Urząd Ochrony Danych Osobowych

Rola i status inspektora ochrony danych w świetle przepisów wdrażających DYREKTYWĘ 2016/680

Monika Młotkiewicz
Dyrektor Zespołu Współpracy z Administratorami Danych
Urząd Ochrony Danych Osobowych

Warszawa, 12 lutego 2019 r.

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

Urząd Ochrony Danych Osobowych

Rola i status inspektora ochrony danych w świetle przepisów wdrażających DYREKTYWĘ 2016/680

Monika Młotkiewicz
Dyrektor Zespołu Współpracy z Administratorami Danych
Urząd Ochrony Danych Osobowych

Warszawa, 12 lutego 2019 r.

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

INSPEKTOR OCHRONY DANYCH
ROZPORZĄDZENIE 2016/679 I DYREKTYWA 2016/680

motyw 97 oraz art. 37-39 **rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych)**

motyw 63 i art. 32-33 **dyrektywy w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH ORAZ POWIADOMIENIA O WYZNACZENIU PREZESA UODO I OSÓB KÓRYCH DANE DOTYCZĄ (art. 46 i art. 98)

WARUNKI, JAKIE MUSI SPEŁNIAĆ IOD I WARUNKI, JAKIE ADMINISTRATOR MUSI ZAPEWNIĆ IOD, ŻEBY MÓGŁ ON PRAWIDŁOWO REALIZOWAĆ SWOJA FUNKCJĘ (ART. 46)

ZADANIA INSPEKTORA OCHRONY DANYCH (art. 47)

- Art. 47 ust 4 Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób realizacji zadań, o których mowa w ust. 1, uwzględniając konieczność **zapewnienia prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.**

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH

Art. 46. ust 1. Administrator wyznacza inspektora ochrony danych.

Ust 2. Inspektorem ochrony danych może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
2) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;
3) nie była skazana prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

Art. 4. Ilekroć w ustawie jest mowa o:

administratorze - rozumie się przez to właściwy organ, który samodzielnie lub wspólnie z innym właściwym organem lub właściwymi organami ustala cele i sposoby przetwarzania danych osobowych,

podmiot wskazany przez ustawę jako administrator, jeżeli cele i sposoby przetwarzania danych osobowych są określone w ustawie,

albo podmiot wskazany przez prawo Unii Europejskiej albo prawo państwa członkowskiego Unii Europejskiej lub podmiot wyznaczony zgodnie z kryteriami określonymi w prawie tego państwa;

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

KTO MA OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH
na podstawie ustawy z dnia 14 grudnia 2018 r.?

Policja
Straż Graniczna
Służba Więzienna
Żandarmeria Wojskowa
Służba Ochrony Państwa
Generalny Inspektor Informacji Finansowej
Krajowa Administracja Skarbowa
Sądy
Prokuratury
Straż gminna / miejska
Inspekcja Drogowa

Minister Środowiska
Główny Inspektorat Ochrony Środowiska
Straż Rybacka
Główny Inspektor Straży Leśnej
Państwowa Straż Łowiecka
Urząd Żeglugi Śródlądowej
urzędy morskie
Państwowa Inspekcja Sanitarna
Podmioty odpowiedzialne za bezpieczeństwo imprez masowych
Przewoźnicy lotniczy (dane PNR)

Urząd Ochrony Danych Osobowych

INSPEKTOR OCHRONY DANYCH
ROZPORZADZENIE 2016/679 – wyznaczenie IOD

Obowiązek wyznaczenia inspektora ochrony wynika z przepisów stosowanego od 25.05.2018 r. RODO

- **art. 37 ust. 1 RODO wprowadza obowiązek wyznaczenia IOD dla określonych kategorii administratorów i podmiotów przetwarzających.**

- **Obowiązek wyznaczenia IOD może wynikać również z prawa Unii lub prawa państwa członkowskiego.**

- **uprawnienie**

Wyznaczenie IOD rekomendowane jest też podmiotom, które nie mają takiego obowiązku
(wytyczne Grupy Roboczej art. 29 dotyczące inspektorów ochrony danych)

Urząd Ochrony Danych Osobowych

WYZNACZANIE IOD WEDŁUG RODO

Obowiązek wyznaczenia IOD posiadają:

- organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości

- podmiot prywatny – decyduje rodzaj głównej działalności podmiotu

Urząd Ochrony Danych Osobowych

JAK ROZUMIEĆ „Z WYJĄTKIEM SĄDÓW W ZAKRESIE SPRAWOWANIA PRZEZ NIE WYMIARU SPRAWIEDLIWOŚCI”?

Motyw 20
RODO ma zastosowanie do działań sądów i innych organów wymiaru sprawiedliwości

- przy czym prawo Unii lub prawo PC **może doprecyzować operacje i procedury** przetwarzania danych osobowych **przez sądy i inne organy wymiaru sprawiedliwości,**
- ponadto by **chronić niezawisłość sądów - nadzór nad przetwarzaniem danych** może być powierzony **specjalnym organom w systemie wymiaru sprawiedliwości PC.**

Oznacza to, że RODO nie zwalnia sądów z obowiązku wyznaczenia IOD, ale zakres działania IOD nie obejmuje tego, co mieści się w pojęciu sprawowania wymiaru sprawiedliwości (jako działalności zastrzeżonej jedynie dla sądów).

„Wymiar sprawiedliwości stanowi działalność państwa polegająca na sądzeniu, czyli wiążącym rozstrzyganiu sporów o prawo, w których przynajmniej jedną ze stron jest jednostka lub inny podmiot podobny” (wyrok TK z 1 grudnia 2008 r. P 54/07)

INSPEKTOR OCHRONY DANYCH
ROZPORZADZENIE 2016/679

Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych

Art. 9. **Przez organy i podmioty publiczne obowiązane do wyznaczenia inspektora**, o których mowa w art. 37 ust. 1 lit. a rozporządzenia 2016/679, rozumie się:

1) **jednostki sektora finansów publicznych;**

2) instytuty badawcze;

3) Narodowy Bank Polski.

Urząd Ochrony Danych Osobowych

Jednostki sektora finansów publicznych czyli:

Art. 9 ustawy o finansach publicznych

Sektor finansów publicznych tworzą:

1. **organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały;**

2. **jednostki samorządu terytorialnego oraz ich związki;**

3. **jednostki budżetowe;**

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

Wszystkie organy i podmioty publiczne podlegające ustawie z 14.12.18 miały już obowiązek wyznaczenia IOD na podstawie RODO

Policja
Straż Graniczna
Służba Więzienna
Żandarmeria Wojskowa
Służba Ochrony Państwa
Generalny Inspektor Informacji Finansowej
Krajowa Administracja Skarbowa
Sądy
Prokuratury
Straż gminna / miejska
Inspekcja Drogowa

Minister Środowiska
Główny Inspektorat Ochrony Środowiska
Straż Rybacka
Główny Inspektor Straży Leśnej
Państwowa Straż Łowiecka
Urząd Żeglugi Śródlądowej
urzędy morskie
Państwowa Inspekcja Sanitarna
Podmioty odpowiedzialne za bezpieczeństwo imprez masowych
Przewoźnicy lotniczy (dane PNR)

