytuacji, w których, pomimo ogólnego zakazu, może on przetwarzać dane osobowe na podstawie tego wyłączenia.

Co więcej, zgodnie z opinią Grupy Roboczej Art. 29 o projektach, w miarę możliwości dla każdego artykułu należy zidentyfikować możliwy szczególny interes publiczny.

Biorąc pod uwagę powyższe, szczególny interes publiczny przewidziany w art. 9 ust. 2 lit. g) należy sprecyzować w treści samego rozporządzenia oraz ewentualnie dokładniej wyjaśnić w jednym z motywów.

Artykuł 12 ust. 5 – w celu doprecyzowania kryteriów i warunków przesadnego charakteru wniosków oraz pobierania opłat, o których mowa w art. 12 ust. 4.

Artykuł 12 dotyczy w szczególności opłat pobieranych, jeśli wniosek złożony przez podmiot danych jest wyraźnie przesadny.

Artykuł 12 ust. 4 stanowi, że przekazanie informacji i podjęcie działań na podstawie wniosków złożonych przez podmioty danych w ramach wykonywania przysługujących im praw są wolne od opłat. Jeśli wnioski są wyraźnie przesadne, w szczególności ze względu na ich powtarzający się charakter, administrator może pobrać opłatę za przekazanie wnioskowanych informacji lub podjęcie żadanego działania lub też może uchylić się od podjęcia żadanego działania. W takim przypadku na administratorze spoczywa ciężar udowodnienia wyraźnie przesadnego charakteru wniosku.

Ustęp 4 artykułu stanowi, że „[...] na administratorze spoczywa ciężar udowodnienia wyraźnie przesadnego charakteru wniosku”. Zgodnie z zasadą rozliczalności do administratora należy ocena, czy wniosek jest wyraźnie przesadny. Ocena taka zawsze odbywa się z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

Ponieważ decyzję, czy wniosek jest wyraźnie przesadny, należy zawsze podejmować dla każdego przypadku oddzielnie z uwzględnieniem wszystkich okoliczności, wydaje się, że właściwszym rozwiązaniem jest doprecyzowanie kryteriów i warunków w bardziej elastycznym instrumencie.

Jeżeli chodzi o opłaty, które można pobierać w przypadku wyraźnie przesadnego wniosku, próba ustalenia tego w prawnie wiążącym dokumencie albo nawet na szczeblu UE wydaje się niemożliwa lub niewłaściwa, ponieważ różnice między państwami członkowskimi ani między sektorami nie zostałyby wówczas uwzględnione.

Podsumowując, wydaje się, że nie ma potrzeby opracowywania dalszych przepisów ani wytycznych dotyczących kryteriów i warunków w zakresie wyraźnie przesadnych wniosków i opłat, o których mowa w art. 12 ust. 4. W stosownych przypadkach maksymalna kwota, którą można pobierać, mogłaby jednak zostać określona w prawie krajowym.

Artykuł 14 ust. 7 – w celu doprecyzowania:

- kryteriów kategorii odbiorców, o których mowa w art. 14 ust. 1 lit. f);
- wymogów dotyczących zawiadomienia o potencjalnym dostępie, o których mowa w art. 14 ust. 1 lit. g);
- kryteriów przekazywania dalszych informacji, o których mowa w art. 14 ust. 1 lit. h), niezbędnych dla niektórych sektorów i w niektórych sytuacjach; oraz
- warunków i odpowiednich gwarancji w przypadku wyjątków określonych w art. 14 ust. 5 lit. b).

W tym celu Komisja podejmie odpowiednie środki w odniesieniu do mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Artykuł 14 dotyczy informacji przekazywanych podmiotowi danych.

Ustęp 1 (lit. f)–h)) stanowi, że w przypadku zbierania danych osobowych odnoszących się do podmiotu danych, administrator udziela temu podmiotowi co najmniej informacji dotyczących odbiorcy lub kategorii odbiorców danych osobowych (lit. f)), w stosownych przypadkach, informacje o zamiarze przekazania danych przez administratora do państwa trzeciego lub organizacji międzynarodowej oraz informacje na temat poziomu ochrony zapewnianego przez to państwo trzecie lub organizację międzynarodową przez odniesienie do decyzji Komisji stwierdzającej odpowiedni poziom ochrony (lit. g)), a także wszelkie dalsze informacje potrzebne do zagwarantowania rzetelnego przetwarzania danych w stosunku do podmiotu danych, uwzględniając konkretne okoliczności, w których odbywa się zbieranie danych (lit. h)).

Ustęp 5 lit. b) stanowi, że pierwszych czterech ustępów art. 14 nie stosuje się, gdy dane nie są zbierane od podmiotu danych, a udzielenie tych informacji okazało się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku.

Prawa i obowiązki przedstawione w tym artykule są już stosunkowo jasne. Szczególnie w porównaniu z obowiązującą dyrektywą 95/46 artykuł ten zapewnia większą jasność i lepsze wytyczne dla odnośnych zainteresowanych stron.

Ponadto należy uwzględnić obowiązki administratora danych, zwłaszcza jeśli chodzi o kryteria dotyczące kategorii odbiorców, o których mowa w art. 14 ust. 1 lit. f), wymagania powiadomienia o potencjalnym dostępie, o których mowa w art. 14 ust. 1 lit. g) oraz kryteriów dotyczących dalszych informacji, o których mowa w art. 14 ust. 1 lit. h), niezbędnych dla niektórych sektorów i w niektórych sytuacjach.

W odniesieniu do warunków i odpowiednich gwarancji dotyczących wyjątków ustanowionych w art. 14 ust. 5 lit. b) administrator powinien także być w stanie ocenić i wykazać, czy udzielenie informacji wymagałoby niewspółmiernie dużego wysiłku, z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

Zapewnienie dalszych wytycznych dotyczących tego, czym jest niewspółmiernie duży wysiłek, byłoby jednak pomocne, ponieważ stanowi to wyjątek od jednego z podstawowych praw podmiotu danych (prawa do informacji). Jest to szczególnie istotne w przypadkach, w których administrator nie otrzymywał danych bezpośrednio od podmiotów danych.

Aby zapewnić harmonizację w tej kwestii, należy zapewnić dalsze wytyczne na szczeblu europejskim. Szczególnie w dzisiejszym świecie pełnym wzajemnych powiązań rozbieżne interpretacje tego wyłączenia miałyby poważny wpływ na podmioty danych i administratorów oraz nie zapewniłyby harmonizacji. Najlepszym rozwiązaniem byłoby opracowanie tych wytycznych przez EROD. Ze względów pewności prawa można rozważyć instrument wiążący, określający jedynie warunki i gwarancje dotyczące głównych ram.

Główne warunki i odpowiednie gwarancje dotyczące wyjątku przewidzianego w art. 14 ust. 5 lit. b) zwalniającego administratora z obowiązku udzielania informacji podmiotowi danych można zawrzeć w akcie delegowanym. Bardziej szczegółowe wytyczne EROD mogłyby jednak pomóc ocenić, w jakich sytuacjach administratorzy mogą korzystać z wyłączenia, na podstawie analizy różnych praktycznych sytuacji i kontekstów.

Nałożenie innych (mniej rygorystycznych) obowiązków na administratorów ze względu na ich wielkość mogłoby poważnie podważyć realizację celu artykułu, jakim jest zobowiązanie administratorów do działania w sposób przejrzysty, aby umożliwić podmiotom danych dokonanie świadomego wyboru. Dlatego też obowiązek przekazywania niezbędnych informacji w celu umożliwienia podmiotowi danych dokonania świadomego wyboru powinien mieć zastosowanie niezależnie od wielkości administratora. Ponadto w akcie delegowanym nie można wprowadzać wyłączeń dla MŚP, których nie przewidziano już w treści samego rozporządzenia.

