GIODO
Generalny Inspektor
Ochrony Danych Osobowych

"OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH I JEGO ROLA W JEDNOSTKACH ADMINISTRACJI PUBLICZNEJ”

MONIKA MŁOTKIEWICZ
DEPARTAMENT REJESTRACJI ADMINISTRATORÓW BEZPIECZEŃSTWA INFORMACJI I ZBIORÓW DANYCH OSOBOWYCH
BIURO GIODO

DLACZEGO RODO WZMACNIA ROLĘ I POZYCJĘ IOD?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- monitorowanie razem z organami nadzorczymi przestrzegania przepisów o ochronie danych osobowych

- zapewnienie fachowego wsparcia administratorom i podmiotom przetwarzającym wobec nowych wyzwań i stanu prawnego opartego na zasadzie rozliczalności

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

- RODO przyznaje inspektorom ochrony danych nową, dużo istotniejszą rolę niż ta, jaką przewidywała dla nich Dyrektywa 95/46/WE i wdrażające ją ustawy krajowe.

- RODO ujednolica terminologię, kryteria powołania, status i zadania inspektorów ochrony danych we wszystkich PC UE.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Administrator Bezpieczeństwa Danych Osobowych (ABI)

Inspektor Ochrony Danych (DPO)

Znowelizowane przepisy UODO w zakresie dotyczącym ABI są bardzo zbliżone do rozwiązań przyjętych w RODO

JAKIE ZMIANY W ZAKRESIE ABI/IOD PRZEWIDUJE RODO?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. obowiązek wyznaczenia inspektora dla wszystkich podmiotów publicznych
2. więcej gwarancji niezależności oraz konkretne formy wsparcia ze strony organizacji

WYZNACZENIE IOD

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Obowiązek dotyczy:

wszystkich organów i podmiotów publicznych,
z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości

Art. 37 ust 1 lit. a RODO

ORGAN LUB PODMIOT PUBLICZNY

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Wobec braku w RODO definicji pojęcia „organu lub podmiotu publicznego” użytego w art. 37 ust 1 lit a pojęcie to powinno zostać określone na poziomie przepisów krajowych.

PROJEKT USTAWY O OCHRONIE DANYCH OSOBOWYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 10. Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora, o których mowa wart. 37 ust. l lit. a rozporządzenia 2016/679, rozumie się:

1) jednostki sektora finansów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych;

2) instytuty badawcze, o których mowa w ustawie z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2017 r. poz. 1158 oraz 1452 i 2201);

3) Narodowy Bank Polski.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

- 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,
- inne państwowe lub samorządowe osoby prawne utworzone na podstawie odrębnych ustaw w celu wykonywania zadań publicznych, z wyłączeniem przedsiębiorstw, instytutów badawczych, banków i spółek prawa handlowego,
- instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Dlaczego obowiązek wyznaczenia IOD mają wszystkie podmioty i organy publiczne?

W przypadku przetwarzania danych przez te podmioty możliwość wpływu osób,, których dane dotyczą na charakter tego przetwarzania może być ograniczona bądź wyłączona, co może wymagać dodatkowej ochrony, jaką daje powołanie IOD

KWALIFIKACJE DO PEŁNIENIA FUNKCJI -KRYTERIA WYBORU ODPOWIEDNIEGO IOD

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- **Wiedza z zakresu** krajowych, europejskich oraz sektorowych **przepisów oraz praktyk** w zakresie ochrony danych osobowych oraz dogłębną znajomość RODO.

- Ponadto wiedza na temat:
  - **procesów przetwarzania**, **systemów informatycznych** oraz **zabezpieczeń** stosowanych u administratora,
  - **sektora**, w którym działa administrator,
  - **procedur administracyjnych i funkcjonowania jednostki.**

- **Umiejętności** wykonywania zadań określonych w art. 39 RODO

NIEZALEŻNOŚĆ IOD

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Inspektorzy ochrony danych – bez względu na to, czy są pracownikami administratora czy też nie – powinni być w stanie wykonywać swoje obowiązki i zadania w sposób **niezależny.** (motyw 97 RODO)

WIĘCEJ GWARANCJI NIEZALEŻNOŚCI IOD ORAZ KONKRETNE FORMY WSPARCIA ZE STRONY ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- **zakomunikowanie** wszystkim w organizacji, kto pełni funkcję IOD i **co należy do jego zadań i uprawnień**

- umiejscowienie IOD w strukturze organizacyjnej jako **bezpośrednio podległego najwyższemu kierownictwu**

WIĘCEJ GWARANCJI NIEZALEŻNOŚCI IOD ORAZ KONKRETNE FORMY WSPARCIA ZE STRONY ADO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- zapewnienie **udziału** IOD **we wszystkich zagadnieniach** związanych z ochroną danych osobowych (art. 38 ust. 1 rodo) od **najwcześniejszego etapu**
- zapewnienie, aby IOD, **nie otrzymywał instrukcji dotyczących wykonywania zadań** (art. 38 ust 3 RODO)
- zapewnienie IOD **możliwości niezależnego przedstawienia swojego stanowiska i kontaktu z organem nadzorczym.**