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH MÓGŁ DOTYCZYĆ PODLEGAJĄCYCH USTAWIE Z 14.12 2018 R. PODMIOTÓW PRYWATNYCH

Policja
Straż Graniczna
Służba Więzienna
Żandarmeria Wojskowa
Służba Ochrony Państwa
Generalny Inspektor Informacji Finansowej
Krajowa Administracja Skarbowa
Sądy
Prokuratury
Straż gminna / miejska
Inspekcja Drogowa

Minister Środowiska
Główny Inspektorat Ochrony Środowiska
Straż Rybacka
Główny Inspektor Straży Leśnej
Państwowa Straż Łowiecka
Urząd Żeglugi Śródlądowej
urzędy morskie
Państwowa Inspekcja Sanitarna
Podmioty odpowiedzialne za bezpieczeństwo imprez masowych
Przewoźnicy lotniczy (dane PNR)

OBOWIĄZEK WYZNACZENIA INSPEKTORA OCHRONY DANYCH WG RODO - PODMIOTY PRYWATNE

Obowiązek wyznaczenia IOD dotyczy:

b) podmiotów, których główna działalność polega na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;

c) podmiotów, których główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych lub danych dotyczących wyroków skazujących lub naruszeń prawa.

- **Podmioty odpowiedzialne za bezpieczeństwo imprez masowych**
- **Przewoźnicy lotniczy (dane PNR)**

Mogli ocenić, ze mają taki obowiązek lub wyznaczyć inspektora dobrowolnie.

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

Skoro organy publiczne i inne podmioty podlegające dyrektywie policyjnej miały od 25 maja tamtego roku obowiązek wyznaczenia inspektora na podstawie RODO, to:

- **Co z inspektorami ochrony danych pełniącymi dotychczas u nich swoje funkcje?**

- **Czy w związku z wejściem w życie ustawy z dnia 14 grudnia 2018 r. muszą one wyznaczyć nowego inspektora ochrony danych?**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R. DOTYCHCZASOWY IOD – TERMIN NA POWIADOMIENIE

Art. 98. 1. **Osoba pełniąca w dniu wejścia w życie** niniejszej **ustawy funkcję inspektora ochrony danych osobowych na podstawie** przepisów **ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. poz. 1000 i 1669), staje się inspektorem ochrony danych i pełni swoją funkcję** nie dłużej jednak niż 3 miesiące od dnia wejścia w życie niniejszej ustawy, **chyba że przed tym dniem administrator zawiadomi** Prezesa Urzędu Ochrony Danych Osobowych o **wyznaczeniu innej osoby** na inspektora ochrony danych, w sposób określony w art. 46.

2. Osoba, która stała się inspektorem ochrony danych na podstawie ust. 1, **pełni swoją funkcję także po upływie 3 miesięcy od dnia wejścia w życie niniejszej ustawy**, jeżeli do tego dnia administrator **zawiadomi** Prezesa Urzędu Ochrony Danych Osobowych o jej wyznaczeniu, w sposób określony w art. 46.

USTAWA Z DNIA 14 GRUDNIA 2018 R. DOTYCHCZASOWY IOD –TERMIN NA POWIADOMIENIE

Czyli:

IOD powołany na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, pełni swoją funkcję tylko do **6 maja 2019 r.**

Po tym dniu dotychczasowy IOD będzie kontynuował pełnienie swojej funkcji, jeżeli do 6 maja 2019 r. **administrator:**

- **prześle zawiadomienie o jego wyznaczeniu do pełnienia funkcji IOD na podstawie dyrektywy policyjnej (korzystając z odpowiedniego formularza).**
- nie wyznaczy na to stanowisko innej osoby (zawiadamiając o tym Prezesa UODO).

Dotychczasowy IOD musi też spełniać wymagania do pełnienia tej funkcji określone w ustawie z dnia 14 grudnia 2019 r.

USTAWA Z DNIA 14 GRUDNIA 2018 R.
WCZEŚNIEJSZY BRAK IOD – TERMIN NA WYZNACZENIE

Art. 98. ust. 3 **Administrator, który do dnia wejścia w życie niniejszej ustawy nie powołał inspektora ochrony danych osobowych na podstawie ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych, jest obowiązany do wyznaczenia inspektora ochrony danych i zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o jego wyznaczeniu, w terminie 1 miesiąca od dnia wejścia w życie niniejszej ustawy.**

Czyli administratorzy podlegający dyrektywie policyjnej, którzy do 6 lutego 2019 r. **nie wyznaczyli** inspektorów ochrony danych **mają czas** na **wyznaczenie takiej osoby i zawiadomienie Prezesa UODO do 6 marca 2019 r.**

- **może to dotyczyć np.** podmiotów odpowiedzialnych za bezpieczeństwo imprez masowych czy przewoźników lotniczych.

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
O OCHRONIE DANYCH OSOBOWYCH PRZETWARZANYCH W ZWIĄZKU Z ZAPOBIEGANIEM I ZWALCZANIEM PRZESTĘPCZOŚCI

- **Co z inspektorami ochrony danych pełniącymi dotychczas swoje funkcje u administratorów podlegających dyrektywie policyjnej?**
- **Czy w związku z wejściem w życie ustawy z dnia 14 grudnia 2018 r. konieczne jest wyznaczenie nowego inspektora ochrony danych?**

Inspektorzy, **jeżeli spełniają warunki** określone w ustawie z 14 grudnia 2018 r., powinni dalej pełnić swoją funkcję.

Konieczne jest zawiadomienie Prezesa UODO o wyznaczeniu IOD na podstawie ustawy z 14 grudnia 2018 r. do 6 maja 2019 r.

Podmioty, które **dotąd nie wyznaczyły IOD**, a podlegają ustawie z 14 grudnia 2018 r., muszą wyznaczyć IOD i zawiadomić Prezesa UODO o wyznaczeniu **do 6 marca 2019 r.**

USTAWA Z DNIA 14 GRUDNIA 2018 R.
TERMIN ZAWIADOMIENIA PO OKRESIE PRZEJŚCIOWYM

Poprzednie terminy dotyczyły podmiotów, które istniały w chwili wejścia ustawy z 14 grudnia 2019 r.

Podmioty, które powstaną po 6 marca 2019 r. mają na zawiadomienie Prezesa UODO 14 dni od momentu wyznaczenia IOD.

Art. 46 ust 9 Administrator zawiadamia Prezesa Urzędu o wyznaczeniu inspektora ochrony danych **w terminie 14 dni od dnia wyznaczenia**, wskazując imię, nazwisko, adres poczty elektronicznej lub numer telefonu inspektora ochrony danych.

