Czy oficer compliance może być inspektorem ochrony danych?

Analiza praktyczna dokonana w świetle nowego unijnego prawa o ochronie danych osobowych

Przyjęte w maju 2016 roku ogólne rozporządzenie w sprawie ochrony danych osobowych (RODO) daje przedsiębiorcom możliwość powołania Inspektora Ochrony Danych (DPO). Na pierwszy rzut oka zmiana ta nie stanowi istotnej różnicy względem obecnie obowiązujących przepisów dotyczących Administratorów Bezpieczeństwa Informacji (ABI). Biorąc pod uwagę, że wielu compliance oficerów odpowiada w swoich organizacjach za kwestie związane z ochroną danych osobowych, niejednokrotnie także pełniąc funkcję ABI, postaramy się odpowiedzieć na pytanie, czy po wejściu w życie przepisów RODO takie rozwiązanie będzie w dalszym ciągu możliwe, a przede wszystkim, bezpieczne.

Kim jest i kto musi powołać Administratora Bezpieczeństwa Informacji?

Funkcja ABI pojawiła się w polskich przepisach dotyczących ochrony danych osobowych już w 2004 roku, jednak dopiero od momentu wprowadzenia szczegółowej regulacji w 2015 roku funkcja ta zaczęła być częściej spotykana w polskich przedsiębiorstwach.

Zgodnie z art. 36a ustawy o ochronie danych osobowych powołanie ABI ma obecnie charakter fakultatywny. Do głównych zadań ABI należy m.in. prowadzenie regularnych audytów zgodności przetwarzania danych z wymogami ustawowymi oraz prowadzenie dokumentacji przetwarzania danych osobowych. Przepisy ustawy o ochronie danych osobowych wprowadzają także podstawowe gwarancje niezależności ABI, takie jak: bezpośrednia podległość administratorowi danych, konieczność zapewnienia przez administratora środków umożliwiających niezależne wykonywanie zadań przez ABI oraz – co najważniejsze – zakaz powierzania ABI innych obowiązków, które mogłyby negatywnie odbić się na możliwościach wykonywania zadań z zakresu ochrony danych osobowych.
W praktyce, szczególnie ostatni z wymogów dotyczących pozycji ABI był sporadycznie egzekwowany przez GIODO. W efekcie, w wielu organizacjach funkcja ABI stanowi dodatek do innych obowiązków (np. compliance officera lub kierownika IT), które wykonuje osoba odpowiedzialna za kwestie związane z bezpieczeństwem danych.

Kim jest i kto musi powołać Inspektora Ochrony Danych?

W myśl przepisów RODO Inspektor Ochrony Danych (DPO) może zostać wyznaczony w każdej organizacji. Istotną nowością względem obecnego stanu prawnego jest nałożenie obowiązku powołania DPO w organizacji na niektóre kategorie administratorów i podmiotów przetwarzających. Zgodnie z art. 37 ust. 1 RODO powołanie DPO będzie więc obowiązkowe zawsze:

- w organach i podmiotach publicznych, które przetwarzają dane osobowe (z wyłączeniem sądów w zakresie sprawowania wymiaru sprawiedliwości);
- gdy główna działalność administratora lub podmiotu przetwarzającego polega na prowadzonych na dużą skalę operacjach przetwarzania danych osobowych, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą;
- gdy główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę danych wrażliwych lub danych dotyczących wyroków skazujących i naruszeń prawa.

Kiedy trzeba powołać DPO?

Jak wskazuje Grupa Robocza Art. 29 w przyjętym w połowie grudnia 2016 r. stanowisku, które precyzuje rozumienie przepisów RODO dotyczących osób pełniących funkcję DPO , o ile nie jest oczywistym, że organizacja nie spełnia żadnego z powyższych kryteriów, pożądane jest, aby proces decyzyjny prowadzący do rozstrzygnięcia o konieczności (lub jej braku) powołania DPO był udokumentowany. Co więcej, zarchiwizowana dokumentacja powinna pozwolić na ustalenie, że w procesie decyzyjnym właściwie przeanalizowano i uwzględniono wszystkie przesłanki związane z koniecznością wyznaczenia DPO.

Z punktu widzenia przedsiębiorstw, które stoją przed dylematem wyznaczenia DPO, najistotniejsze będzie więc ustalenie znaczenia trzech przesłanek: (i) głównej działalności, (ii) przetwarzania danych na dużą skalę oraz (iii) regularnego i systematycznego monitorowania osób, których dane dotyczą.

Czym jest główna działalność administratora według RODO?

Pojęcie „głównej działalności" administratora zostało zdefiniowane zarówno w RODO, jak w stanowisku Grupy Roboczej Art. 29. Jak wskazuje Grupa Robocza Art. 29 pojęcie to będzie rozumiane stosunkowo szeroko i obejmie także takie rodzaje działalności gospodarczej, w których operacje przetwarzania danych osobowych nie stanowią same w sobie głównego przedmiotu działalności organizacji, ale jednocześnie świadczenie usług bez przetwarzania danych osobowych jest praktycznie niemożliwe. Przykładowo głównym przedmiotem działalności banku jest udzielanie kredytów i prowadzenie rachunków bankowych, jednak działalność ta byłaby niemożliwa bez gromadzenia i przetwarzania danych osobowych klientów. W efekcie, działalność banku klasyfikowana będzie jako polegająca na przetwarzaniu danych.

