Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Warszawa, dn. 26.01.2017 r.

Uwagi Stowarzyszenia Administratorów Bezpieczeństwa Informacji (SABI) do dokumentu Grupy Roboczej art. 29 Dyrektywy 95/46/WE (GR29), przyjętego w dniu 13 grudnia 2016. „Wytyczne dotyczące inspektorów ochrony danych" (WP243)

Stowarzyszenie Administratorów Bezpieczeństwa Informacji (SABI) ocenia jako niezmiernie ważne wytyczne dotyczące inspektorów ochrony danych przedstawione przez Grupę Roboczą art. 29 Dyrektywy 95/46/WE (GR29), ponieważ stanowią one ważny element zapewniania zgodności z zasadami ochrony danych osobowych w jednostkach organizacyjnych, w tym wdrażania samego ogólnego rozporządzenia o ochronie danych (RODO). Wytyczne z pewnością przyczynią się do lepszego stosowania przepisów RODO dotyczących inspektora ochrony danych (DPO) oraz wspomogą prawidłowe wyznaczanie DPO, ustalanie ich pozycji w organizacji i wykonywanie zadań.

Jednocześnie SABI zauważa, że wytyczne wymagają uzupełnienia o zagadnienia odnoszące się do DPO, które nie zostały poruszone lub zostały poruszone w niewystarczającym stopniu. Wyjaśnienia wymagają również niektóre stanowiska zawarte w wytycznych. Uwagi w tym zakresie przedstawiamy poniżej.

I. Wyznaczenie DPO przez organy publiczne i podmioty publiczne

Wątpliwości merytoryczne budzi wyodrębnienie w wytycznych w pkt 2.1.1 dwóch różnych grup podmiotów:

a) „organy i podmioty publiczne" wykonujące zadania realizowane w interesie publicznym oraz sprawujące władzę publiczną, które mają obowiązek wyznaczenia DPO;

b) inne organy i podmioty wykonujące zadania realizowane w interesie publicznym oraz sprawujące władzę publiczną, które nie mają obowiązku wyznaczania DPO, a tylko zaleca się, aby powoływały one DPO.

Zdaniem SABI wyodrębnienie drugiej kategorii podmiotów nie znajduje podstaw prawnych w RODO i jest niejasne w interpretacji, także na gruncie przepisów krajowych. Należy zwrócić uwagę, że obowiązek wyznaczenia DPO nałożono zarówno na organy publiczne, jak i podmioty publiczne. Gdy w RODO celem jest zawężenie przepisu tylko do organów publicznych, czyni się to wprost, jak w art. 4 pkt 9 RODO (wytłumaczenie jakie występują przykładowe organy publiczne znajduje się w motywie 31 preambuły RODO). Podmioty publiczne to odmienna kategoria od organów publicznych, i o tym jakie podmioty do niej zaliczyć decydują przesłanki „sprawowania władztwa publicznego" oraz „realizowania interesu publicznego", jak również podleganie „prawu publicznemu". Odpowiedź czy spełnione są wymienione przesłanki zależy od przepisów krajowych oraz szczególnych przepisów Unii Europejskiej. Jeżeli na gruncie tych przepisów zostanie uznane, że spełnione zostały przesłanki to istnieje podmiot publiczny w rozumieniu art. 37 ust.1 lit. a) RODO, który ma obowiązek wyznaczenia DPO. Natomiast nie występuje już podstawa do wyodrębniania dalszej kategorii podmiotów, które mimo wykonywania tych zadań i podlegania prawu publicznemu nie mają obowiązku wyznania DPO.

II. Wyznaczenie jednego DPO dla kilku podmiotów publicznych

1. W wytycznych nie określono jaki podmiot (lub podmioty) z grupy przedsiębiorców może wyznaczyć jednego DPO dla całej grupy. Do rozważenia pozostają przynajmniej dwie możliwości: DPO wyznacza „spółka matka"(parent company) lub DPO wyznacza każdy przedsiębiorca w tej grupie. W opinii SABI nawet jeżeli będzie przyjęte pierwsze ze stanowisk, to każdy z przedsiębiorców, u którego DPO będzie wykonywał funkcję musi to potwierdzić. Dopiero po takim potwierdzeniu nie będzie wątpliwości, że DPO może wykonywać zadania w przedsiębiorstwie potwierdzającym, jak również zwiększa to transparentność wykonywania funkcji DPO.
2. Podobny problem może zaistnieć w grupie organów lub podmiotów publicznych, tzn. czy każdy z nich musi wyznaczyć DPO, czy tylko ten organ (podmiot), który posiada pozycje nadrzędną względem innych organów (podmiotów) ze względu na zależności kierownictwa, nadzoru lub kontroli. Zdaniem SABI decyduje o tym prawo krajowe, które określa relacje między podmiotami (organami) publicznymi. Jednakże nawet w sytuacji ścisłych relacji nadrzędności w relacjach między podmiotami (np. jeden organ z mocy prawa kieruje pracą innego podmiotu) aktualne pozostaje stanowisko z pkt 1), że każdy podmiot, u którego DPO ma wykonywać zadania musi to potwierdzić. Aktualność także zachowuje uzasadnienie takiego stanowiska przedstawione w pkt 1.
3. W przypadku organów lub podmiotów publicznych nie wskazano jak rozumieć zwrot „kilka podmiotów" w kontekście pełnienia w nich funkcji przez jednego DPO, co może powodować