DO OBOWIĄZKÓW ADMINISTRATORÓW DANYCH NALEŻY ZAPEWNIENIE, ABY INSPEKTOR OCHRONY DANYCH:

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- **zakaz odwołania lub ukarania IOD** za wypełnianie przez niego jego zadań (art. 38 ust. 3 RODO),

- **zakaz otrzymywania innych zadań i obowiązków,** jeśli mogłyby one spowodować konflikt interesów (art. 38 ust. 6 RODO)

- **obowiązek wspierania** inspektora ochrony danych w wypełnianiu przez niego zadań, m.in. poprzez **zapewnienie mu zasobów niezbędnych do wykonywania zadań oraz utrzymania fachowej wiedzy.**

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Nowe wymagania wobec funkcji IOD zmuszają do dokonania oceny:

- czy osoba, która ma pełnić tą funkcję spełnia kryteria z RODO (wiedza, umiejętności, pozycja w strukturze organizacyjnej, konflikt interesów)

- jakie w związku z wyznaczeniem tej osoby obowiązki ma administrator i w jaki sposób zostaną one spełnione

KTO PONOSI ODPOWIEDZIALNOŚĆ ZA ZAPEWNIENIE ZGODNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH Z PRAWEM?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zgodność z przepisami dotyczącymi ochrony danych jest obowiązkiem administratora lub podmiotu przetwarzającego.

To **administrator lub podmiot przetwarzający musi zapewnić i móc wykazać**, że przetwarzanie jest wykonywane zgodnie z RODO.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art 83 ust. 4 RODO - **naruszenia obowiązków administratorów i podmiotów przetwarzających, o których mowa w art. 37–39 RODO** podlega karze w wysokości 10 mln EUR a w przypadku przedsiębiorstwa - w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

Obowiązki w zakresie:

- wyznaczenia IOD
- gwarancji jego niezależności
- udzielania IOD wsparcia
- zapewnienia prawidłowego wykonania zadań IOD

ZADANIA DPO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. **INFORMOWANIE I DORADZANIE** W ZAKRESIE OBOWIĄZKÓW CIĄŻĄCYCH NA ADMINISTRATORZE, PODMIOCIE PRZETWARZAJĄCYM I PRACOWNIKACH
2. **MONITOROWANIE** PRZESTRZEGANIA PRZEPISÓW I POLITYK W DZIEDZINIE OCHRONY DANYCH OSOBOWYCH
3. **ZALECENIA I KONSULTACJE** CO DO OCENY SKUTKÓW DLA OCHRONY DANYCH I MONITOROWANIE JEJ WYKONANIA
4. **WSPÓŁPRACA** Z ORGANEM NADZORCZYM
5. PEŁNIENIE FUNKCJI **PUNKTU KONTAKTOWEGO** DLA ORGANU NADZORCZEGO (w tym uprzednie konsultacje z art. 36)
6. PEŁNIENIE FUNKCJI **PUNKTU KONTAKTOWEGO** DLA OSÓB, KTÓRYCH DANE DOTYCZĄ

Charakter zadań inspektora wskazuje, że osoba ta ma pełnić rolę:

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- **audytorską** wobec działań i decyzji administratorów danych i podmiotów przetwarzających dane (monitorowanie)

- **doradczą i edukacyjną (**informowanie, doradzanie, ułatwienie dokonania oceny skutków dla ochrony danych)

- p**ośrednika pomiędzy zainteresowanymi stronami** (między ADO a organem ochrony danych osobowych, między ADO a osobami, których dane dotyczą)

ART. 272. USTAWY O FINANSACH PUBLICZNYCH [POJĘCIE AUDYTU WEWNĘTRZNEGO]

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Audyt wewnętrzny jest działalnością **niezależną i obiektywną,** której celem jest **wspieranie ministra kierującego działem lub kierownika jednostki w realizacji celów i zadań** przez systematyczną **ocenę kontroli zarządczej oraz czynności doradcze**.

2. Ocena, o której mowa w ust. 1, dotyczy w szczególności adekwatności, **skuteczności i efektywności** kontroli zarządczej w dziale administracji rządowej lub jednostce.

ART. 68. [POJĘCIE I CELE KONTROLI ZARZĄDCZEJ]

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. **Kontrolę zarządczą** w jednostkach sektora finansów publicznych stanowi **ogół działań podejmowanych dla zapewnienia realizacji celów i zadań w sposób zgodny z prawem, efektywny,** oszczędny i terminowy.