Artykuł 15 ust. 3 – w celu doprecyzowania kryteriów i wymogów dotyczących informowania podmiotu danych o treści danych osobowych, o których mowa w art. 15 ust. 1 lit. g).

Artykuł 15 dotyczy prawa dostępu przysługującego podmiotowi danych, zaś w art. 15 ust. 1 lit. g) szczegółowo omawia się przekazanie danych osobowych podlegających przetwarzaniu i wszelkich dostępnych informacji o ich źródle.

Kwestia wymagająca doprecyzowania w proponowanym akcie delegowanym dotyczy obowiązków nałożonych na administratorów, mimo że art. 15 jako taki dotyczy prawa dostępu przysługującego podmiotom danych. Pod tym względem, zgodnie z zasadą odpowiedzialności, administrator powinien odpowiadać za zapewnienie zgodności z prawem, z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

Ponadto prawo dostępu przysługujące podmiotowi danych jasno stanowi, że podmiotowi danych należy przekazać informacje dotyczące danych osobowych podlegających przetwarzaniu i wszelkich dostępnych informacji o ich źródle.

Dlatego też wydaje się, że dalsze przepisy i wytyczne nie są konieczne.

Nb. Przydatne byłoby jednak dalsze wyjaśnienie, czy art. 15 ust. 1 lit. g) rzeczywiście oznacza także faktyczne dane osobowe podlegające przetwarzaniu, jak można wywnioskować z ust. 3.

Artykuł 17 ust. 9 – w celu doprecyzowania:

- kryteriów i wymogów stosowania art. 17 ust. 1 (prawo do bycia zapomnianym) w poszczególnych sektorach oraz w szczególnych sytuacjach przetwarzania danych; oraz
- warunków usuwania linków do danych, kopii lub replikacji danych osobowych z publicznie dostępnych usług łączności, o których mowa w art. 17 ust. 2 (informowanie osób trzecich); oraz
- kryteriów i warunków ograniczania przetwarzania danych osobowych, o których mowa w art. 17 ust. 4.

Artykuł 17 dotyczy prawa do bycia zapomnianym

Ustęp 1 stanowi, że podmiot danych ma prawo do uzyskania od administratora usunięcia danych osobowych odnoszących się do niego oraz zaprzestania dalszego rozpowszechniania tych danych, zwłaszcza w odniesieniu do danych osobowych, które zostały udostępnione przez podmiot danych, kiedy był on dzieckiem, kiedy dane nie są już potrzebne do celów, do których były zebrane lub przetwarzane w inny sposób (lit. a)), podmiot danych odwołuje zgodę lub gdy minął okres przechowywania, na który wyrażono zgodę oraz jeśli nie ma już podstawy prawnej przetwarzania danych (lit. b)), podmiot danych sprzeciwia się przetwarzaniu danych osobowych zgodnie z art. 19 (lit. c)) lub przetwarzanie danych nie jest zgodne z niniejszym rozporządzeniem z innych powodów (lit. d)).

W proponowanych aktach delegowanych zostałyby doprecyzowane wymogi dotyczące stosowania prawa do bycia zapomnianym w różnych sektorach lub operacjach przetwarzania, warunków usuwania linków do danych, kopii i replikacji tych danych oraz ograniczeń operacji przetwarzania.

W celu zapewnienia zharmonizowanej interpretacji i wykonania art. 17 korzystne byłoby przedstawienie dalszych wytycznych na szczeblu europejskim, tak aby zarówno podmioty danych, jak i administratorzy znali swoje prawa i obowiązki w całej UE.

Ponieważ w samym rozporządzeniu nie można odpowiednio uwzględnić wszystkich istotnych sytuacji, dalsze wytyczne należy przedstawić w innym dokumencie.

W celu zapewnienia pewności prawa podmiotom danych i administratorom danych kwestie stosowania prawa do bycia zapomnianym w różnych sektorach lub operacjach przetwarzania, warunki usuwania linków do danych, kopii i replikacji tych danych i ograniczenia operacji przetwarzania należy uwzględnić w prawnie wiążącym dokumencie.

Dlatego też akt delegowany rzeczywiście wydaje się najwłaściwszym rozwiązaniem, pod warunkiem że zostanie przyjęty z chwilą wejścia w życie rozporządzenia.

Artykuł 20 ust. 5 – w celu doprecyzowania kryteriów i warunków odpowiednich środków służących zabezpieczeniu słusznym interesów podmiotu danych, o których mowa w art. 20 ust. 2 (wyjątki od zakazu profilowania).

Artykuł 20 dotyczy profilowania; ust. 2 tego artykułu stanowi, że z zastrzeżeniem innych przepisów niniejszego rozporządzenia, dana osoba może zostać poddana profilowaniu, jeżeli przetwarzanie odbywa się w trakcie zawierania lub wykonania umowy, jeśli wniosek w sprawie zawarcia lub wykonania umowy złożony przez podmiot danych został zrealizowany lub jeśli przewidziano właściwe środki w celu zabezpieczenia słusznym interesów podmiotu danych, jak np. prawo do uzyskania interwencji ze strony człowieka (lit. a)), jest wyraźnie dozwolone przez prawo Unii lub państwa członkowskiego, które ustanawia również właściwe środki w celu zabezpieczenia słusznym interesów podmiotu danych (lit. b)) lub odbywa się na podstawie zgody podmiotu danych (lit. c)).

Artykuł 20 ust. 1 stanowi, że „każda osoba fizyczna ma prawo nie podlegać środkowi, który wywołuje skutki prawne [...] lub ma istotny wpływ na tę osobę fizyczną [...] mającym służyć ocenie niektórych aspektów osobistych [...] lub też analizie bądź przewidzeniu zwłaszcza wyników w pracy, sytuacji ekonomicznej, miejsca przebywania, zdrowia, preferencji osobistych, wiarygodności lub zachowania tej osoby fizycznej”. Ustęp 2 zawiera trzy wyjątki od tego prawa.

Wydaje się, że kwestia, która ma zostać omówiona w proponowanym akcie delegowanym lub aktach delegowanych, odnosi się do nałożonego na administratora danych obowiązku ustalenia, czy osoba fizyczna może zostać poddana środkom, o których mowa w art. 20 ust. 1, na podstawie słusznym interesów podmiotu danych pomimo ogólnego zakazu.

Ze względu na fakt, że administrator nie zawsze może ustalić, jakiego rodzaju środki są odpowiednie do zabezpieczenia słusznym interesów podmiotu danych oraz ponieważ przepis ten dotyczy wyjątku od prawa przysługującego podmiotowi danych, który jest uprawniony do pewności prawa, wydaje się, że najwłaściwszym rozwiązaniem jest prawnie wiążący instrument. W celu uniknięcia fragmentacji oraz zagwarantowania takiego samego poziomu ochrony wszystkim osobom fizycznym należy zapewnić doprecyzowanie na szczeblu europejskim.

Dlatego też akt delegowany mógłby być właściwym instrumentem, pod warunkiem że zostanie przyjęty z chwilą wejścia w życie rozporządzenia. Ponadto wskazane byłoby również, aby EROD wydała dalsze wytyczne dotyczące kryteriów i warunków odpowiednich środków służących zabezpieczeniu słusznym interesów podmiotu danych.