próby podawania konkretnej maksymalnej liczby podmiotów, u których można wyznaczać jednego DPO (np. nie wyższej niż 9). W ocenie SABI nie powinno się z góry wskazywać maksymalnej liczby organów lub podmiotów publicznych, ale ważne jest, że powinna to być na tyle niewielka liczba podmiotów, aby biorąc pod uwagę „strukturę organizacyjną i wielkość" możliwe było prawidłowe wykonywanie w nich zadań przez DPO. W konkretnych okolicznościach warunek ten może być spełniony także w sytuacji wyznaczenia jednego DPO dla więcej niż 9 organów (podmiotów).

III. Wyznaczenie zespołu DPO

Co prawda w punkcie 3.2 („Niezbędne zasoby") w części 3 „Pozycja DPO", a nie w części 2 („Wyznaczanie DPO") poruszono kwestię zespołu DPO, ale rozwinięcie jej ma podstawowe znaczenie dla samego wyznaczenia DPO oraz jego pozycji. Wątpliwości budzi, czy wszystkie osoby w tym zespole będą pełniły funkcję DPO, co wiąże się z tym, że jednej strony muszą one spełnić warunek kwalifikacji zawodowych, ale z drugiej powinny korzystać z gwarancji przewidzianej dla funkcji DPO (niezależność w wykonywaniu zadań, zakaz odwoływania lub karania, zakaz istnienia konfliktów interesów). Wątpliwości wzmacnia rozbieżność w traktowaniu w wytycznych „DPO wewnętrznego" oraz „DPO zewnętrznego" (spoza organizacji). W przypadku „DPO wewnętrznego" w wytycznych mowa jest o zespole DPO, tj. DPO i jego współpracownikach (staff) (czyli jest jeden DPO, a pozostałe osoby to jedynie jego współpracownicy), natomiast w sytuacji „DPO zewnętrznego" zespół pracowników może wykonywać zadania DPO, a jeden z nich staje się tylko osobą kontaktową do kontaktów z klientem.

Zdaniem SABI w przypadku jednostek organizacyjnych o dużym rozmiarze i strukturze organizacyjnej powinno być dopuszczone powoływanie zespołu więcej niż jednej osoby pełniącej zadania DPO, gdy zachodzi potrzeba takiego działania dla prawidłowej ochrony danych osobowych. Każdej z tych osób z zespołu powinny przysługiwać gwarancje przewidziane w RODO dla DPO (niezależność w wykonywaniu zadań, zakaz odwoływania lub karania, zakaz istnienia konfliktów interesów). Natomiast w żadnej z wykładni przepisów RODO nie powinno się różnicować sytuacji prawnej DPO wewnętrznego oraz DPO zewnętrznego. Dodatkowo w sytuacji wykonywania funkcji przez tylko jednego DPO należy zalecić, aby administrator danych przewidywał osobę zastępującą DPO na czas jego nieobecności spowodowanej np. urlopem czy chorobą, która spełnia warunek kwalifikacji zawodowych oraz korzysta z gwarancji przewidzianych dla DPO.

IV. Kwalifikacje zawodowe DPO

Zgodnie z art. 37 (5) RODO na kwalifikacje zawodowe składają się wiedza fachowa oraz umiejętności wypełniania zadań. Tymczasem w wytycznych nie wyjaśniono warunków dotyczących umiejętności. Zdaniem SABI należy w tym zakresie w szczególności uwzględnić umiejętności związane z kształtowaniem relacji z osobami trzecimi, tj. z podmiotami danych, które zwracają się do DPO realizując swoje prawa oraz z osobami w organizacji, w stosunku do których DPO prowadzi działania informacyjne. Natomiast gdy chodzi o wiedzę fachową warto położyć akcent na posiadanie jej w zakresie umożliwiającym zidentyfikowanie zagrożeń oraz ocenę ryzyka, które są związane z realizacją procesów przetwarzania danych osobowych.