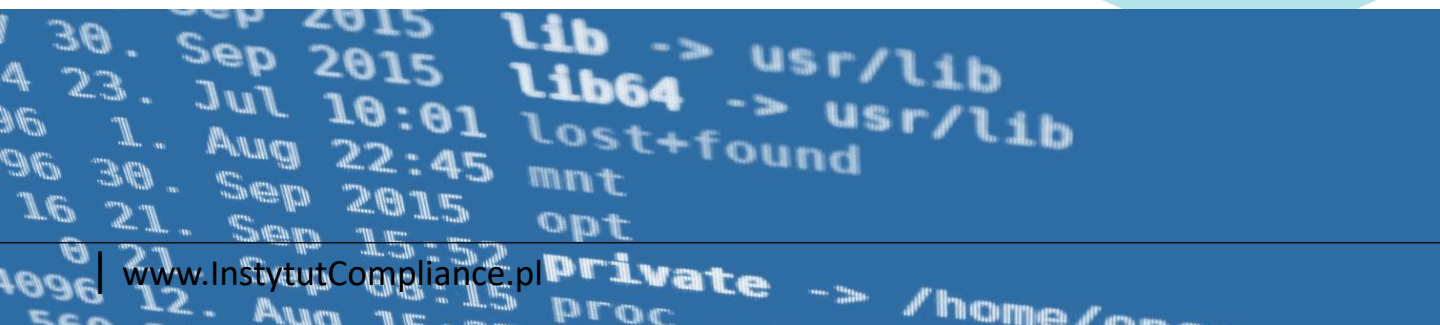
Kiedy dochodzi do przetwarzania danych osobowych na dużą skalę?

Wskazanie obiektywnych kryteriów, które pozwalałaby na określenie, kiedy przetwarzanie danych osobowych ma dużą skalę, jest trudne. Zdaniem Grupy Roboczej Art. 29, pewne standardy w tym zakresie mogą pojawić się w przyszłości, w miarę rozwoju praktyki stosowania przepisów RODO. Wśród kryteriów, które mogą być pomocne przy ustalaniu skali przetwarzania danych w tym momencie, Grupa Robocza Art. 29 wymienia jednak:

- zakres geograficzny operacji przetwarzania danych osobowych;
- okres, przez jaki przetwarzane będą dane osobowe;
- zakres przetwarzanych danych osobowych;
- ilość osób, których dane są przetwarzane.

W naszej ocenie, organizacje, które z pewnością będzie można zaklasyfikować do grupy przetwarzających dane na dużą skalę, to m. in. banki, instytucje finansowe i ubezpieczeniowe, szpitale, dostawcy usług telekomunikacyjnych i internetowych, firmy farmaceutyczne oraz dostawcy usług powszechnych i komunalnych (np. dystrybutorzy gazu, wody, etc.).

Czytaj dalej...



Kiedy działalność administratora wymagać będzie monitorowania osób, których dane dotyczą?

Kolejną z przesłanek wyznaczenia DPO w organizacji jest prowadzenie przez administratora działalności, która ze względu na swój zakres, charakter lub cele wymaga regularnego i systematycznego monitorowania osób, których dane dotyczą. Zdaniem Grupy Roboczej Art. 29 do przykładów takich działań zalicza się m.in. działania związane z profilowaniem i monitorowaniem zachowań użytkowników w Internecie oraz – co szczególnie istotne z punktu widzenia compliance – czynności związane z profilowaniem osób fizycznych w celu zapobiegania nadużyciom wewnętrznym i zapobieganiu praniu brudnych pieniędzy.

Zdaniem Grupy Roboczej Art. 29 powyższe działania będą miały regularny charakter zawsze wtedy gdy:

- odbywają się w określonym z góry przedziale czasu;
- są powtarzane lub ponawiane w ustalonych z góry okresach;
- mają charakter ciągły albo długookresowy.

O systematycznym monitorowaniu będzie można z kolei mówić w sytuacji, gdy działania te odbywają się (i) w ustalony z góry, systemowy sposób; (ii) według określonej metodologii lub organizacji; (iii) w ramach szerokiego planu działań dotyczących zbierania danych osobowych; (iv) jako element strategii biznesowej przedsiębiorstwa.

Jaka jest pozycja DPO w organizacji?