2. Celem kontroli zarządczej jest zapewnienie w szczególności:

1) **zgodności działalności z przepisami prawa oraz procedurami wewnętrznymi**;

2) **skuteczności i efektywności** działania;

3) wiarygodności sprawozdań;

4) **ochrony zasobów**;

5) przestrzegania i promowania zasad etycznego postępowania;

6) **efektywności i skuteczności przepływu informacji;**

7) **zarządzania ryzykiem.**

ROZPORZĄDZENIE MF W SPRAWIE AUDYTU WEWNĘTRZNEGO ORAZ INFORMACJI O PRACY I WYNIKACH TEGO AUDYTU

GIODO
Generalny Inspektor Ochrony Danych Osobowych

§ 23. Audytor wewnętrzny **powstrzymuje się od wykonywania czynności doradczych, które prowadziłyby do przyjęcia przez niego obowiązków, odpowiedzialności lub uprawnień wchodzących w zakres zarządzania jednostką, i informuje o tym kierownika jednostki.**

WIELE PODMIOTÓW PUBLICZNYCH (KIEROWNICTWO)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- nie prowadziło dotychczas działań przygotowawczych do stosowania RODO
- dopiero teraz uświadamia sobie, że RODO nakłada na nie obowiązek wyznaczenia IOD
- identyfikuje problem deficytu wykwalifikowanych kadr w zakresie ochrony danych osobowych lub nieprawidłowości dotyczących funkcjonowania dotychczasowego ABI
- błędnie pojmuje istotę funkcji ABI/IOD

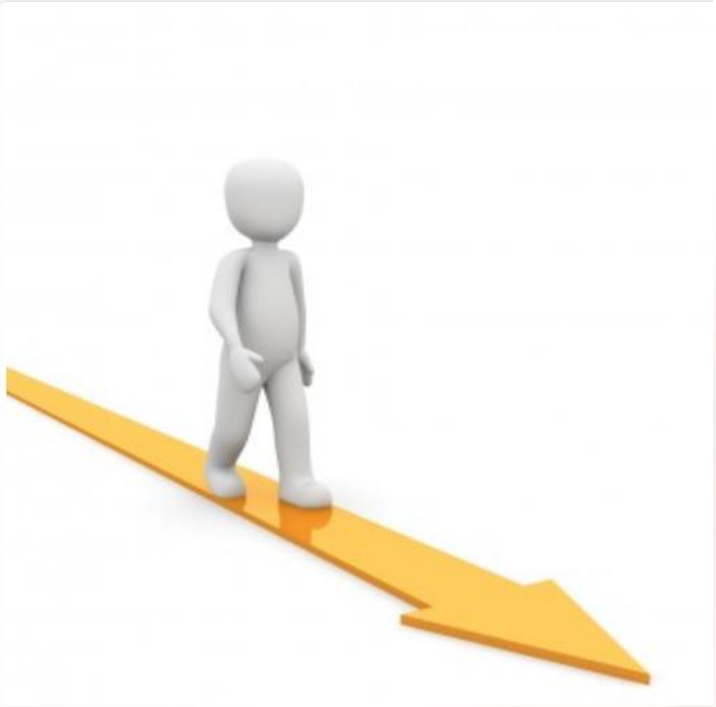
GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Od 25 maja 2018 r. inspektor ochrony danych obowiązkowy we wszystkich podmiotach publicznych

Metadane

Wszystkie podmioty sektora publicznego od 25 maja 2018 r., czyli od dnia, w którym zaczniemy w Polsce stosować RODO, będą zobowiązane do posiadania inspektora ochrony danych i udzielania mu wsparcia w zakresie wykonywania jego zadań.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 (ogólne rozporządzenie o ochronie danych - RODO) nakłada obowiązek wyznaczenia inspektora ochrony danych przez każdy organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości (art. 37 ust. 1 pkt a RODO). RODO wprowadziło w tym zakresie istotną zmianę. Wyznaczenie inspektora ochrony danych (obecnego ABI) w podmiotach sektora publicznego nie będzie, jak dotąd (na mocy ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych) uprawnieniem, lecz stanie się obowiązkiem wszystkich organów i podmiotów publicznych.



GIODO
Generalny Inspektor
Ochrony Danych Osobowych

ABI nie powinien nadawać upoważnień do przetwarzania danych osobowych

Metadane

Administrator danych nie powinien przyznawać administratorowi bezpieczeństwa informacji (czyli ABI, a na gruncie ogólnego rozporządzenia o ochronie danych - inspektorowi ochrony danych) uprawnień do nadawania w jego imieniu upoważnień do przetwarzania danych osobowych. Rolą ABI jest bowiem kontrolowanie działalności administratora pod kątem zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Generalny Inspektor Ochrony Danych Osobowych (GIODO), odpowiadając na sygnalizowane mu w tym zakresie wątpliwości, w wyjaśnieniach opublikowanych właśnie w ABI-informatorze (sekcja „Pytania i odpowiedzi", zakładka Zadania ABI) podkreśla jednocześnie, że sama procedura nadawania upoważnień oraz treść upoważnienia może być skonsultowana z powołanym administratorem bezpieczeństwa informacji, który jako specjalista z zakresu ochrony danych osobowych, powinien również i w tym zakresie doradzić administratorowi danych, a następnie

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

DZIĘKUJĘ ZA UWAGĘ