V. Niezależność DPO

W pkt 3.3 wytycznych wyjaśnia się rozumienie gwarancji niezależności DPO na podstawie RODO. Według art. 38 (3) RODO administrator danych i przetwarzający zapewniają, aby DPO nie otrzymywał instrukcji dotyczących wykonywania zadań. Ponieważ jest to główny przepis gwarantujący niezależność DPO to zdaniem SABI należy uzupełnić wytyczne w zakresie jego rozumienia. Zgodnie ze standardami dotyczącymi innych zawodów i funkcji, niezależność w wykonywaniu działalności obejmuje niezależność umysłu oraz niezależność wizerunku. Wydany związku z tym zakaz wydawania instrukcji powinien być rozumiany w ten sposób, że niedozwolona jest jakakolwiek ingerencja, która narusza stan niezależności umysłu oraz niezależności wizerunku.

VI. Zadania DPO

Najdalej idące uwagi należy odnieść do pkt 4 (Zadania), ponieważ na pięć zadań wymienionych w art. 39 (1) RODO w wyjaśnieniach pomięto wyjaśnienie aż 3 z nich, tj.

- informowanie i doradzanie w sprawach obowiązków spoczywających na mocy rozporządzenia oraz innych przepisów o ochronie danych osobowych,
- współpraca z organem nadzorczym,
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami oraz w stosownych przypadkach prowadzenia konsultacji we wszystkich innych sprawach.

SABI postuluje uzupełnienie wytycznych w tym zakresie, ponieważ realizacja przez DPO zadań bezpośrednio wpływa na standard ochrony danych osobowych, a generalne przepisy RODO w tym względzie nie określają sposobu i trybu wykonywania zadań przez DPO, w tym form działania DPO. W przypadku Polski stanowi to daleko idącą zmianę w stosunku do obecnie obowiązujących przepisów o ochronie danych osobowych, w których nie tylko w ustawie o ochronie danych osobowych, ale także w wykonujących ustawę rozporządzeniach ministra cyfryzacji szczegółowo określono sposób i tryb wykonywania zadań przez administratora bezpieczeństwa informacji.

VII. Zadanie monitorowania zgodności z RODO

W pkt 4.1 znajdują się wyjaśnienia dotyczące zadania monitorowania przestrzegana RODO. Jednak w wytycznych niewystarczająco wyjaśnia się jakie działania może podjąć DPO w przypadku stwierdzenia naruszenia RODO lub potrzeby podwyższenia poziomu ochrony danych osobowych. Wytyczne wskazują, że DPO może „informować, doradzać i rekomendować określone działania". Jednak w przypadku informowania i doradzania stanowi to powtórzenie kompetencji określonych w art. 39 (1) lit. a) RODO, natomiast zalecenie dotyczące rekomendowania nie określa szczegółów tego działania.
Zdaniem SABI trzeba określić jakie działania DPO może podjąć w przypadku stwierdzenia w trakcie monitorowania potrzeby podwyższenia poziomu ochrony danych, czy naruszenia ochrony danych osobowych. Działania DPO mogą polegać na zidentyfikowaniu obszaru wymagającego poprawy oraz dookreśleniu czynności które jego zdaniem pozwolą zapewnić stan prawidłowy, wraz z ewentualnym harmonogramem tych czynności. W przypadku naruszenia ochrony danych działania DPO należy zestawić z obowiązkami administratora danych dotyczącymi zgłoszenia naruszenia do organu nadzorczego (art. 33 RODO) lub do osoby, której dane dotyczą (art. 34 RODO). W szczególności DPO może oceniać, czy doszło do naruszenia, czy zachodzi obowiązek informowania oraz jakie działania zaradcze mogą zostać podjęte.

VIII. Zadania inspektora w wiążących regułach korporacyjnych

W wytycznych nie odniesiono się także do zadania dotyczącego wiążących reguł korporacyjnych, określonego w art. 47 ust. 2 pkt h RODO (monitorowanie przestrzegania wiążących reguł korporacyjnych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz monitorowanie szkoleń i rozpatrywanie skarg). Należy zwrócić uwagę, że odmiennie niż w art. 39 (1) lit b) RODO monitoring odnosi się nie tylko do monitorowania przestrzegania określonych zasad, ale także monitorowania szkoleń i rozpatrywania skarg. Dlatego

zasadne jest, aby wyjaśnić na czym mają polegać i w jaki sposób mają być wykonywane zadania monitorowania w ramach wiążących reguł korporacyjnych oraz jak je odnieść do zadania monitoringu określonego w art. art. 39 (1) lit b) RODO.

