Które i jakie organizacje będą zobowiązane do wyznaczenia inspektora ochrony danych (IOD/DPO)

Prowadzi: **Piotr Glen**

Ekspert ds. ochrony danych osobowych

Administrator bezpieczeństwa informacji

INFORAKADEMIA

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r.

w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE

(ogólne rozporządzenie o ochronie danych)

(dalej RODO)

Gotowość na 25 maja 2018 roku

INFORAKADEMIA

Uodo:

Administrator danych może powołać administratora bezpieczeństwa informacji. W przypadku niepowołania administratora bezpieczeństwa informacji zadania ABI (określone w ustawie) wykonuje administrator danych (uodo art. 36a)

RODO:

Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy: …… (RODO art. 37)

W przypadkach innych można wyznaczyć lub jeżeli wymaga tego prawo Unii lub prawo państwa członkowskiego, wyznacza się inspektora ochrony danych.

INFORAKADEMIA

Wyznaczenie inspektora ochrony danych art. 37 ogólnego rozporządzenia o ochronie danych - RODO

1. Administrator i podmiot przetwarzający wyznaczają inspektora ochrony danych, zawsze gdy:

a) przetwarzania dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;

b) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;

c) główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych.

INFORAKADEMIA

Jak wskazuje projekt nowej ustawy o ochronie danych osobowych (wersja z 3 marca 2018 r.), przez organy i podmioty publiczne zobowiązane do wyznaczenia inspektora ochrony danych rozumiane będą organy oraz podmioty publiczne wskazane w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych oraz instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych. Jeśli przepis w takim brzmieniu zostanie uchwalony, to obowiązek wyznaczenia inspektora ochrony danych, będą miały, m.in:

- organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały,
- jednostki samorządu terytorialnego oraz ich związki,
- samodzielne publiczne zakłady opieki zdrowotnej,
- uczelnie publiczne,
- instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych.

Grupa przedsiębiorstw może wyznaczyć jednego inspektora ochrony danych, o ile można będzie łatwo nawiązać z nim kontakt z każdej jednostki organizacyjnej.

Jeżeli administrator lub podmiot przetwarzający są organem lub podmiotem publicznym, dla kilku takich organów lub podmiotów można wyznaczyć – z uwzględnieniem ich struktury organizacyjnej i wielkości – jednego inspektora ochrony danych.

W przypadkach innych wyznaczenie inspektora jest fakultatywne, z wyjątkiem przypadków określonych w szczególnych przepisach prawa.

Inspektor ochrony danych jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań.

Inspektor ochrony danych może być członkiem personelu administratora lub podmiotu przetwarzającego lub wykonywać zadania na podstawie umowy o świadczenie usług.

Administrator lub podmiot przetwarzający publikują dane kontaktowe inspektora ochrony danych i zawiadamiają o nich organ nadzorczy.

Status inspektora ochrony danych

Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

Czyli np.:

- Udział Inspektora (DPO) w spotkaniach przedstawicieli wyższego i średniego szczebla organizacji;
- Uczestnictwo DPO przy podejmowaniu decyzji dotyczących przetwarzania danych osobowych. Niezbędne informacje powinny zostać udostępnione DPO odpowiednio wcześniej, umożliwiając DPO zajęcie stanowiska;
- Stanowisko DPO powinno być zawsze brane pod uwagę. GR Art. 29 zaleca, w ramach dobrych praktyk, dokumentowanie przypadków i powodów postępowania niezgodnego z zaleceniem DPO;
- W przypadku stwierdzenia naruszenia albo innego zdarzenia związanego z danymi osobowymi należy natychmiast skonsultować się z DPO.

Niezbędne zasoby

Artykuł 38(2) nakłada obowiązek wspierania „inspektora ochrony danych w wypełnianiu przez niego zadań[..], zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.”