Ten sam termin dotyczy przypadków zmiany danych lub odwołania IOD

Art. 46 ust. 10 Administrator zawiadamia Prezesa Urzędu o każdej zmianie danych, o których mowa w ust. 9, oraz o odwołaniu inspektora ochrony danych, w terminie **14 dni od dnia zaistnienia zmiany lub odwołania.**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
FORMA ZAWIADOMIENIA O WYZNACZENIU IOD

Art. 46 ust. 9 Administrator zawiadamia Prezesa Urzędu o wyznaczeniu inspektora ochrony danych w terminie 14 dni od dnia wyznaczenia, wskazując **imię, nazwisko, adres poczty elektronicznej lub numer telefonu IOD.** Zawiadomienie sporządza się **w postaci elektronicznej i opatruje kwalifikowanym podpisem elektronicznym albo podpisem zaufanym**. Zawiadomienie może zostać dokonane przez pełnomocnika. Do zawiadomienia dołącza się **pełnomocnictwo udzielone w formie elektronicznej.**

Formularze zawiadomień IOD - załatw online na biznes.gov.pl

Zawiadomienie na podstawie RODO

- Wyznaczenie nowego inspektora ochrony danych
- Zmiana danych kontaktowych dotychczasowego inspektora ochrony danych
- Odwołanie dotychczasowego inspektora ochrony danych
- Odwołanie dotychczasowego inspektora ochrony danych i wyznaczenie nowego

Zawiadomienie na podstawie DODO

Inspektor ochrony danych

- Wyznaczenie nowego inspektora ochrony danych
- Zmiana danych kontaktowych dotychczasowego inspektora ochrony danych
- Odwołanie dotychczasowego inspektora ochrony danych
- Odwołanie dotychczasowego inspektora ochrony danych i wyznaczeniu nowego

Zastępca inspektora ochrony danych

- Wyznaczenie nowego zastępcy inspektora ochrony danych
- Zmiana danych kontaktowych dotychczasowego zastępcy inspektora ochrony danych
- Odwołanie dotychczasowego zastępcy inspektora ochrony danych
- Odwołanie dotychczasowego zastępcy i wyznaczeniu nowego zastępcy inspektora ochrony danych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
ZAWIADOMIENIA O WYZNACZENIU IOD – POMOCNE WSKAZÓWKI

Administrator

- **W jaki sposób powiadomić Prezesa UODO o naruszeniu?**
- Obowiązki związane z naruszeniami ochrony danych osobowych
- Zgłaszanie naruszeń przez operatorów telekomunikacyjnych
- Analiza ryzyka
- Rejestr czynności przetwarzania
- Uprzednie konsultacje

Inspektor Ochrony Danych

- Wyznaczenie i status IOD
- Zawiadomienia Prezesa UODO związane z IOD
- Zadania IOD

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
ZAWIADOMIENIA O WYZNACZENIU IOD – POMOCNE WSKAZÓWKI

- Jak wysłać zawiadomienie dotyczące IOD przez ePUAP?
- Jak złożyć kwalifikowany podpis elektroniczny pod zawiadomieniem dotyczącym IOD?
- Dlaczego przy wgrywaniu podpisanego pliku xml otrzymuję komunikaty o błędach?
- Czy istnieje możliwość zawiadomienia o wyznaczeniu IOD przez pełnomocnika?
- Czy pełnomocnik ujawniony w CEIDG, może w imieniu tego podmiotu dokonać zawiadomienia?
- Jak podpisać jeden dokument przez więcej niż jedną osobę?
- Jak powinno wyglądać pełnomocnictwo dla osoby zgłaszającej IOD?
- W jakiej formie administrator/podmiot przetwarzający powinien udzielić pełnomocnictwa?
- Co należy rozumieć przez formę elektroniczną pełnomocnictwa?
- Jak skutecznie podpisać pełnomocnictwo w formie elektronicznej?
- Czy notariusz może uwierzytelnić elektronicznie pełnomocnictwo upoważniające do zawiadomienia?
- Czy od przesłanego pełnomocnictwa pobierana jest opłata skarbowa?
- Czy należy dołączyć do pełnomocnictwa potwierdzenie dokonania opłaty skarbowej?

USTAWA Z DNIA 14 GRUDNIA 2018 R.
POINFORMOWANIE O INSPEKTORZE OSÓB, KTÓRYCH DANE DOTYCZĄ

Art. 46 ust. 11. Administrator udostępnia dane inspektora ochrony danych, o których mowa w ust. 9, **niezwłocznie po jego wyznaczeniu**, **na swojej stronie internetowej,** a jeżeli nie prowadzi własnej strony internetowej, w sposób ogólnie dostępny w miejscu prowadzenia działalności.

Na stronie internetowej należy podać **imię, nazwisko, adres poczty elektronicznej lub numer telefonu IOD**

Rozdział 4

Prawa osoby, której dane dotyczą

Art. 22. [Obowiązki informacyjne ciążące na administratorze]

1. Administrator udostępnia informacje o:
   1) nazwie, siedzibie i danych kontaktowych administratora;
   2) w razie potrzeby danych kontaktowych inspektora ochrony danych;
   3) celu, do których mają posłużyć dane osobowe;
   4) prawie wniesienia do Prezesa Urzędu lub innego organu sprawującego nadzór

USTAWA Z DNIA 14 GRUDNIA 2018 R. WYZNACZENIE IOD - JAKI WARUNKI MUSI SPEŁNIAĆ OSOBA WYZNACZONA?

Art. 46 ust. 2
Inspektorem ochrony danych może być osoba, która:

1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;

2) posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;

3) nie była skazana prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

USTAWA Z DNIA 14 GRUDNIA 2018 R. WYZNACZENIE IOD - JAKI WARUNKI MUSI SPEŁNIAĆ OSOBA WYZNACZONA? – WIEDZA I UMIĘJĘTNOŚCI

… posiada odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań, o których mowa w art. 47 ust. 1;

Poziom wiedzy fachowej należy ustalać zwłaszcza **w świetle prowadzonych operacji przetwarzania danych** oraz **ochrony, której wymagają dane osobowe przetwarzane przez administratora (motyw 63 dyrektywy).**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R. WYZNACZENIE IOD - JAKI WARUNKI MUSI SPEŁNIAĆ OSOBA WYZNACZONA? – WIEDZA I UMIĘJĘTNOŚCI

Co to oznacza?

IOD wyznaczeni przez administratorów podlegających dyrektywie policyjnej powinny zatem posiadać wiedzę w zakresie ochrony, której wymagają dane osobowe przetwarzane w związku z zapobieganiem i zwalczaniem przestępczości.

Należy pamiętać tu o zasadzie, że prawo krajowe ma być tak dalece jak to tylko możliwe interpretowane w zgodzie z prawem Unii, w celu zapewnienia spójnego i efektywnego systemu ochrony danych osobowych, również na poziomie wewnętrznym administratorów.

Praktyki, procedury, sposoby zabezpieczeń wypracowane na podstawie RODO i ustawy o ochronie danych osobowych powinny być rozwijane i kontynuowane, bo przestrzeganie przepisów RODO i dyrektywy 2016/680 powinno prowadzić do stosowania jednego spójnego systemu.

USTAWA Z DNIA 14 GRUDNIA 2018 R.
MOŻLIWOŚĆ WYZNACZENIA OSOBY ZASTĘPUJĄCEJ IOD

Art. 46 ust. 4 Administrator, który wyznaczył inspektora, **może** wyznaczyć osobę zastępującą inspektora w czasie jego nieobecności, z uwzględnieniem kryteriów, o których mowa w ust. 2.

5. **W związku z wykonywaniem obowiązków inspektora w czasie jego nieobecności do osoby go zastępującej stosuje się odpowiednio przepisy dotyczące inspektora**.