Artykuł 22 ust. 4 – w celu doprecyzowania:

- dalszych kryteriów i wymogów dotyczących właściwych środków, o których mowa w art. 22 ust. 1, innych niż te omówione w art. 22 ust. 2;
- warunków mechanizmów weryfikacji i audytu, o których mowa w art. 22 ust. 3; oraz
- kryteriów proporcjonalności zgodnie z art. 22 ust. 3, oraz rozważenia szczególnych środków dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Artykuł 22 jest tak zwanym „artykułem ogólnej rozliczalności”; ust. 1 tego artykułu stanowi, że administrator przyjmuje polityki i realizuje odpowiednie środki w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z niniejszym rozporządzeniem, oraz wykazania tej zgodności. Ustęp 2 zawiera listę takich środków, natomiast ust. 3 stanowi, że administrator wdraża mechanizmy służące zapewnieniu weryfikacji skuteczności środków. Jeśli jest to właściwe, weryfikacja ta przeprowadzona jest przez niezależnych audytorów wewnętrznych lub zewnętrznych.

W art. 22 określa się obowiązek nałożony na administratorów dotyczący zapewnienia zgodności oraz opiera się na zasadzie odpowiedzialności. Zgodnie z tą zasadą wybór polityk i środków stosowanych w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z niniejszym rozporządzeniem, oraz wykazania tej zgodności należy pozostawić administratorowi, o ile są one właściwe i skuteczne zarazem. Odbywa się to zawsze z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej.

Ponieważ ust. 2 tego artykułu zawiera już niewyczerpujący zestaw przykładów dotyczących sposobów skonkretyzowania tego ogólnego obowiązku, wydaje się, że nawet doprecyzowanie dodatkowych kryteriów i wymogów nie jest konieczne.

Wdrażanie mechanizmów służących zapewnieniu weryfikacji skuteczności przyjętych środków również należy pozostawić administratorowi, ponieważ wybór najbardziej odpowiedniego mechanizmu zależy od sektora lub modelu biznesowego.

Podsumowując, ponieważ artykuł jako taki konkretyzuje zasadę rozliczalności, wydaje się, że nie jest konieczne doprecyzowanie dalszych kryteriów i wymogów dotyczących właściwych środków innych niż te omówione w ust. 2 ani warunków mechanizmów weryfikacji i audytu.

Jeżeli chodzi o szczególne traktowanie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, ogólny obowiązek dotyczący rozliczalności oraz przyjmowania polityk i realizowania odpowiednich środków w celu zapewnienia, by przetwarzanie danych osobowych odbywało się zgodnie z niniejszym rozporządzeniem, oraz wykazania tej zgodności powinny mieć zastosowanie niezależnie od wielkości administratora. Chociaż, oczywiście, należy umożliwić mikroprzedsiębiorcom oraz małym i średnim przedsiębiorcom przyjmowanie takich skalowalnych mechanizmów i środków. Ponadto w akcie delegowanym

nie można nigdy wprowadzać wyłączeń dla MŚP, których nie przewidziano już w treści samego rozporządzenia.

Artykuł 23 ust. 3 – w celu doprecyzowania kryteriów i wymogów dotyczących właściwych środków i mechanizmów, o których mowa w art. 23 ust. 1 i 2, w szczególności wymogów w zakresie uwzględnienia ochrony danych już w fazie projektowania w odniesieniu do sektorów, produktów i usług.

Artykuł 23 dotyczy zasad ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej.

Zgodnie z zasadą rozliczalności przewidzianą w art. 22 administrator powinien decydować, które odpowiednie środki i procedury techniczne i organizacyjne należy wdrożyć, aby zapewnić zgodność z zasadami ochrony danych już w fazie projektowania oraz ochrony danych jako opcji domyślnej.

Ponadto obowiązek nałożony na administratorów w art. 23 jest już wystarczająco jasny, ponieważ obciąża administratora odpowiedzialnością za wdrożenie odpowiednich środków i procedur.

Ponieważ podjęcie przez administratora odpowiednich środków i procedur można ocenić tylko w poszczególnych przypadkach, uwzględniając najnowsze osiągnięcia techniczne oraz koszty ich wdrożenia, uwzględnienie wszystkich sytuacji w rozporządzeniu wydaje się praktycznie niemożliwe.

Podsumowując, wydaje się, że dalsze przepisy lub wytyczne nie są konieczne. Użyteczne mogą się jednak okazać wytyczne wydane przez EROD.

Artykuł 26 ust. 5 – w celu doprecyzowania:

- kryteriów i wymogów dotyczących zakresu odpowiedzialności, obowiązków i zadań w odniesieniu do podmiotu przetwarzającego zgodnie z art. 26 ust. 1; oraz
- warunków, które umożliwiają uproszczenie przetwarzania danych osobowych w ramach grupy przedsiębiorstw, w szczególności do celów kontroli i sprawozdawczości.

Artykuł 26 ust. 1 stanowi, że jeśli operacja przetwarzania jest realizowana w imieniu administratora, administrator wybiera podmiot przetwarzający dający wystarczające gwarancje wdrożenia odpowiednich środków i procedur technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia i gwarantowało ochronę praw podmiotów danych, w szczególności jeśli chodzi o techniczne środki bezpieczeństwa i środki organizacyjne regulujące przetwarzanie, które ma być prowadzone, oraz zapewnia zgodność z tym środkami.

Wydaje się, że nie ma potrzeby doprecyzowania kryteriów i wymogów dotyczących zakresu odpowiedzialności, obowiązków i zadań w odniesieniu do podmiotu przetwarzającego ani też doprecyzowania warunków, które umożliwiają uproszczenie przetwarzania danych osobowych w ramach grupy przedsiębiorstw, w szczególności do celów kontroli i sprawozdawczości, biorąc pod uwagę wymogi już określone w rozporządzeniu, zwłaszcza w zakresie rozliczalności administratora.

Administratorzy mają obowiązek dopilnować, aby podmiot przetwarzający dawał wystarczające gwarancje, tak by przetwarzanie odpowiadało wymogom rozporządzenia. Ponadto w ust. 2 tego artykułu określono już, jakie aspekty należy uwzględnić w umowie lub w innym wiążącym dokumencie.

Ponadto ponieważ wiele różnych czynników może wpływać na relację pomiędzy administratorem a podmiotem przetwarzającym dane, sposób skonkretyzowania tego obowiązku należy oceniać w każdym przypadku oddzielnie.

Jeżeli chodzi o doprecyzowanie warunków, które umożliwiają uproszczenie przetwarzania danych osobowych w ramach grupy przedsiębiorstw, również tę kwestię należy pozostawić administratorowi zgodnie z zasadą rozliczalności, zważywszy że istnieje już obowiązek dopilnowania w ramach wiążącej umowy, aby operacja przetwarzania spełniała wymogi rozporządzenia.

Co więcej, w przypadku wymiany danych z częściami przedsiębiorstwa spoza EOG w rozporządzeniu przewiduje się już możliwość stosowania wiążących reguł korporacyjnych.

Z uwagi na powyższe żadne dalsze przepisy ani wytyczne nie są konieczne.

Artykuł 28 ust. 5 – w celu doprecyzowania kryteriów i wymogów dotyczących dokumentacji, o której mowa w art. 28 ust. 1, by uwzględnić w szczególności zakres odpowiedzialności administratora i podmiotu przetwarzającego oraz ewentualnie przedstawiciela administratora.

Artykuł 28 dotyczy obowiązku administratorów w zakresie prowadzenia dokumentacji.

Zgodnie z zasadą rozliczalności wydaje się właściwe, aby wybór konkretnego sposobu zapewnienia zgodności z dokumentacją pozostawić administratorowi, podmiotowi przetwarzającemu oraz przedstawicielowi administratora.