IX. Zadania DPO związane z organem nadzorczym

W wytycznych w ogóle nie odniesiono się do relacji DPO oraz organu nadzorczego. W art. 39 (1) RODO określono dwa zadania dotyczące tych relacji (lit d i e) i w pierwszej kolejności określić należy na czym polega różnica między nimi. Zdaniem ABI użycie słowa „współpraca" oznacza, dwukierunkowość relacji, także w tym znaczeniu, że każda ze stron współpracy może osiągnąć w jej wyniku korzyści. Zadanie współpracy warto odnieść nie tylko do generalnych działań organu nadzorczego, ale także do konkretnych spraw prowadzonych przez organ nadzorczy. Działania organu nadzorczego nie powinny ograniczać się tylko do przedstawiania swoich stanowisk, ale mieć również interaktywny charakter (forum wymiany poglądów, formularze umożliwiające zadanie pytania przez DPO, bezpośrednie konsultacje). Z kolei rola punktu kontaktowego nie powinna doprowadzić do tego, że DPO będzie pozostawał w konflikcie interesów w związku z obowiązkiem lojalności wobec administratora danych (podmiotu przetwarzającego), czy też będzie zobowiązywany do ujawniania tajemnic administratora danych (podmiotu przetwarzającego). W tym zakresie w pełni zgadzamy się z argumentami podniesionymi w notatce („Results of the discusion") po Fablab workshop „*GDPR/from concepts to operational toolbox, DIY*", które odbyły się w Brukseli 26 lipca 2016 r.

X. Zadania punktu kontaktowego dla osób, których dane dotyczą

W wielu systemach prawnych w tym prawie polskim, nowym rozwiązaniem jest zapewnienie podmiotom danych możliwości kontaktowania się z DPO we wszystkich sprawach dotyczących przetwarzania ich danych osobowych oraz w wykonywaniem ich uprawnień określonych w RODO. Tym ważniejsze jest wyjaśnienie jakie konkretne obowiązki spoczywają na DPO w związku z tym rozwiązaniem oraz w jaki sposób DPO ma realizować te obwiązki. W opinii SABI istotne znaczenie może mieć podejście oparte na procedurach wewnętrznych, w których określony jest zakres czynności DPO oraz jego współdziałanie z innymi osobami i komórkami w organizacji. Ważnymi elementami, które należy wziąć pod uwagę w procedurze są: potrzeba wstępnej weryfikacji trafiających do DPO spraw (czy są to sprawy z zakresu ochrony danych osobowych), określenie roli DPO po otrzymaniu sprawy (czy jest jedynie punktem kontaktowych czy też uczestniczy merytorycznie w załatwieniu sprawy) oraz komu w organizacji i w jaki sposób przekazuje sprawę, jeśli

nie jest właściwy do jej samodzielnego załatwienia. Ważna jest też potrzeba odpowiedniego wsparcia DPO w realizacji jego zadania, szczególnie w okresie dużego zainteresowania ze strony podmiotów danych (czas reakcji na zapytanie).

XI. Zobowiązanie inspektora do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

W wytycznych nie odniesiono się do obowiązku zachowania tajemnicy lub poufności przez DPO. Taką tajemnicę przewiduje się w art. 38 (5) RODO, jednak w opinii SABI przepis ten wymaga dalszych wyjaśnień. Podstawowe pytanie dotyczy tego, czy przepis RODO tworzy samodzielny obowiązek tajemnicy (poufności), czy też stanowi on wyłącznie odesłanie do przepisów krajowych oraz prawa Unii Europejskiej, w zakresie tajemnic określonych w tamtych systemach prawnych. Jeżeli właściwe jest pierwsze podejście, wyjaśnienia wymagają dalsze kwestie: czym różnią się obowiązki tajemnicy i poufności, jakich informacji dotyczy obowiązek (wszystkich pozyskanych przez DPO czy tylko określonych), w jakim zakresie i wobec kogo następuje wyłączenie obowiązku DPO. Natomiast w przypadku gdyby przepis art. 38 (5) RODO stanowił jedynie odesłanie do innych przepisów (krajowych oraz Unii Europejskiej) to nie tworzy się w nim żadnego nowego obowiązku tajemnicy (poufności), ponad te, które i tak wymagane są wobec DPO w przepisach krajowych oraz w przepisach Unii Europejskiej.

Zarząd Stowarzyszenia Administratorów
Bezpieczeństwa Informacji