6. Podmiot, który wyznaczył osobę zastępującą inspektora, **zawiadamia Prezesa Urzędu o jego wyznaczeniu w trybie określonym w ust. 10 oraz udostępnia jego dane zgodnie z ust. 11.**

USTAWA Z DNIA 14 GRUDNIA 2018 R.
MOŻLIWOŚĆ WYZNACZENIA OSOBY ZASTĘPUJĄCEJ IOD

Osoba zastępująca IOD:

- Musi **spełniać te same warunki co IOD** czyli:

1) pełna zdolność do czynności prawnych i korzystanie z pełni praw publicznych;
2) odpowiednie kwalifikacje zawodowe, w szczególności wiedzę fachową na temat prawa i praktyki w dziedzinie ochrony danych osobowych, oraz umiejętności niezbędne do wykonywania zadań,
3) brak skazania prawomocnym wyrokiem orzeczonym za przestępstwo lub przestępstwo skarbowe popełnione z winy umyślnej.

- **W czasie nieobecności IOD wykonuje jego zadania (określone w art. 47)**, w tym:

- **pełni funkcję punktu kontaktowego wobec Prezesa UODO**
- **pełni funkcję punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw**

- **Jej** dane w zakresie: **imię, nazwisko, adres poczty elektronicznej lub numer telefonu muszą być przekazane Prezesowi UODO** w formie elektronicznej **i**osobom, których dane dotyczą **na stronie internetowej administratora.**
- **Może wchodzić w skład zespołu IOD.**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
MOŻLIWOŚĆ WYZNACZENIA OSOBY ZASTĘPUJĄCEJ IOD

Wytyczne Gr. Roboczej art. 29 dot. inspektorów ochrony danych:

DPO, **przy pomocy zespołu jeśli to niezbędne, powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą** i **współpracy z właściwym organem nadzorczym.** Oznacza to również, że komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze i osoby, których dane dotyczą. **Dostępność DPO** (…) **jest fundamentalna** dla zapewnienia osobom, których dane dotyczą możliwości skontaktowania się z DPO.

Zgodnie z artykułem 37(3) jeden DPO może zostać **wyznaczony dla kilku organów lub podmiotów publicznych**, po uwzględnieniu ich struktury organizacyjnej i wielkości. Te same ustalenia mają zastosowanie do zasobów i komunikacji. Biorąc pod uwagę fakt, iż **DPO posiada wiele zadań, administrator albo podmiot przetwarzający musi mieć pewność, że jeden DPO, z zespołem jeśli jest to niezbędne,** pozytywnie wypełni swoje obowiązki pomimo wyznaczenia go dla kilku podmiotów i organów publicznych.

Urząd Ochrony Danych Osobowych

WYTYCZNE DOTYCZĄCE INSPEKTORÓW OCHRONY DANYCH ('DPO') PRZYJĘTE PRZEZ GRUPĘ ROBOCZĄ ART. 29. - mają zastosowanie również do dyrektywy 2016/680

[1] 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). RODO jest istotne dla EOG i będzie miało zastosowanie po jego uwzględnieniu w Porozumieniu EOG.

[2] Wyznaczenie DPO jest również obowiązkiem właściwych organów na podstawie artykułu 32 Dyrektywy 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającej decyzję ramową Rady 2008/977/WSiSW (Dz.Urz.UE L 119/89) i krajowych przepisów wykonawczych. Wytyczne tutaj przedstawione mają zastosowanie do RODO, jednak można również je odnieść od przepisów dyrektywy 2016/618.

[3] Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz. U. UE L 281, 23.11.1995, str. 31).

[4] http://ec.europa.eu/justice/data-protection/article-29/documentation/otherdocument/files/2015/20150617_appendix_core_issues_plenary_en.pdf

5

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
WYZNACZENIE IOD - **JEDEN INSPEKTOR DLA KILKU ORGANÓW**

Art. 46 ust 3. Administratorzy mogą wyznaczyć jednego inspektora ochrony danych **dla kilku właściwych organów**, **uwzględniając ich strukturę organizacyjną i wielkość.**

Podmioty takie - ze względu na realizowanie zadań publicznych w tym samym obszarze - mogą przyjmować podobne rozwiązania organizacyjne i korzystać z tych samych procedur.

Ale :
Konieczne jest uwzględnienie wielkości i sposobu organizacji tych podmiotów i dokonanie starannej analizy, czy wyznaczona osoba będzie w stanie prawidłowo wypełniać wszystkie swoje obowiązki wobec każdego administratora danych.

Ponadto trzeba pamiętać, że wiele z obowiązków inspektorów przewidzianych w RODO wymaga stałego zaangażowania na rzecz administratora, który inspektora wyznaczył oraz tzw. „efektywnej dostępności" inspektora dla osób z danej organizacji oraz osób, których dane administrator przetwarza.

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
WYZNACZENIE IOD - **JEDEN INSPEKTOR DLA KILKU ORGANÓW**

- Jak wiele organów może obsługiwać jeden IOD?

To zależy, od m.in. :

- efektywnej **dostępności inspektora**,
- możliwości uzyskania przez niego **szczegółowej wiedzy na temat** funkcjonowania **podmiotu**,
- dysponowania przez niego **odpowiednią** do zakresu zadań i specyfiki procesów przetwarzania danych **ilością czasu,** konieczności **unikania konfliktu interesów**
- oraz **wielkości i struktury organizacyjnej** jednostek będących administratorami danych.

Rozstrzygać należy w kontekście powyższych kryteriów, ze świadomością ciążącej na administratorach danych odpowiedzialności za prawidłowe przestrzeganie przepisów prawa.

Urząd Ochrony Danych Osobowych

JAKIE WARUNKI MUSI SPEŁNIĆ ADMINISTRATOR WOBEC IOD

Motyw 63 Dyrektywy 2016/680

(…) Inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny, zgodnie z prawem państwa członkowskiego.

Motyw 97 rozporządzenia 2016/679

(…) inspektorzy ochrony danych - bez względu na to, czy są pracownikami administratora - powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

Niezależne wykonywanie funkcji IOD jest jedną z najważniejszych cech inspektora jako osoby stojącej na straży przestrzegania prawa, w tym prawa podstawowego jednostki, jakim jest prawo do ochrony danych osobowych.

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
JAKIE WARUNKI MUSI SPEŁNIĆ ADMINISTRATOR WOBEC IOD

ustawa z 14 grudnia 2018 odnosi się do niezależności IOD tylko w jednym przepisie

- Art. 47 ust 4 Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób realizacji zadań, o których mowa w ust. 1, uwzględniając konieczność **zapewnienia prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.**

Urząd Ochrony Danych Osobowych

USTAWA Z DNIA 14 GRUDNIA 2018 R.
JAKIE WARUNKI MUSI SPEŁNIĆ ADMINISTRATOR WOBEC IOD

Gwarancje niezależnego i prawidłowego wykonywania funkcji:

Art. 46 ust 7 Inspektor ochrony danych **podlega bezpośrednio kierownikowi jednostki organizacyjnej** lub osobie fizycznej będącej administratorem lub podmiotem przetwarzającym.

Art. 46 ust. 8. Administrator **zapewnia odpowiednie i niezwłoczne włączenie inspektora** ochrony danych **we wszystkie sprawy dotyczące ochrony danych osobowych.**

Art. 47 ust. 2. Administrator **wspiera inspektora ochrony danych w wypełnianiu zadań**, o których mowa w ust. 1, **zapewniając środki niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania oraz do podnoszenia wiedzy fachowej**.