Ponadto art. 28 ust. 2 zawiera już niewyczerpującą listę minimalnych informacji, które powinna zawierać dokumentacja. **Wydaje się, że jeszcze dalsze doprecyzowanie kryteriów i wymogów nie jest konieczne.**

Artykuł 30 ust. 3 – w celu doprecyzowania kryteriów i warunków dotyczących środków technicznych i organizacyjnych, o których mowa w art. 30 ust. 1 i 2, w tym zdefiniowania pojęcia najnowszych osiągnięć technicznych, dla konkretnych sektorów oraz w konkretnych sytuacjach przetwarzania danych, uwzględniając w szczególności rozwój technologii oraz rozwiązania w zakresie uwzględnienia ochrony prywatności już w fazie projektowania oraz ochrony danych jako opcji domyślnej, chyba że zastosowanie ma art. 30 ust. 4 (akty wykonawcze).

Artykuł 30 dotyczy bezpieczeństwa przetwarzania.

Zgodnie z zasadą rozliczalności decyzję w kwestii wdrażania odpowiednich środków technicznych i organizacyjnych, by zapewnić poziom bezpieczeństwa stosowny do ryzyk związanych z przetwarzaniem oraz charakterem danych osobowych, które należy chronić, uwzględniając najnowsze osiągnięcia techniczne oraz koszty ich wdrożenia należy pozostawić administratorowi.

Doprecyzowanie kryteriów i warunków dotyczących środków technicznych i organizacyjnych nie pozwoliłoby na uwzględnienie wszystkich różnych sytuacji, do których dochodzi pomiędzy sektorami a operacjami przetwarzania.

Jednym z celów przeglądu pakietu prawnego w zakresie ochrony danych jest zachowanie neutralności pod względem technologicznym. W proponowanych aktach delegowanych znalazłoby się jednak również doprecyzowanie definicji pojęcia najnowszych osiągnięć technicznych. Mimo iż akt delegowany jako taki może nie być neutralny pod względem technologicznym, określenie pojęcia najnowszych osiągnięć technicznych w prawnie wiążącym instrumencie może być niewłaściwe. Ponadto wiązałoby się z tym poważne ryzyko, że taka definicja już w chwili przyjęcia byłaby nieaktualna.

Dlatego też wydaje się, że doprecyzowanie poprzez przyjęcie aktu delegowanego nie jest właściwe. W stosownych przypadkach można by było jednak przewidzieć dalsze wytyczne EDOR.

Artykuł 31 ust. 5 – w celu doprecyzowania kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych osobowych, o którym mowa w art. 31 ust. 1 i 2, oraz szczególnych okoliczności, w których administrator i podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych.

Artykuł 31 dotyczy obowiązku administratora dotyczącego zgłoszenia organowi nadzorczemu naruszenia ochrony danych osobowych.

Ustęp 1 stanowi, że w przypadku naruszenia ochrony danych osobowych administrator zgłasza organowi nadzorczemu takie naruszenie bez nieuzasadnionej zwłoki i, jeśli jest to możliwe, nie później niż w ciągu 24 godzin od momentu dowiedzenia się o tym naruszeniu. Jeśli organ nadzorczy nie zostanie zawiadomiony w ciągu 24 godzin, do zgłoszenia należy dołączyć umotywowane wyjaśnienie.

Ustęp 2 stanowi, że na mocy art. 26 ust. 2 lit. f) podmiot przetwarzający ostrzega i informuje administratora niezwłocznie po stwierdzeniu naruszenia ochrony danych osobowych.

Proponowany akt delegowany odnosi się do kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych oraz do szczególnych okoliczności, w których administrator i podmiot przetwarzający mają obowiązek zgłosić naruszenie ochrony danych osobowych.

Zapewnienie wytycznych w zakresie kryteriów i wymogów dotyczących stwierdzenia naruszenia ochrony danych oraz szczególnych okoliczności, w których należy zgłosić takie naruszenie, jest istotne; należy wyjaśnić, co stanowi naruszenie ochrony danych osobowych.

Aby zapewnić zharmonizowane wdrażanie i stosowanie obowiązku zgłaszania organowi nadzorczemu naruszenia ochrony danych osobowych, należy zapewnić dalsze wytyczne na szczeblu europejskim.

Zważywszy na znaczenie tej kwestii dla wszystkich właściwych zainteresowanych stron, należy zapewnić jasność w prawie wiążącym akcie, a ponieważ stanowi ona istotną część zasad i obowiązków, należy ją uwzględnić w treści samego rozporządzenia.

Dlatego też zamiast doprecyzowywać kryteria i wymogi dotyczące stwierdzenia naruszenia ochrony danych oraz okoliczności, w których należy zgłosić takie naruszenie, w akcie delegowanym, przynajmniej główne ramy należy jasno określić w treści rozporządzenia.

Określenie pewnych szczegółów w akcie delegowanym byłoby pożądane, pod warunkiem że zostanie on przyjęty co najmniej z chwilą wejścia rozporządzenia w życie.

Artykuł 32 ust. 5 – w celu doprecyzowania kryteriów i wymogów dotyczących okoliczności, w których naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na dane osobowe, o których mowa w art. 32 ust. 1.

Artykuł 32 dotyczy obowiązku informowania przez administratora podmiotu danych o naruszeniu ochrony danych osobowych.

Ustęp 1 stanowi, że gdy istnieje prawdopodobieństwo, że naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na ochronę danych osobowych lub prywatność podmiotu danych, administrator, po dokonaniu zgłoszenia organowi nadzorczemu, bez nieuzasadnionej zwłoki informuje podmiot danych o naruszeniu ochrony danych osobowych.

Proponowany akt delegowany odnosi się do kryteriów i wymogów dotyczących okoliczności, w których naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na dane osobowe (ich ochronę) lub prywatność podmiotu danych.

Zapewnienie wytycznych w sprawie kryteriów i wymogów dotyczących okoliczności, w których naruszenie ochrony danych osobowych może mieć taki niekorzystny wpływ, jest faktycznie istotne. Należy wyjaśnić, w jakich warunkach wymaga się informowania podmiotu danych.

Aby zapewnić zharmonizowane wdrażanie i stosowanie obowiązku dotyczącego informowania podmiotu danych o naruszeniu ochrony danych osobowych, należy lepiej wyjaśnić tę kwestię na szczeblu europejskim.

Zważywszy na znaczenie tej kwestii dla wszystkich właściwych zainteresowanych stron, należy zapewnić jasność w prawnie wiążącym akcie, a ponieważ stanowi ona istotną część zasad i obowiązków, należy ją uwzględnić w treści samego rozporządzenia.

Dlatego też zamiast doprecyzowywać kryteria i wymogi dotyczące okoliczności, w których naruszenie ochrony danych osobowych może niekorzystnie wpłynąć na dane osobowe i w których należy poinformować podmiot danych o takim naruszeniu, w akcie delegowanym, przynajmniej główne ramy należy jasno określić w treści rozporządzenia.

Określenie pewnych szczegółów w akcie delegowanym byłoby pożądane, pod warunkiem że jego pierwsze przyjęcie nastąpi przed wejściem rozporządzenia w życie.

Artykuł 33 ust. 6 – w celu doprecyzowania:

- kryteriów i warunków operacji przetwarzania mogących stwarzać szczególne ryzyko, o którym mowa w art. 33 ust. 1 i 2 oraz

- wymogów w zakresie oceny, o których mowa w art. 33 ust. 3, w tym warunków skalowalności, weryfikowalności i sprawdzenia.

W tym celu Komisja rozważa szczególne środki dla mikroprzedsiębiorców oraz małych i średnich przedsiębiorców.

Artykuł 36 dotyczy obowiązku przeprowadzenia oceny skutków w zakresie ochrony danych.