Następujące aspekty powinny zostać wzięte pod uwagę:

- Wsparcie DPO ze strony kadry kierowniczej (np. na poziomie zarządu);
- Wymiar czasu umożliwiający DPO wykonywanie zadań;
- Odpowiednie wsparcie finansowe, infrastrukturalne (pomieszczenia, sprzęt, wyposażenie) i kadrowe, gdy to właściwe;
- Oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia DPO, tak aby wiedzieli o jego istnieniu oraz o pełnionych przez niego funkcjach
- Umożliwienie dostępu do innych działów organizacji, np. HR, działu prawnego, IT, ochrony etc., celem stworzenia przepływu informacji między tymi jednostkami a DPO i zapewnienia mu niezbędnego wsparcia;
- Ciągłe szkolenie;
- W zależności od rozmiaru i struktury organizacji przydatne może być powołanie zespołu inspektora ochrony danych (DPO i jego współpracowników).

Instrukcje i „wykonywanie zadań w sposób niezależny”

Administrator / podmiot przetwarzający mają w szczególności zapewnić „by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań.”

Oznacza to, że w ramach wypełniania zadań Inspektor nie może otrzymywać instrukcji dotyczących sposobu rozpoznania sprawy, środków jakie mają zostać podjęte czy celu jaki powinien zostać osiągnięty, czy też faktu, czy należy skontaktować się z organem nadzorczym. Nie może również zostać zobligowany do przyjęcia określonego stanowiska w sprawie z zakresu prawa ochrony danych, np. określonej wykładni przepisów.

W sytuacji podjęcia przez administratora lub podmiot przetwarzający decyzji niezgodnej z przepisami RODO i zaleceniami DPO, Inspektor powinien mieć możliwość jasnego przedstawienia swojego stanowiska osobom podejmującym decyzję.

Niezależność DPO nie oznacza jednak, iż DPO posiada uprawnienia decyzyjne wykraczające poza zadania z art. 39.

Odwołanie lub kara za wykonywanie zadań DPO

Artykuł 38(3) stanowi również, że DPO „nie jest odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań.”

Zgodnie z normalnymi regułami, przepisami karnymi i prawa pracy, jak w przypadku każdego innego pracownika, DPO może zostać odwołany w uzasadnionych sytuacjach z przyczyn innych niż wykonywanie obowiązków DPO (np. kradzież, nękanie fizyczne i psychiczne, molestowanie seksualne, ciężkie naruszenie obowiązków).

Konflikt interesów

Inspektor ochrony danych może wykonywać inne zadania i obowiązki. Administrator lub podmiot przetwarzający zapewniają, by takie zadania i obowiązki nie powodowały konfliktu interesów.

Jako regułę można uznać, że za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT (ASI)),

ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.

Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy rozporządzenia.

Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

Zadania inspektora ochrony danych art. 39 RODO

Monitorowanie zgodności z RODO

monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub krajowych o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

W ramach monitorowania DPO mogą między innymi:

- Zbierać informacje w celu identyfikacji procesów przetwarzania;
- Analizować i sprawdzać zgodność tego przetwarzania;
- Informować, doradzać i rekomendować określone działania administratorowi albo podmiotowi przetwarzającemu.

Monitorowanie nie oznacza odpowiedzialności DPO w przypadkach naruszenia RODO. Z rozporządzenia jasno wynika, iż to administrator, a nie DPO „wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać” (Artykuł 24(1)). Spełnianie wymogów rozporządzenia należy do obowiązków korporacyjnych administratora, a nie DPO.

Korzyści wynikające z wyznaczenia IOD

- Realizacja obowiązku prawnego – dla podmiotów zobowiązanych do wyznaczenia IOD;
- Uzyskanie przez administratora danych efektywnego wewnętrznego nadzoru nad prawidłową realizacją obowiązków wynikających z przepisów o ochronie danych osobowych.
- Zwiększenie autokontroli administratorów danych i podniesienie poziomu bezpieczeństwa danych osobowych.
- Wzmocnienie zaufania do administratorów danych ze strony osób, których dane dotyczą oraz innych administratorów danych, a także podmiotów współpracujących z administratorem danych.