Art. 47 ust. 3. Administrator może powierzyć inspektorowi ochrony danych wykonywanie **innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań inspektora ochrony danych oraz nie spowoduje to konfliktu interesów.**

BEZPOŚREDNIA PODLEGŁOŚĆ KIEROWNICTWU

- daje inspektorowi wysoką pozycję w strukturze organizacji,
- skraca drogę raportowania
- jest jedną z gwarancji jego niezależności.

Urząd Ochrony Danych Osobowych

ZAPEWNIENIE UDZIAŁU INSPEKTORA WE WSZYSTKICH ZAGADNIENIACH ZWIĄZANYCH Z OCHRONĄ DANYCH OSOBOWYCH

Angażowanie inspektora powinno być **standardową procedurą w organizacji** i służyć zapewnieniu zgodności z prawem i uwzględnianiu ochrony danych w fazie projektowania.

W tym celu należy zapewnić:

- ❑ **udział IOD w spotkaniach kierownictwa, na których podejmowane są decyzje dotyczące przetwarzania danych osobowych**
- ❑ **dostęp IOD do niezbędnych informacji odpowiednio wcześniej, by umożliwić mu zajęcie stanowiska;**
- ❑ **każdorazowe rozważenie stanowiska IOD oraz dokumentowanie przypadków i powodów postępowania niezgodnego z jego zaleceniem**
- ❑ **opracowanie zasad i procedur, które wskazywały przypadki wymagające konsultacji z IOD**

ZASOBY NIEZBĘDNE DO WYKONYWANIA ZADAŃ I UTRZYMANIA WIEDZY FACHOWEJ

Zasada jest taka, że im bardziej skomplikowane procesy przetwarzania danych, tym więcej środków należy przeznaczyć na wsparcie inspektora.

Formy udzielania wsparcia inspektorowi, to np.:

- ustalenie odpowiedniego wymiaru czasu na wykonywanie zadań (zwłaszcza w przypadku IOD zatrudnionych w niepełnym wymiarze, albo łączących obowiązki IOD z innymi zadaniami)
- odpowiednie wsparcie finansowe, kadrowe i infrastrukturalne (pomieszczenia, sprzęt, wyposażenie)
- w uzasadnionych przypadkach powołanie zespołu (IOD i jego pracownicy)
- oficjalne zakomunikowanie wszystkim pracownikom faktu wyznaczenia IOD.
- dostęp do informacji o strukturze organizacyjnej (np. w celu ustalenia przepływu danych)

NAKŁADANIE INNYCH OBOWIĄZKÓW TYLKO, JEŻELI NIE NARUSZY TO PRAWIDŁOWEGO WYKONYWANIA ZADAŃ IOD ORAZ NIE SPOWODUJE KONFLIKTU INTERESÓW.

Co do zasady, za powodujące konflikt interesów uważane będą stanowiska kierownicze (dyrektor generalny, dyrektor ds. operacyjnych, dyrektor finansowy, dyrektor ds. medycznych, kierownik działu marketingu, kierownik działu HR, kierownik działu IT), ale również niższe stanowiska, jeśli biorą udział w określaniu celów i sposobów przetwarzania danych.

Pytania i odpowiedzi w zakładce „Inspektor Ochrony Danych" na stronie uodo.gov.pl:

- **Czy administrator bezpieczeństwa informacji może jednocześnie pełnić funkcję pełnomocnika do spraw ochrony informacji niejawnych?**
- **Czy możliwe jest łączenie funkcji ABI z obowiązkami administratora systemu informatycznego (ASI)?**
- **Czy administratorem bezpieczeństwa informacji może być osoba pełniąca funkcję kierownika komórki w organizacji (np. będąca dyrektorem departamentu, kierownikiem działu IT)?**

NAKŁADANIE INNYCH OBOWIĄZKÓW TYLKO, JEŻELI NIE NARUSZY TO PRAWIDŁOWEGO WYKONYWANIA ZADAŃ IOD ORAZ NIE SPOWODUJE KONFLIKTU INTERESÓW.

Na inspektora nie powinny być nakładane zadania:

- **które mogą być następnie przedmiotem dokonywania przez niego czynności monitorowania lub nadzoru**
- **związane z podejmowaniem decyzji w zakresie celów i środków dot. przetwarzania i zabezpieczania danych**

Urząd Ochrony Danych Osobowych

ROLA INSPEKTORA OCHRONY DANYCH ROZPORZĄDZENIE 2016/679 I DYREKTYWA 2016/680

Motyw 63 Dyrektywy 2016/680

Administrator powinien wyznaczyć osobę, która będzie pomagać mu w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie dyrektywy, z wyjątkiem sytuacji, w której państwo członkowskie podejmie decyzję o zwolnieniu z tego obowiązku sądów i innych niezależnych organów wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości.

Osoba ta powinna pomagać administratorowi i pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony danych.

ROLA INSPEKTORA OCHRONY DANYCH ROZPORZĄDZENIE 2016/679 I DYREKTYWA 2016/680

Motyw 63 Dyrektywy 2016/680

Administrator powinien wyznaczyć osobę, która będzie pomagać mu w monitorowaniu wewnętrznego przestrzegania przepisów przyjętych na podstawie dyrektywy, z wyjątkiem sytuacji, w której państwo członkowskie podejmie decyzję o zwolnieniu z tego obowiązku sądów i innych niezależnych organów wymiaru sprawiedliwości w toku sprawowania przez nie wymiaru sprawiedliwości.

Osoba ta powinna pomagać administratorowi i pracownikom przetwarzającym dane osobowe, dostarczając im informacji i porad na temat przestrzegania spoczywających na nich obowiązków w zakresie ochrony danych. Inspektorzy ochrony danych powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny, zgodnie z prawem państwa członkowskiego.

Motyw 97 rozporządzenia 2016/679

Jeżeli przetwarzania dokonuje organ publiczny z wyjątkiem sądów lub niezależnych organów wymiaru sprawiedliwości w ramach sprawowania wymiaru sprawiedliwości (…) to w monitorowaniu wewnętrznego przestrzegania rozporządzenia administrator lub podmiot przetwarzający powinni być wspomagani przez osobę dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych. Tacy inspektorzy ochrony danych - bez względu na to, czy są pracownikami administratora - powinni być w stanie wykonywać swoje obowiązki i zadania w sposób niezależny.

USTAWA Z DNIA 14 GRUDNIA 2018 R.
ZADANIA IOD

Art. 47. 1. Do zadań inspektora ochrony danych należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;

2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;

3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych;

4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;

5) współpraca z Prezesem Urzędu;

6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4, oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;

7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;

8) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw, o których mowa w rozdziale 4;

9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;

10) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

4. Prezes Rady Ministrów określi, w drodze rozporządzenia, tryb i sposób realizacji zadań, o których mowa w ust. 1, uwzględniając konieczność zapewnienia prawidłowości realizacji zadań inspektora ochrony danych oraz niezależności i organizacyjnej odrębności w wykonywaniu przez niego zadań.