Ustęp 1 stanowi, że jeśli operacje przetwarzania stwarzają szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów, administrator lub podmiot przetwarzający przeprowadzają w imieniu administratora danych ocenę skutków przewidywanych operacji przetwarzania w zakresie ochrony danych osobowych. W ust. 2 przewiduje się 5 operacji przetwarzania, które stwarzają szczególne ryzyko.

Ustęp 3 stanowi, że ocena obejmuje przynajmniej ogólny opis przewidywanych operacji przetwarzania, ocenę ryzyka dla praw i wolności podmiotów danych, środki przewidywane w celu sprostania ryzykom, gwarancje, środki i mechanizmy bezpieczeństwa mające zagwarantować ochronę danych osobowych oraz wykazać zgodność z niniejszym rozporządzeniem, uwzględniając prawa i słusze interesy podmiotów danych i innych zainteresowanych osób.

Administratorzy przeprowadzają ocenę skutków ochrony danych, jeśli operacja przetwarzania stwarza (może stwarzać) szczególne ryzyko dla praw i wolności podmiotów danych z racji swego charakteru, zakresu lub celów. Zgodnie z zasadą rozliczalności ustalenie, czy operacje przetwarzania stwarzają (mogą stwarzać) szczególne ryzyko dla praw i wolności podmiotów danych, należy pozostawić administratorowi.

Jest to jednak istotna kwestia wpływająca na to, czy administrator ma obowiązek przeprowadzenia oceny skutków ochrony danych oraz czy stwarza ona szczególne ryzyko dla praw i wolności podmiotów danych. Spójność na szczeblu europejskim jest istotna, aby zapewnić zharmonizowaną interpretację i stosowanie artykułu.

Ogólne wymogi dotyczące oceny, czy operacja przetwarzania stwarza szczególne ryzyko, można ustanowić w akcie delegowanym. EROD mogłaby ewentualnie lub dodatkowo zapewnić dalsze wytyczne, pod warunkiem, że żadna ewentualna lista operacji przetwarzania zidentyfikowanych jako stwarzające szczególne ryzyko nie byłaby wyczerpująca.

Jeżeli chodzi o szczególne traktowanie mikroprzedsiębiorców oraz małych i średnich przedsiębiorców, wydaje się, że brakuje przesłanek, by uznać to za konieczne. Ponieważ cele

tego artykułu polegają na ustanowieniu dodatkowych gwarancji w przypadkach, gdy operacja przetwarzania stwarza (przypuszczalnie stworzy) szczególne ryzyko dla praw i wolności podmiotów danych, tym bardziej nie należy zwalniać administratorów z tego obowiązku ze względu na ich wielkość. Ponadto już w samym artykule ustanawia się próg przez sformułowanie „stwarzają (mogą stwarzać) szczególne ryzyko [...]”, co stanowi wyłączenie ze względu na charakter przetwarzania, co jest bardziej uzasadnione niż wyłączenie ze względu na liczbę pracowników. Ponadto w akcie delegowanym nie można nigdy wprowadzać wyłączeń dla MŚP, których nie przewidziano już w treści samego rozporządzenia.

Artykuł 34 ust. 8 – w celu doprecyzowania kryteriów i warunków ustalenia wysokiego poziomu szczególnych ryzyk, o których mowa w art. 34 ust. 2 lit. a) (uprzednia konsultacja po ocenie skutków ochrony danych).

Artykuł 34 dotyczy obowiązku nałożonego na administratorów dotyczącego uzyskania uprzedniego zezwolenia od organu nadzorczego lub konsultacji z takim organem. W art. 34 ust. 2 lit. a) szczegółowo omawia się nałożony na administratorów obowiązek przeprowadzenia konsultacji z organem nadzorczym przez przetwarzaniem danych osobowych, by zapewnić zgodność planowanego przetwarzania z niniejszym rozporządzeniem, w szczególności by złagodzić ryzyko dla podmiotów danych, jeśli ocena skutków w zakresie ochrony danych wskazała, że operacje przetwarzania danych mogą, ze względu na swój charakter, zakres lub cele, wiązać się z wysokim poziomem szczególnych ryzyk.

Proponowany akt delegowany lub proponowane akty delegowane doprecyzowałyby kryteria i wymogi dotyczące określania wysokiego poziomu szczególnych ryzyk stwarzanych przez operację przetwarzania, po przeprowadzeniu oceny skutków w zakresie ochrony danych.

Chociaż wskazane wydawałoby się pozostawienie administratorowi decyzji, czy ryzyko zidentyfikowane po przeprowadzeniu tej oceny jest ryzykiem wysokim, chodzi tutaj o ryzyko związane z danymi lub prywatnością podmiotu danych, co oznacza, że istotne jest zapewnienie dalszych wytycznych. W celu zapewnienia zharmonizowanego podejścia w UE należy doprecyzować kryteria i wymogi na szczeblu europejskim.

Ponieważ każda operacja przetwarzania jest inna, wystąpienie wysokiego poziomu szczególnych ryzyk zależałoby od meritum sprawy. Uwzględnienie wszystkich możliwych sytuacji w prawnie wiążącym dokumencie jest praktycznie niemożliwe, dlatego też właściwy wydaje się bardziej elastyczny instrument.

Ponadto ponieważ organy nadzorcze muszą rozpatrywać wnioski o uprzednie zezwolenie i uprzednią konsultację, najbardziej właściwe byłoby, aby EROD wydawała wytyczne, tym bardziej, że EROD jest już zaangażowana w sprawy, w których organy uznają uprzednią konsultację za niezbędną.

Podsumowując, zamiast aktu delegowanego wytyczne EROD byłyby najwłaściwszym rozwiązaniem w celu doprecyzowania kryteriów i wymogów dotyczących określania wysokiego poziomu szczególnych ryzyk, które stwarzają (przypuszczalnie tworzą) operacje przetwarzania w następstwie oceny skutków w zakresie ochrony danych.

Artykuł 35 ust. 11 – w celu doprecyzowania:

- kryteriów i wymogów dotyczących głównej działalności administratora lub podmiotu przetwarzającego, o której mowa art. 35 ust. 1 lit. c) oraz**
- kryteriów dotyczących kwalifikacji zawodowych inspektora ochrony danych, o których mowa w art. 35 ust. 5.**

W art. 35 nakłada się na administratorów i podmioty przetwarzające obowiązek wyznaczenia inspektora ochrony danych w każdym przypadku, w którym przetwarzania dokonuje organ lub podmiot publiczny (ust. 1 lit. a)); przetwarzania dokonuje przedsiębiorstwo zatrudniające 250 osób lub więcej (ust. 1 lit. b)); lub główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych (ust. 1 lit. c)).

Artykuł 35 ust. 5 stanowi, że administrator lub podmiot przetwarzający wyznaczają inspektora ochrony danych na podstawie jego kwalifikacji zawodowych oraz w szczególności jego wiedzy specjalistycznej z zakresu prawa ochrony danych oraz praktyki w tym zakresie.

Jeden z proponowanych aktów delegowanych zawierałby doprecyzowanie kryteriów i wymogów dotyczących głównej działalności administratora lub podmiotu przetwarzającego polegającej na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych.

W celu zapewnienia zharmonizowanej interpretacji i stosowania art. 35 korzystne byłyby dalsze przepisy na szczeblu europejskim. Ustanowienie takich przepisów w prawnie wiążącym dokumencie mogłoby objąć wiele różnych sytuacji, przynajmniej w głównych ramach, chociaż prawdopodobnie nie byłyby one wyczerpujące.