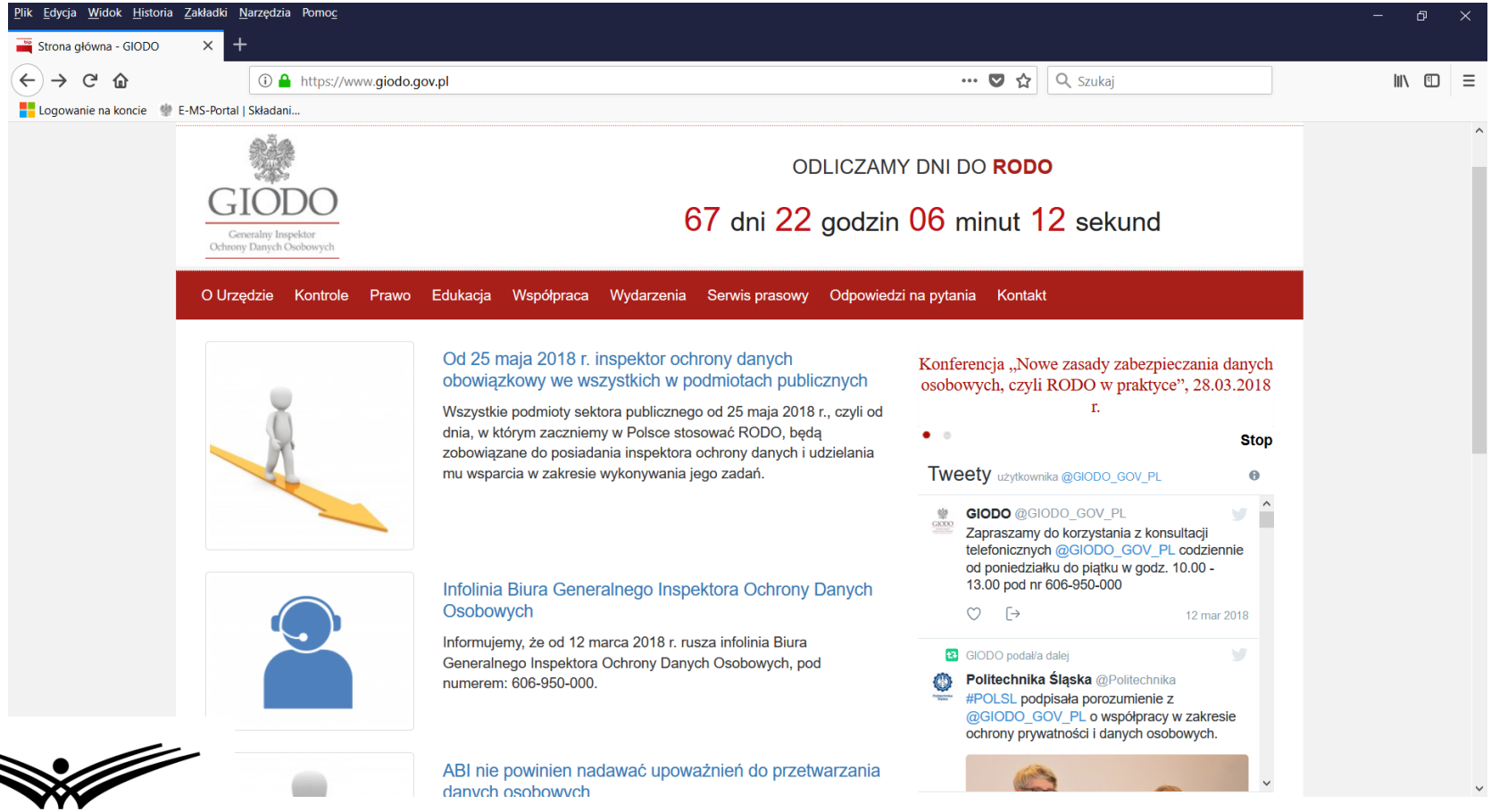
INFORAKADEMIA

Opinie, wytyczne, wskazówki

Poradnik dla Inspektorów Ochrony Danych

Wytyczne GR Ar. 29

http://www.giodo.gov.pl/ Reforma przepisów



INFORAKADEMIA