Urząd Ochrony Danych Osobowych

CHARAKTER ZADAŃ INSPEKTORA WSKAZUJE, ŻE OSOBA TA PEŁNI ROLĘ:

- audytorską wobec działań i decyzji administratorów (monitorowanie)

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

- pośrednika pomiędzy zainteresowanymi stronami (między administratorem a organem ochrony danych osobowych, między administratorem a osobami, których dane dotyczą)

ROLA AUDYTORSKA (MONITOROWANIE)

Art. 47 ust. 1

3) monitorowanie zgodności przetwarzania danych przez administratora oraz osoby zajmujące się przetwarzaniem danych osobowych z przepisami niniejszej ustawy oraz innymi przepisami dotyczącymi ochrony danych;

4) monitorowanie realizowania polityk administratora w dziedzinie ochrony danych osobowych, w tym przydział na ich podstawie obowiązków dla osób zajmujących się przetwarzaniem;

6) monitorowanie realizacji zaleceń (*wydanych przez Prezesa UODO w trybie uprzednich konsultacji*), oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;

9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;

10) sporządzanie i przekazywanie administratorowi raz na rok, do końca I kwartału za rok ubiegły, sprawozdania z wykonywania zadań z zakresu ochrony i sposobu przetwarzania danych osobowych.

Urząd Ochrony Danych Osobowych

ROLA AUDYTORSKA (MONITOROWANIE)

Zapewnienie zgodności **nie jest działaniem jednorazowym, wymaga ciągłego monitorowania i doskonalenia rozwiązań.**

Monitorowanie to

- ❑ zbieranie informacji w celu identyfikacji procesów przetwarzania,
- ❑ analizowanie informacji, ich ocena pod kątem zgodności przetwarzania z prawem
- ❑ przekazywanie tych informacji administratorowi wraz z rekomendowaniem podjęcia określonych działań (sprawozdania)

Monitorowanie powinno obejmować wszystkie procesy przetwarzania i ich zgodność ze wszystkimi:

- przepisami o ochronie danych osobowych (dyrektywy 2016/680, RODO, ustaw krajowych, ustaw sektorowych)
- politykami wewnętrznymi administratora
- podziałem obowiązków
- zaleceniami w zakresie oceny skutków dla ochrony danych, w tym wydanymi przez Prezesa UODO w ramach uprzednich konsultacji.

Rozporządzenie Prezesa RM w sprawie trybu i sposobu realizacji zadań IOD?

USTAWA Z DNIA 14 GRUDNIA 2018 R.
ZADANIA IOD – MONITOROWANIE - SPRAWDZENIA

Art. 11. 1. Prezes Urzędu może zwrócić się bezpośrednio do inspektora ochrony danych, o którym mowa w art. 46, o przeprowadzenie sprawdzenia stosowania przepisów niniejszej ustawy przez administratora, który go wyznaczył, wskazując zakres i termin tego sprawdzenia.

2. Po przeprowadzeniu sprawdzenia, o którym mowa w ust. 1, inspektor ochrony danych, za pośrednictwem administratora, przedstawia Prezesowi Urzędu sprawozdanie z przeprowadzonego sprawdzenia.

3. Przeprowadzenie przez inspektora ochrony danych sprawdzenia w przypadku, o którym mowa w ust. 1, nie wyłącza prawa Prezesa Urzędu do przeprowadzenia kontroli, o której mowa w art. 7.

Urząd Ochrony Danych Osobowych

ARCHIWALNA STRONA GIODO – ZAKŁADKA KONTROLE

Sektorowe sprawdzenia dla GIODO – sprawdzenia kompleksowe lub częściowe wskazane w rocznym harmonogramie sprawdzeń, dotyczące wybranej kategorii podmiotów lub zagadnień prowadzone na podstawie art. 19b ustawy o ochronie danych osobowych.

- 2017 r.
  - Wyniki kontroli doraźnych
  - Informacje o kontrolach doraźnych
  - Plan sektorowych sprawdzeń dla GIODO
  - Plan kontroli sektorowych
- 2016 r.
  - Plan kontroli sektorowych
  - Plan sektorowych sprawdzeń dla GIODO
  - Wyniki sektorowych sprawdzeń dla GIODO

ROLA DORADCZA, KONSULTACYJNA I EDUKACYJNA

Art. 47. 1. Do zadań inspektora ochrony danych należy:

1) informowanie administratora oraz osób zajmujących się przetwarzaniem o obowiązkach spoczywających na nich na mocy niniejszej ustawy oraz innych przepisów dotyczących ochrony danych;

2) prowadzenie działań podnoszących świadomość oraz organizowanie szkoleń dla osób uczestniczących w operacjach przetwarzania;

9) przygotowywanie zaleceń co do oceny skutków dla ochrony danych osobowych, w przypadku, o którym mowa w art. 37, oraz monitorowanie wykonania tych zaleceń;

ROLA POŚREDNIKA POMIĘDZY ZAINTERESOWANYMI STRONAMI

(między administratorem a organem ochrony danych osobowych, między administratorem a osobami, których dane dotyczą)

Art. 47. 1. Do zadań inspektora ochrony danych należy:

5) współpraca z Prezesem Urzędu;

6) monitorowanie realizacji zaleceń, o których mowa w art. 38 ust. 4 (uprzednie konsultacje), oraz przedstawianie Prezesowi Urzędu stanu ich realizacji;

7) pełnienie funkcji punktu kontaktowego wobec Prezesa Urzędu w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 38, oraz prowadzenie z Prezesem Urzędu konsultacji we wszelkich innych sprawach;

8) pełnienie funkcji punktu kontaktowego wobec osób, których dane dotyczą w zakresie przysługujących jej praw, o których mowa w rozdziale 4;

PRZYKŁAD: WSPÓŁPRACA W ZAKRESIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Dyrektywa ustawa z dnia 14 grudnia 2018 przewiduje – podobnie jak RODO - obowiązek zgłaszania naruszeń

Art. 4 pkt 6 ustawy z 14.12.2018

Naruszeniem ochrony danych osobowych – jest **naruszenie bezpieczeństwa** prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

PRZYKŁAD: WSPÓŁPRACA W ZAKRESIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

Art. 44. [Zgłoszenie naruszenia ochrony danych osobowych]

1. W przypadku naruszenia ochrony danych osobowych, administrator, bez zbędnej zwłoki, nie później jednak niż **w ciągu 72 godzin po stwierdzeniu naruszenia**, zgłasza naruszenie Prezesowi Urzędu. Przepisu nie stosuje się, jeżeli nie wystąpiło ryzyko naruszenia praw i wolności osób fizycznych.

4. Zgłoszenie, o którym mowa w ust. 1 i 3, zawiera co najmniej następujące informacje:

1)opis charakteru naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wykazów danych osobowych, których dotyczy naruszenie;

2)imię i nazwisko lub nazwę oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, który może udzielić dodatkowych informacji;

3)opis możliwych konsekwencji naruszenia ochrony danych osobowych;

4)opis środków zastosowanych lub zaproponowanych przez administratora w celu usunięcia naruszenia ochrony danych osobowych, w tym zminimalizowania jego ewentualnych negatywnych skutków.