Akt delegowany określający główne ramy byłby właściwym instrumentem. Dodatkowo wytyczne EDOR mogłoby pomóc w doprecyzowaniu kryteriów i wymogów dotyczących głównej działalności administratora lub podmiotu przetwarzającego wymagającej monitorowania podmiotów danych.

Proponuje się również przyjęcie aktu delegowanego w celu doprecyzowania kryteriów dotyczących kwalifikacji zawodowych inspektora ochrony danych.

Zgodnie z zasadą rozliczalności ocena kwalifikacji zawodowych inspektora ochrony danych powinna przynajmniej do pewnego stopnia leżeć w gestii administratora lub podmiotu przetwarzającego. Rodzaj kwalifikacji zawodowych, jakie powinien mieć inspektor ochrony danych, w dużej mierze zależy od sektora i modelu biznesowego. Znaczna rozbieżność w podejściu do tej kwestii w poszczególnych państwach członkowskich – na poziomie sektora

bądź na innym poziomie – poważnie naruszyłyby jednak równe warunki działania i wzajemne zaufanie będące celem rozporządzenia, którego dotyczy wniosek.

Podsumowując, właściwe byłoby, aby w akcie delegowanym doprecyzować główne ramy kryteriów dotyczących kwalifikacji zawodowych inspektora ochrony danych. Dodatkowe wytyczne mogłaby zapewnić EDOR.

Artykuł 37 ust. 2 – w celu doprecyzowania kryteriów i wymogów dotyczących zadań, certyfikacji, statusu, uprawnień i zasobów inspektora ochrony danych, o których mowa w art. 37 ust. 1.

Artykuł 37 dotyczy zadań inspektora ochrony danych; w ustępie 1 tego artykułu wymienia się minimalny zakres zadań powierzanych inspektorowi ochrony danych przez administratora lub podmiot przetwarzający.

Ogólny obowiązek przewidziany w art. 37 ust. 1 jest już dosyć jasny, ponieważ odpowiedzialność za dopilnowanie, aby określone zadania zostały powierzone inspektorowi ochrony danych, nakłada się w nim na administratora i podmiot przetwarzający. Ponadto ust. 1 zawiera już listę określającą minimalny zakres zadań, które należy powierzyć inspektorowi ochrony danych.

Zgodnie z zasadą rozliczalności określenie warunków działania inspektora ochrony danych powinno przynajmniej do pewnego stopnia leżeć w gestii administratora lub podmiotu przetwarzającego. Rodzaj tych warunków może być uzależniony od różnych czynników.

Znaczna rozbieżność w podejściu do tej kwestii w poszczególnych państwach członkowskich – na poziomie sektora bądź na innym poziomie – również w tym przypadku poważnie naruszyłaby jednak równość warunków działania i wzajemne zaufanie będące celem rozporządzenia, którego dotyczy wniosek. Ponadto warunki te wpłynęłyby również na niezależną pozycję inspektorów ochrony danych.

Podsumowując, właściwe byłoby, aby w akcie delegowanym doprecyzować główne ramy zadań, certyfikacji, statusu, uprawnień i zasobów inspektora ochrony danych, o których mowa w art. 37 ust. 1. Dodatkowe wytyczne mogłaby zapewnić EROD.

Artykuł 39 ust. 2 – w celu doprecyzowania:

- kryteriów i wymogów dotyczących mechanizmów certyfikacji w zakresie danych osobowych, o których mowa w art. 39 ust. 1, w tym warunków przyznawania i odwoływania; oraz**
- wymogów w zakresie uznawania na terytorium Unii i w państwach trzecich.**

Artykuł 39 stanowi, że państwa członkowskie i Komisja zachęcają, w szczególności na poziomie europejskim, do ustanawiania mechanizmów certyfikacji w zakresie danych osobowych oraz pieczęci i oznaczeń w zakresie ochrony danych, które umożliwią podmiotom danych szybką ocenę poziomu ochrony danych zapewnionej przez administratorów i podmioty przetwarzające.

Biorąc pod uwagę fakt, że wiarygodność mechanizmów certyfikacji w zakresie danych osobowych, pieczęci i oznaczeń w dużym stopniu zależy od kryteriów i wymogów określonych w celu ich ustanowienia, istotne jest, aby zapewnić dalsze wytyczne.

Ponieważ do stosowania mechanizmów certyfikacji należy zachęcać w szczególności na szczeblu europejskim, określenia dalszych kryteriów i wymogów również należy dokonać na szczeblu europejskim.

Ponieważ szczegółowe określenie wszystkich kryteriów i wymogów w całości w treści rozporządzenia byłoby trudne, właściwe byłoby przyjęcie bardziej elastycznego instrumentu w celu zapewnienia dalszych kryteriów i wytycznych dotyczących mechanizmów certyfikacji w zakresie danych osobowych, w tym warunków przyznawania i odwoływania oraz wymogów w zakresie uznawania na terytorium Unii i w państwach trzecich.

Wydaje się, że najwłaściwszym instrumentem do zapewnienia pewności prawa wobec podmiotów danych, które polegają na mechanizmach certyfikacji, pieczęciach i oznaczeniach, byłby istotnie akt delegowany.

Artykuł 43 ust. 3 – w celu doprecyzowania:

- kryteriów i wymogów dotyczących wiążących reguł korporacyjnych w rozumieniu tego artykułu, w szczególności jeśli chodzi o kryteria ich zatwierdzania;
- stosowania art. 43 ust. 2 lit. b), d), e) i f) do wiążących reguł korporacyjnych, które przyjęły podmioty przetwarzające; oraz
- innych niezbędnych wymogów w celu zapewnienia ochrony danych osobowych podmiotu danych.

Artykuł 43 dotyczy międzynarodowych transferów na podstawie wiążących reguł korporacyjnych. Ustęp 2 lit. b), d) e) i f) stanowi, że wiążące reguły korporacyjne powinny określać co najmniej operację lub zestaw operacji przekazywania danych (lit. b)), ogólne zasady ochrony danych, środki mające na celu zapewnienie bezpieczeństwa danych oraz wymogi w zakresie dalszego przekazywania organizacjom, które nie są związane politykami (lit. d)), prawa podmiotów danych oraz środki umożliwiające wykonywanie tych praw (lit. e)) oraz przyjęcie przez administratora lub podmiot przetwarzający mających siedzibę na terytorium państwa członkowskiego odpowiedzialności za naruszenie wiążących reguł korporacyjnych przez członka grupy przedsiębiorstw niemającego siedziby na terytorium Unii (lit. f)).

Po pierwsze, akty delegowane przewiduje się w celu doprecyzowania kryteriów i wymogów dotyczących wiążących reguł korporacyjnych w rozumieniu tego artykułu ogółem, a w szczególności jeżeli chodzi o kryteria ich zatwierdzania. Już jednak ust. 1 stanowi, że zgodnie z mechanizmem zgodności przewidzianym w art. 58 zatwierdzenie wiążących reguł korporacyjnych leży w gestii organu nadzorczego. W tym samym ustępie określa się również pewne wymogi, które organ nadzorczy musi uwzględnić.

Wydaje się, że już te przepisy ustanawiają wystarczającą liczbę mechanizmów kontrolnych i równoważących, aby zapewnić uwzględnienie wszystkich wymaganych aspektów w wiążącej regule korporacyjnej. Ponadto, biorąc pod uwagę fakt, że przy zatwierdzaniu wiążącej reguły korporacyjnej należy stosować mechanizm zgodności, zaangażowanie na szczeblu europejskim już istnieje.

Co więcej, zatwierdzanie wiążących reguł korporacyjnych jest zadaniem organów nadzorczych. Akty delegowane dotyczące doprecyzowania kryteriów i wymogów ogółem, a w szczególności ich zatwierdzania, stwarzałyby ryzyko naruszenia niezależności organów nadzorczych i EROD.