Inspektor Ochrony Danych musi być właściwie i niezwłocznie angażowany we wszystkie sprawy dotyczące ochrony danych . Oznacza to, że powinien on uczestniczyć we wszystkich pracach, które mogą wpływać na kształt operacji związanych z przetwarzaniem danych osobowych w organizacji. Szczególną rolę DPO w procesie przetwarzania danych podkreśla art. 35 ust. 2 RODO, który nakłada na administratora danych obowiązek konsultowania się z DPO w ramach procesu prowadzenia oceny ryzyka dla przetwarzanych danych. Wśród praktycznych rekomendacji związanych z zapewnieniem właściwego włączenia DPO w procesy biznesowe, Grupa Robocza Art. 29 wymienia m. in. udział DPO w spotkaniach kadry zarządzającej oraz włączenie DPO w działania związane z usuwaniem skutków naruszeń bezpieczeństwa. Pożądane jest także precyzyjne wskazanie w ramach dokumentacji wewnętrznej przedsiębiorstwa innych działań, w których DPO powinien być konsultowany.

Konieczne zasoby i niezależność

DPO musi posiadać zasoby niezbędne do wykonywania powierzonych mu zadań, dostęp do danych osobowych gromadzonych w organizacji oraz zasoby, które pozwolą na utrzymanie właściwego poziomu wiedzy fachowej. Pojęcie właściwych zasobów jest rozumiane także jako konieczność utrzymania właściwego podziału obowiązków między zadania związane z ochroną danych osobowych oraz inne powierzone DPO zadania.

Ponadto, Inspektor Ochrony Danych nie może być związany otrzymywanymi instrukcjami, nie może być odwoływany ani karany za wypełnianie swoich zadań (chodzi o sytuację, gdy ocena dokonana przez DPO nie jest zbieżna z planami biznesowymi organizacji) oraz musi podlegać bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego.

W swojej opinii, Grupa Robocza Art. 29 zwraca także uwagę na konieczność dogłębnej znajomości przepisów RODO przez DPO oraz znajomość specyfiki sektora, w jakim działa zatrudniające go przedsiębiorstwo. Oczekiwania wobec fachowości Inspektora będą tym większe, im wyższe są ryzyka związane z procesami przetwarzania danych osobowych zachodzącymi w organizacji.

DPO a oficer compliance

Mając na uwadze powyższe, wysokie wymogi stawiane wobec osoby pełniącej funkcję DPO, wydaje się, że pogodzenie roli DPO i oficera compliance będzie bardzo trudne. Z jednej strony, przepisy RODO nie zabraniają łączenia funkcji DPO z innymi obowiązkami zawodowymi. Co więcej, wobec przerzucenia ciężaru prowadzenia oceny ryzyka związanego z operacjami przetwarzania danych osobowych na przedsiębiorców, oficer compliance, jako osoba posiadająca praktyczne doświadczenie w identyfikowaniu obszarów ryzyka i jego minimalizowaniu, stanowić może naturalnego kandydata do pełnienia tej funkcji. Z drugiej strony, duża ilość obowiązków nałożonych na przedsiębiorców przepisami RODO w połączeniu z koniecznością aktywnego uczestnictwa DPO w planowaniu działań biznesowych, będzie wymuszać konieczność ciągłego wyboru między konfliktującymi obowiązkami. W dłuższej perspektywie prowadzić może to do obniżenia skuteczności działań albo w zakresie ochrony danych osobowych, albo w zakresie compliance. Problem ten będzie szczególnie widoczny w dużych organizacjach.

Co dalej?

W naszej ocenie, początek 2017 roku to ostatni dzwonek do rozpoczęcia procesu dostosowywania działalności organizacji do wymogów RODO, a sygnał w tym zakresie z pewnością może (i powinien) wyjść od compliance officerów. Należy mieć jednak świadomość, że podjęcie decyzji co do wyznaczenia DPO oraz dokonanie ewentualnego podziału kompetencji w zakresie ochrony danych pomiędzy DPO a compliance officera to tylko jedno z wielu działań, które trzeba podjąć na podstawie przepisów RODO. Punktem wyjścia do wszelkich aktywności musi być staranna identyfikacja procesów, w których dochodzi do przetwarzania danych osobowych oraz kompleksowa ocena ryzyk z nimi związanych. Nawet jeżeli ochrona danych osobowych przestaje powoli być zadaniem dla compliance officerów, to ich zaangażowanie oraz pomoc we właściwej identyfikacji i ocenie źródeł ryzyka są niezbędne.

dr Anna Partyka-Opiela
Senior Associate, Domański Zakrzewski Palinka sp. k.

Jędrzej Stępniowski
Associate, Domański Zakrzewski Palinka sp. k.

Blog ekspercki | DZP Compliance Blog

O skutecznych systemach compliance i przeciwdziałaniu korupcji pisze Zespół Compliance kancelarii DZP

- Piszemy o nowych regulacjach i dobrych praktykach w zakresie systemów compliance.
- Prezentujemy rozwiązania przeciwdziałania korupcji, zarówno w sektorze publicznym jak i prywatnym, stosowane w Polsce i za granicą.
- Informujemy o ciekawych wydarzeniach i inicjatywach związanych z compliance.

DZP
więcej niż prawo

Odwiedź nas na
https://blog.dzp.pl/compliance