Urząd Ochrony Danych Osobowych

NARUSZENIA OCHRONY DANYCH OSOBOWYCH - RODO

Szczegółowe obowiązki związane z naruszeniem danych osobowych:

- wprowadzenie **procedur umożliwiających stwierdzanie i ocenę naruszeń** pod kątem wystąpienia ryzyka naruszenia praw i wolności osób fizycznych;
- prowadzenie **wewnętrznej ewidencji naruszeń**;
- **zgłaszanie naruszeń organowi nadzorczemu**;
- **powiadamianie osoby, której dane dotyczą o naruszeniu**;
- **podejmowanie działań mających na celu przeciwdziałanie skutkom naruszenia i zapobieganie im w przyszłości.**

Ważnym, jeśli nie najważniejszym, elementem całego procesu związanego ze zgłaszaniem naruszenia ochrony danych, **jest szybkość podjęcia niezbędnych działań, zarówno wobec organu nadzorczego, jak i osób, których dane dotyczą.**

Aby zapewnić działania bez zbędnej zwłoki administratorzy powinni więc **opracować i wdrożyć procedury postępowania na wypadek wystąpienia naruszenia ochrony danych.** Taka procedura pomaga ujednolicić, usprawnić oraz przyśpieszyć działania w przypadku wykrycia naruszenia ochrony danych osobowych.

Urząd Ochrony Danych Osobowych

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Ustawa z 14.12.2018 r.:

Zgodnie z art. 44 ust 6 ustawy administrator zobowiązany jest do dokumentowania dla celów kontrolnych **jedynie przypadków naruszenia ochrony danych osobowych, które podlegają zgłoszeniu Prezesowi UODO.**

RODO odnosi ten obowiązek do wszystkich naruszeń ochrony danych osobowych.

Dokumentowania wszelkich naruszeń wymaga też dyrektywa 2016/680

Art. 30 ust 5. Państwa członkowskie zapewniają, by administrator dokumentował wszelkie naruszenia ochrony danych osobowych, o których mowa w ust. 1, wraz z okolicznościami naruszenia danych osobowych, jego skutkami oraz podjętymi działaniami naprawczymi. Dokumentacja ta pozwala organowi nadzorczemu na weryfikację przestrzegania niniejszego artykułu.

Urząd Ochrony Danych Osobowych

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Druga ważna różnica – przypadki wysokiego ryzyka dla praw i wolności osoby - wyjątki od obowiązku zawiadamiania osoby, której dane dotyczą

Art. 31 ust. 5 **dyrektywa 2016/680** Skierowane do osoby, której dane dotyczą, zawiadomienie wskazane w ust. 1 niniejszego artykułu można opóźnić, ograniczyć lub pominąć, z zastrzeżeniem warunków i z powodów wskazanych w art. 13 ust. 3.

Art. 13 ust. 3 . Państwa członkowskie mogą przyjąć akty prawne pozwalające opóźnić, ograniczyć lub pominąć informowanie osoby, której dane dotyczą, przewidziane w ust. 2 **w takim zakresie i przez taki czas, w jakim odnośny środek jest działaniem koniecznym i proporcjonalnym w społeczeństwie demokratycznym, z należytym uwzględnieniem praw podstawowych i uzasadnionych interesów danej osoby fizycznej,** aby:

a)uniemożliwić utrudnianie czynności postępowań urzędowych lub sądowych, postępowań przygotowawczych lub procedur;

b)uniemożliwić zakłócanie zapobieganiu przestępczości, prowadzeniu postępowań przygotowawczych, wykrywaniu i ściganiu czynów zabronionych i wykonywaniu kar;

c)chronić bezpieczeństwo publiczne;

d)chronić bezpieczeństwo narodowe;

e)chronić prawa i wolności innych osób.

Urząd Ochrony Danych Osobowych

NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Wyjątki od obowiązku zawiadamiania osoby, której dane dotyczą w ustawie z 14.12.2018 r.

Zgodnie z art. 45 ust 6 W przypadku, o którym mowa w art. 26 ust. 1, zawiadomienie, o którym mowa w ust. 1, można opóźnić, ograniczyć lub pominąć.
Art. 26. [Negatywne przesłanki przekazywania informacji i udostępniania danych osobowych]1. Nie przekazuje się informacji, o których mowa w przepisach niniejszego rozdziału, oraz nie udostępnia się danych osobowych, jeżeli mogłoby to powodować:
1)ujawnienie informacji uzyskanych w wyniku czynności operacyjno-rozpoznawczych;
2)utrudnienie lub uniemożliwienie rozpoznawania, zapobiegania, wykrywania lub zwalczania czynów zabronionych;
3)utrudnienie prowadzenia postępowania karnego, karnego wykonawczego, karnego skarbowego lub w sprawach o wykroczenia lub wykroczenia skarbowe;
4)zagrożenie życia, zdrowia ludzkiego lub bezpieczeństwa i porządku publicznego;
5)zagrożenie bezpieczeństwa narodowego, w tym obronności lub bezpieczeństwa oraz ekonomicznych podstaw funkcjonowania państwa;
6)istotne naruszenie dóbr osobistych innych osób.
2. Administrator może przekazać osobie, której dane dotyczą, informacje, o których mowa w ust. 1, w przypadku gdy ich ujawnienie byłoby niezbędne do ochrony życia lub zdrowia ludzkiego.

Urząd Ochrony Danych Osobowych

WSPÓŁPRACA W ZAKRESIE NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

IOD jako punkt kontaktowy dla organu nadzorczego w ramach zgłaszania naruszeń ochrony danych:

- uzyskiwanie przez organ informacji w przypadku niekompletnych lub niespójnych zgłoszeń
- fachowa wiedza IOD i znajomość okoliczności zdarzenia może ułatwić i usprawnić działania organu i administratora
- ważne jest, aby kontakt do inspektora był rzeczywistym i efektywnym kanałem komunikacji

Ostatnie 8 miesięcy to czas wielu pozytywnych doświadczeń w zakresie współpracy z IOD.

Ale zdarzają się też trudności i nieprawidłowości:

- brak wiedzy o zdarzeniu w przypadku (np. IOD obsługujących zbyt wielu inspektorów, słaby przepływ informacji między administratorem a IOD)

- brak możliwości szybkiego skontaktowania się z inspektorem (podany numer telefonu nie odpowiada, nie jest bezpośrednim numerem inspektora, a numerem infolinii lub centrali firmy, brak odpowiedzi na wiadomości elektroniczne, w przypadku nieobecności IOD brak wyznaczonej osoby, która mogłaby udzielić informacji dotyczących naruszeń.

Urząd Ochrony Danych Osobowych

Dziękuję za uwagę!

Urząd Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.uodo.gov.pl
kancelaria@uodo.gov.pl

WYSTĄPIENIE DO ADMINISTRATORA

Naruszenie poufności danych, w szczególności danych dotyczących numeru PESEL wraz z imieniem i nazwiskiem, danymi lokalizacyjnymi oraz danymi kontaktowymi, stanowi poważne naruszenie bezpieczeństwa danych oraz powoduje wysokie ryzyko naruszenia praw i wolności osób fizycznych.

Naruszenie dotyczyło umożliwienia osobom nieupoważnionym, dostępu do wielu kategorii danych osobowych klientów administratora (imię, nazwisko, PESEL, adres zamieszkania, dane kontaktowe, dowodu rejestracyjnego pojazdu oraz wzór podpisu).