Dlatego też wydaje się, że doprecyzowanie kryteriów i wymogów dotyczących wiążących reguł korporacyjnych ogółem, a w szczególności ich zatwierdzania, nie jest konieczne.

Po drugie, akty delegowane przewiduje się w celu doprecyzowania stosowania art. 43 ust. 2 lit. b), d), e) i f) w odniesieniu do wiążących reguł korporacyjnych, które przyjęły podmioty

przetwarzające. Zważywszy że chodzi o kluczowe kwestie, do których należy się odnieść w wiążących regułach korporacyjnych, zapewnienie dalszej harmonizacji byłoby korzystne.

Ponieważ wiążąca reguła korporacyjna będzie stosowana w całej UE, należy zapewnić zharmonizowane stosowanie i zharmonizowaną wykładnię.

Biorąc pod uwagę fakt, że każda wiążąca reguła korporacyjna zależy od modelu biznesowego przedsiębiorstwa i sektora, w którym prowadzi ono działalność, uwzględnienie wszystkich sytuacji w treści samego rozporządzenia jest praktycznie niemożliwe. Dlatego też można zastosować bardziej elastyczny instrument.

Akt delegowany byłby właściwym instrumentem. Dodatkowo, ponieważ EROD będzie zaangażowana w proces wynikający z obowiązku stosowania mechanizmu zgodności przy zatwierdzaniu wiążących reguł korporacyjnych, wskazane byłoby, aby EROD wydała wytyczne dotyczące stosowania artykułów w odniesieniu do wiążących reguł korporacyjnych, które przyjęły podmioty przetwarzające.

Po trzecie, akty delegowane proponuje się w odniesieniu do dalszych niezbędnych wymogów w celu zapewnienia ochrony danych osobowych podmiotu danych.

Zgodnie z zasadą rozliczalności zapewnienie zgodności z prawem, zawsze z zastrzeżeniem nadzoru, egzekwowania i kontroli sądowej, należy pozostawić administratorowi lub podmiotowi przetwarzającemu. Ponadto, wydaje się, że artykuł wystarczająco jasno wyjaśnia, w jaki sposób należy zatwierdzać wiążącą regułę korporacyjną, kto za to odpowiada, na podstawie jakich kryteriów i jaki powinien być minimalny zakres wiążącej reguły korporacyjnej.

Rolą organów nadzorczych jest zatwierdzanie wiążących reguł korporacyjnych oraz, w razie potrzeby, podejmowanie działań w zakresie egzekwowania, dlatego też akty delegowane dotyczące dalszych niezbędnych wymogów w celu zapewnienia ochrony danych osobowych podmiotu danych stwarzałyby poważne ryzyko naruszenia niezależności organów nadzorczych.

Ponieważ EROD będzie zaangażowana w proces wynikający z obowiązku stosowania mechanizmu zgodności przy zatwierdzaniu wiążących reguł korporacyjnych, wskazane byłoby, aby Europejska Rada Ochrony Danych wydała wytyczne dotyczące stosowania artykułów w odniesieniu do wiążących reguł korporacyjnych, które przyjęły podmioty przetwarzające.

Artykuł 44 ust. 7 – w celu doprecyzowania:

- „istotnego interesu publicznego” w rozumieniu art. 44 ust. 1 lit d); a także
- kryteriów i wymogów dotyczących odpowiednich gwarancji, o których mowa w art. 44 ust. 1 lit. h).

Artykuł 44 dotyczy odstępstw od ogólnego zakazu przekazywania danych osobowych państwom trzecim i organizacjom międzynarodowym

Ustęp 1 lit. d) stanowi, że operacja lub zestaw operacji przekazywania danych osobowych państwu trzeciemu lub organizacji międzynarodowej może nastąpić pod warunkiem, że przekazanie jest niezbędne ze względu na istotny interes publiczny.

Ustęp 1 lit. h) stanowi, że operacja lub zestaw operacji przekazywania danych osobowych państwu trzeciemu lub organizacji międzynarodowej może nastąpić pod warunkiem, że przekazanie jest konieczne dla potrzeb wynikających ze słuszných interesów administratora lub podmiotu przetwarzającego, których nie można uznać za częste lub masowe i jeżeli administrator lub podmiot przetwarzający ocenili wszystkie okoliczności towarzyszące operacji przekazywania danych lub operacjom przekazywania danych i na podstawie tej oceny w razie potrzeby przewidzieli odpowiednie gwarancje w zakresie ochrony danych osobowych.

Akty delegowane proponuje się w celu doprecyzowania, co stanowi „istotny interes publiczny” w odniesieniu do odstępstwa od ogólnego zakazu przekazywania danych osobowych państwom trzecim lub organizacjom międzynarodowym. Doprecyzowanie „istotnego interesu publicznego” dotyczy zasadniczego elementu określającego zgodność z prawem operacji przekazywania danych, dlatego też należy uwzględnić tę kwestię w treści samego rozporządzenia.

W celu zapewnienia zharmonizowanego stosowania w UE należy doprecyzować tę kwestię w treści samego rozporządzenia.

Akty delegowane przewiduje się w celu doprecyzowania kryteriów i wymogów dotyczących odpowiednich gwarancji, o których mowa w art. 44 ust. 1 lit h).

Grupa robocza pragnie podkreślić konieczność doprecyzowania pojęcia „słusznego interesu” w art. 44 ust. 1 lit. h) rozporządzenia, o którym była już również mowa w odniesieniu do proponowanego aktu delegowanego w art. 6 ust. 5. Wskazówki takie można by było zapewnić w odpowiednich wytycznych EROD; alternatywnym lub dodatkowym rozwiązaniem mogłoby być przedstawienie niewyczerpującej listy przykładów „słusznego interesu” w jednym z motywów rozporządzenia.

Jeżeli chodzi o ustalenie, co stanowiłoby odpowiednią gwarancję, dalsze wytyczne wydają się istotne, ponieważ dotyczą one odstępstwa od ogólnego zakazu przekazywania danych państwom trzecim lub organizacjom międzynarodowym zgodnie ze słusznym interesem i bez udziału organu nadzorczego.

Uwzględnienie wszystkich możliwych rodzajów odpowiednich gwarancji (obecnie i w przyszłości) w treści samego rozporządzenia byłoby jednak niemożliwe. Dlatego też właściwszy byłby bardziej elastyczny instrument.

Wydaje się zatem, że w celu zapewnienia harmonizacji interpretacji i stosowania właściwym instrumentem będzie akt delegowany. Europejska Rada Ochrony Danych mogłaby dodatkowo wydać wytyczne w celu doprecyzowania, co stanowi odpowiednie gwarancje, o których mowa w art. 44 ust. 1 lit. h).

Artykuł 79 ust. 7 – w celu aktualizacji kwot grzywien administracyjnych, o których mowa w art. 79 ust. 4, 5 i 6, biorąc pod uwagę warunki, o których mowa w art. 79 ust. 2.

Artykuł 79 dotyczy sankcji administracyjnych. W ust. 4, 5 i 6 określa się maksymalne kwoty grzywien, a ust. 2 stanowi, że sankcja administracyjna w każdym indywidualnym przypadku jest skuteczna, proporcjonalna i odstrasżająca oraz zawiera dalsze kryteria określania wysokości grzywny.

Zważywszy że nowy pakiet prawny powinien mieć zastosowanie przez co najmniej kilka dekad, istotne jest, aby umożliwić indeksację grzywien, a tym samym dopuścić dostosowywania do kwot grzywien w przyszłości.

W celu uniknięcia różnic między państwami członkowskimi oraz zapewnienia zharmonizowanego maksymalnego poziomu w UE aktualizacje te należy ustanawiać na szczeblu UE.

Aby zapewnić przejrzystości dla wszystkich zainteresowanych stron, należy zastosować prawnie wiążący dokument.

Właściwe wydaje się zatem zastosowanie aktów delegowanych w celu aktualizacji kwot grzywien administracyjnych, o których mowa w art. 79 ust. 4, 5 i 6, z uwzględnieniem kryteriów zawartych w ust. 2 tego artykułu.

Artykuł 81 ust. 3 –w celu dalszego określenia innych przesłanek z zakresu interesu publicznego w obszarze zdrowia publicznego, o których mowa w art. 81 ust. 1 lit. b), jak również

- kryteriów i wymogów dla gwarancji przetwarzania danych osobowych dla celów, o których mowa w art. 81 ust. 1.

Artykuł 81 stanowi, że w granicach niniejszego rozporządzenia i zgodnie z art. 9 ust. 2 lit. h) przetwarzanie danych osobowych dotyczących zdrowia musi odbywać się na podstawie prawa Unii lub prawa państwa członkowskiego, które przewiduje odpowiednie i konkretne środki mające na celu zabezpieczenie uzasadnionych interesów podmiotu danych i które są niezbędne dla celów medycyny prewencyjnej lub medycyny pracy (lit. a)) lub ze względu na interes publiczny w dziedzinie zdrowia publicznego (lit. b)) lub ze względu na inne przesłanki z zakresu interesu publicznego (lit. c)).

Proponowany akt delegowany lub proponowane akty delegowane zawierałyby doprecyzowanie przesłanek z zakresu interesu publicznego w dziedzinie zdrowia publicznego, jak również kryteriów i wymogów dla gwarancji przetwarzania danych osobowych do celów, o których mowa w art. 81 ust. 1.

Jakie są przesłanki z zakresu interesu publicznego w dziedzinie zdrowia publicznego oraz kryteria i wymogi dla gwarancji należy określić w wiążącym akcie prawnym. Ponieważ zawarcie tak szczegółowych informacji w treści samego rozporządzenia jest niemożliwe, bardziej właściwy byłby inny instrument.

W art. 81 ust. 1 to państwom członkowskim pozostawiono w pewnym zakresie zadanie zadbania w prawie krajowym o to, by przetwarzanie danych w sektorze opieki zdrowotnej odbywało się zgodnie z prawem.

Akty delegowane wydają się zatem najwłaściwszymi instrumentami, z zastrzeżeniem jednak art. 81 ust. 1.

Artykuł 82 ust. 3 – w celu dalszego określenia innych warunków i wymogów gwarancji przetwarzania danych osobowych dla celów, o których mowa w art. 82 ust. 1.

Artykuł 82 dotyczy przetwarzania danych w kontekście zatrudnienia.

Proponowany akt delegowany lub proponowane akty delegowane zawierałyby doprecyzowanie kryteriów i wymogów gwarancji przetwarzania danych osobowych w kontekście zatrudnienia.

Dalsze kryteria i wymogi gwarancji przetwarzania danych osobowych w tym kontekście należy określić w wiążącym akcie prawnym. Ponieważ zawarcie tak szczegółowych informacji w treści samego rozporządzenia jest niemożliwe, bardziej właściwy byłby inny instrument.

W art. 82 ust. 1 to państwom członkowskim pozostawiono w pewnym zakresie zadanie zadbania w prawie krajowym o to, by przetwarzanie danych w kontekście zatrudnienia odbywało się zgodnie z prawem.

Akty delegowane wydają się zatem najwłaściwszymi instrumentami, z zastrzeżeniem jednak art. 82 ust. 1.

Artykuł 83 ust. 3 – w celu doprecyzowania:

- kryteriów i wymogów dotyczących przetwarzania danych osobowych dla celów, o których mowa w art. 83 ust. 1 i ust. 2, jak również
- niezbędnych ograniczeń prawa do informacji i dostępu przysługującego podmiotowi danych; oraz
- doprecyzowania warunków praw podmiotów danych w tych okolicznościach i gwarancji tych praw.

Artykuł 83 dotyczy przetwarzania do celów dokumentacji, statystyki i badań naukowych.

Ustęp 1 stanowi, że w granicach omawianego rozporządzenia można przetwarzać dane osobowe do celów dokumentacji, statystyki i badań naukowych jedynie wtedy, gdy nie można ich inaczej uzyskać przez przetwarzanie danych, które nie umożliwiają lub przestały umożliwiać identyfikację osoby, której dane dotyczą (lit. a)) oraz dane umożliwiające przypisanie informacji do zidentyfikowanej podmiotu danych lub do zidentyfikowania, są przechowywane oddzielnie od innych informacji, tak długo jak cele te można osiągnąć w ten sposób (lit. b)).

Ustęp 2 stanowi, że podmioty prowadzące badania historyczne, statystyczne lub naukowe mogą publikować lub ujawniać publicznie w inny sposób dane osobowe jedynie wtedy, gdy podmiot danych udzielił zgody (lit. a)), publikacja danych osobowych jest niezbędna do zaprezentowania ustaleń uzyskanych w wyniku badań lub do ułatwienia badań w takim zakresie, w jakim interesy lub podstawowe prawa i wolności podmiotu danych nie mają charakteru nadrzędnego (lit. b)) lub osoba, której dane dotyczą podała dane do wiadomości publicznej (lit. c)).

Proponuje się akty delegowane w celu doprecyzowania kryteriów i wymogów dotyczących przetwarzania danych osobowych do celów dokumentacji, statystyki i badań naukowych, jeżeli spełnia ono kryteria i wymogi zawarte w ust. 1 i 2.

Kryteria określone w artykule są już stosunkowo jasne, ponieważ stanowią, iż dane można przetwarzać do celów dokumentacji, statystyki i badań naukowych, wyłącznie jeśli takie przetwarzanie spełnia dwa wymienione warunki. We wszystkich innych przypadkach jest to zabronione. Kryteria te są zasadniczymi elementami przy ustalaniu zgodności z prawem przetwarzania.

Jeżeli spełnienie dodatkowych kryteriów jest konieczne, aby móc przetwarzać dane do celów dokumentacji, statystyki i badań naukowych, wymogi te należy zawrzeć w treści samego rozporządzenia w celu zapewnienia zharmonizowanej praktyki oraz przejrzystości i pewności prawa dla wszystkich zainteresowanych stron.

Jeżeli chodzi o proponowane akty delegowane mające na celu doprecyzowanie niezbędnych ograniczeń prawa do informacji i dostępu przysługującego podmiotowi danych oraz akty proponowane w celu doprecyzowania warunków praw podmiotów danych w tych okolicznościach i gwarancji tych praw, nie jest jasne, gdzie przewidziano możliwość ograniczenia tych praw (nie przewidziano tego w art. 14 ani w art. 15). Ponieważ jednak jest to zasadniczy element, należy go zawrzeć w treści samego rozporządzenia.

Jeżeli istnieje możliwość, aby organy prowadzące badania do celów dokumentacji, statystyki i badań naukowych ograniczały prawa podmiotów danych, należy uwzględnić tę kwestię w prawnie wiążącym dokumencie w celu zapewnienia przejrzystości i pewności dla podmiotów danych.

Należy zatem albo w pełni uwzględnić tę kwestię w treści samego rozporządzenia, albo doprecyzować ją w akcie delegowanym, który zostanie przyjęty wraz z wejściem rozporządzenia w życie.

W stosownych przypadkach dalsze wytyczne mogłaby przedstawić EDOR lub można by było je ustanowić w ogólnoeuropejskim kodeksie postępowania.