Naruszenie powoduje prawdopodobieństwo wysokiego ryzyka negatywnych skutków dla osób, których dane dotyczą, poprzez nieuprawnione wykorzystanie ich danych m.in. w celu:

- ***uzyskania przez osoby trzecie, na szkodę osób, których danych naruszenie dotyczyło, kredytów w instytucjach pozabankowych;***
- ***uzyskanie dostępu do danych o stanie zdrowia lub korzystania ze świadczeń opieki zdrowotnej przysługujących osobom, których danych dotyczyło naruszenie;***
- ***korzystanie z praw obywatelskich np. wykorzystania danych do oddania głosu w głosowaniu nad środkami budżetu obywatelskiego;***
- ***wyrobienia fałszywych dokumentów tj. dowód osobisty, prawo jazdy.***
- ***zawarcie umowy najmu nieruchomości***
- ***zarejestrowanie na dane karty telefonicznej typu pre-paid, w celu posłużenia się nią do celów przestępczych***
- ***posłużenie się danymi przy otrzymywaniu mandatu np. za spożywanie napojów alkoholowych w miejscu publicznym***

WYSTĄPIENIE DO ADMINISTRATORA

*W zawiadomieniu powinno znajdować się wskazanie **zagrożeń płynących z faktu ujawnienia danych osobowych** oraz wskazanie **ewentualnych środków zabezpieczających prawa i wolności osób**, których dane dotyczą przed negatywnymi skutkami naruszenia np.:*

- *możliwość założenia konta w systemie informacji kredytowej i gospodarczej celem monitorowania swojej aktywności kredytowej;*
- *zachowanie ostrożności przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem internetu czy telefonu.*

PRZYKŁADOWE ZAGROŻENIA PŁYNĄCE Z FAKTU UJAWNIENIA DANYCH OSOBOWYCH

Naruszone dane: imię nazwisko adres PESEL, seria i numer dowodu osobistego, numery telefonów, e-mail:

- **Rejestracja karty SIM na Pani/Pana dane osobowe (analiza konta)**
- **Zaciągnięcie zobowiązań w Pani imieniu**
- **Przetwarzanie Pani danych w celach marketingowych/niezamówiona poczta elektroniczna/ niezamówione telefony marketingowe**
- **Założenie na Pani dane konta internetowego (np. w serwisach społecznościowych, poczta elektroniczna)**
- **Próba wykorzystania Pani danych do uwierzytelnienia (weryfikacji tożsamości) np. w firmach/ instytucjach, portalach społecznościowych/ sklepach internetowych**

*PRZYKŁADOWE ŚRODKI ZABEZPIECZAJĄCE PRAWA I WOLNOŚCI **OSÓB**, KTÓRYCH DANE DOTYCZĄ PRZED NEGATYWNYMI SKUTKAMI NARUSZENIA*

Naruszone dane: imię nazwisko adres PESEL, seria i numer dowodu osobistego, numery telefonów, e-mail:

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia administrator zaleca:

a) **Ignorowanie nieoczekiwanych wiadomości e-mail, w szczególności od nieznanych nadawców, nieotwieranie nieznanych załączników,**

b) **Nieodpisywanie na nieoczekiwane wiadomości SMS, w szczególności od nieznanych nadawców;**

c) **Nieużywanie linków do stron internetowych otrzymanych od nieznanych nadawców w wiadomościach e-mail lub SMS-ach;**

d) **Zmiana hasła do konta abonenta, zmiana hasła do skrzynki poczty elektronicznej**

e) **Zastrzeżenie dokumentu tożsamości w systemie dokumenty zastrzeżone (informacje na stronie www.dokumentyzastrzeżone.pl) i jego wymiane**

f) Nieudostępnianie jakichkolwiek haseł lub kodów dostępu osobom nieuprawnionym

g) Weryfikację ustawień w prywatnej skrzynce poczty elektronicznej

h) Okresową weryfikację informacji o sobie np. w biurach informacji kredytowej

KONSTRUKCJA POWIADOMIENIA OSÓB, KTÓRYCH DOTYCZYŁO NARUSZENIE

- **Tytuł: Informacja o naruszeniu Pani danych osobowych**
- **Wstęp: w ostatnim czasie doszło do incydentu wskutek którego Pani dane mogły się dostać w niepowołane ręce**
- **Przekazujemy informacje na temat incydentu oraz działań jakie w związku z nim podejmujemy**
- **Podajemy tez infomacje o krokach, które może Pani podać w związku z incydentem. Prosimy o zapoznanie się z poniższym powiadomieniem.**

Co się stało?

Możliwe konsekwencje dla Pani:

Działania podjęte przez nas:

Co może Pani zrobić?

Więcej informacji:

Urząd Ochrony Danych Osobowych

ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH PRZEZ PODMIOT PRZETWARZAJĄCY

Podmiot przetwarzający nie jest zobowiązany do zgłaszania naruszeń organowi nadzorczemu. Obowiązek ten ciąży na administratorze. Natomiast zgodnie z art. 33 ust. 2 RODO podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych **bez zbędnej zwłoki** zgłasza je administratorowi. Również art. 28 ust. 3 lit. f RODO zobowiązuje podmiot przetwarzający do pomagania administratorowi z wywiązania się z obowiązków określonych w art. 33 RODO np. poprzez udzielenie dostępnych mu w danej sprawie informacji. **Natomiast decyzję o właściwym zaklasyfikowaniu naruszenia w zależności od poziomu ryzyka dla praw i wolności osób, których dane dotyczą, a tym samym o konieczności zgłoszenia naruszenia Prezesowi UODO podejmuje wyłącznie administrator.**

WYSYŁANIE PRZEZ ADMINISTRATORÓW WADLIWYCH ZAWIADOMIEŃ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH DO OSÓB, KTÓRYCH DANE DOTYCZĄ

Zgodnie z art. 34 ust. 2 RODO, gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator, bez zbędnej zwłoki, jasnym i prostym językiem zawiadamia osoby, których naruszenie dotyczy, opisując charakter naruszenia oraz wskazując przynajmniej:

- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, od którego można uzyskać więcej informacji;
- **możliwe konsekwencje naruszenia ochrony danych osobowych** (np. poinformowanie o możliwości kradzieży lub sfałszowaniu tożsamości);
- **środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych,**
- w tym w stosowanych przypadkach **środki w celu zminimalizowania jego ewentualnych negatywnych skutków** (np. możliwość założenia konta w systemie informacji kredytowej celem monitorowania prób uzyskania kredytu, czy zgłoszenie faktu naruszenia danych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości”).

PODANIE W TREŚCI ZGŁOSZENIA DANYCH OSOBOWYCH OSÓB, KTÓRYCH DOTYCZY NARUSZENIE

W zgłoszeniu naruszenia należy podać jedynie informacje wskazane w art. 33 ust. 3 RODO. Przepis ten m.in. wskazuje, że administrator powinien w zgłoszeniu podać tylko kategorie danych osobowych, których dotyczy naruszenie**. Niewłaściwą praktyką jest zatem podawanie w zgłoszeniu naruszenia jakichkolwiek konkretnych imion, nazwisk czy adresów zamieszkania osób, których dane dotyczą.**