NOWE OBOWIĄZKI DYREKTORA JAKO ADMINISTRATORA DANYCH OSOBOWYCH

TOMASZ PAPROCKI

WWW.ABIFUSION24.PL

Ten i inne materiały konferencyjne XIV Konferencji OSKKO znajdziesz na stronie: www.oskko.edu.pl/konferencjaoskko2017

w zakładce *materiały do pobrania*.

Przepisy Prawa

- Ustawa o ochronie danych osobowych;
- Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych;
- Rozporządzenie w sprawie zadań ABI;
- Rozporządzenie w sprawie wzoru zgłoszenia ABI do rejestracji;
- Rozporządzenie w sprawie prowadzenia rejestru przez ABI.
- Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679
- Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680

ZAKRES ZASTOSOWANIA USTAWY

Ustawę stosuje się do przetwarzania danych osobowych:

- w kartotekach, skorowidzach, księgach, wykazach i w innych zbiorach ewidencyjnych (przetwarzanie w formie papierowej);
- w systemach informatycznych, także w przypadku przetwarzania danych poza zbiorem danych (przetwarzanie w formie elektronicznej).

Administrator danych

- **art. 7 pkt 4 u.o.d.o**.
- administrator danych - to organ, jednostka organizacyjna, podmiot lub osoba, o których mowa w art. 3, decydujące o celach i środkach przetwarzania danych osobowych
- **art. 3. u.o.d.o.**
- 1. Ustawę stosuje się do organów państwowych, organów samorządu terytorialnego oraz do państwowych i komunalnych jednostek organizacyjnych.
- 2. Ustawę stosuje się również do:
- 1) podmiotów niepublicznych realizujących zadania publiczne,

art. 36 ust. 1 Ust. o ODO

- administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich :
- udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem

ABI
Administrator Bezpieczeństwa Informacji

Art. 36a. 1. Administrator danych **może** powołać administratora bezpieczeństwa informacji.

Art. 36a. 4. Administrator danych **może** powierzyć administratorowi bezpieczeństwa informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2.

ABI
Administrator Bezpieczeństwa Informacji

- Art. 36a. 5. Administratorem bezpieczeństwa informacji może być osoba, która:
- 1) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych;
- 2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;
- 3) nie była karana za umyślne przestępstwo.

ABI
Administrator Bezpieczeństwa Informacji

Art. 36a .7. Administrator bezpieczeństwa informacji **podlega bezpośrednio kierownikowi jednostki organizacyjnej** lub osobie fizycznej będącej administratorem danych.

Art. 36a.8. Administrator danych **zapewnia** środki i organizacyjną odrębność administratora bezpieczeństwa informacji niezbędne do niezależnego wykonywania przez niego zadań, o których mowa w ust. 2.

Konieczny urzędowy formularz

- Zgłoszenia powołania administratora bezpieczeństwa informacji należy dokonać na urzędowym formularzu, którego wzór określony został w załączniku nr 1 rozporządzenia Ministra Administracji i Cyfryzacji z dnia 10 grudnia 2014 r. w sprawie wzorów zgłoszeń powołania i odwołania administratora bezpieczeństwa informacji (Dz. U. z 2014 r., poz. 1934).

Ten i inne materiały konferencyjne XIV Konferencji OSKKO znajdziesz na stronie: www.oskko.edu.pl/konferencjaoskko2017
w zakładce *materiały do pobrania.*

GIODO odpowiada

- Organizacyjna odrębność umożliwia ABI wykonywanie swoich obowiązków niezależnie od pozostałych komórek organizacyjnych jednostki. Oznacza to także, iż ma on zapewnione odpowiednie środki organizacyjne (ewentualny personel wspierający), jak i finansowe (środki na prowadzenie szkoleń, weryfikowanie zabezpieczeń itp.). Oznacza to też, że w ramach podejmowanych przez siebie czynności ABI nie może podlegać innym osobom lub jednostkom organizacyjnym wchodzącym w skład struktury administratora danych.

źródło www.giodo.gov.pl

GIODO odpowiada

- Przepisy u.o.d.o. nie ustalają konkretnego sposobu powołania ABI przez administratora danych. W przypadku ewentualnej kontroli GIODO istotna będzie możliwość udowodnienia dokonania tej czynności i przyjęcia tej funkcji przez osobą powoływaną.
- Możliwe jest wprowadzenie nowych obowiązków np. aneksem do umowy o pracę albo zawarcie odrębnej umowy w przypadku innej podstawy zatrudnienia .

źródło www.giodo.gov.pl

Czy łączenie funkcji administratora systemu informatycznego i ABI będzie zgodne z przepisami ustawy? GIODO odpowiada

- Łączenie funkcji ABI z obowiązkami administratora systemu informatycznego (ASI) jest przedmiotem dyskusji. Należy mieć świadomość, że powierzenie obu tych funkcji jednej osobie może skutkować brakiem nadzoru nad prawidłową realizacją w sferze bezpieczeństwa przetwarzania danych osobowych. Konsolidacja tych funkcji generuje zagrożenia dla bezpieczeństwa przetwarzania danych osobowych… cdn. >

- > ponieważ w praktyce doprowadza do sytuacji, w której osoba odpowiadająca za bieżące prowadzenie i zabezpieczanie zbiorów danych w systemach informatycznych, jednocześnie sprawuje nadzór nad zgodnością z prawem wykonywanych przez siebie działań.

źródło www.giodo.gov.pl

Przepisy prawa UE

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/680

RODO

- Rozporządzenie znajdzie bezpośrednie zastosowanie od 25 maja 2018 roku, natomiast na implementację dyrektywy i wydanie odpowiednich ustaw krajowych państwa członkowskie mają czas do 6 maja 2018 roku.

Jak RODO definiuje administratora danych

- **Artykuł 4 rozporządzenia stanowi:**

„(…) administratorem jest osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Natomiast jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania”.

Inspektor Ochrony Danych IOD/DPO

- Nowe przepisy istotnie wzmacniają rolę i pozycję inspektorów ochrony danych. Jednym z najważniejszych przejawów tego wzmocnienia jest fakt, że wyznaczenie inspektora ochrony danych, stanie się w wielu przypadkach **obowiązkiem**, a nie jak dotąd, uprawnieniem administratora danych.

Inspektor Ochrony Danych IOD/DPO w RODO

Sekcja 4

Inspektor ochrony danych

Artykuł 37

Wyznaczenie inspektora ochrony danych

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;

ABI

- Art. 36a. 1. Administrator danych **<u>może</u>** powołać administratora bezpieczeństwa informacji.

IOD/DPO

- Artykuł 37

Wyznaczenie inspektora ochrony danych

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

a) przetwarzania dokonują organ lub podmiot publiczny

ABI

Art. 36a. 5. Administratorem bezpieczeństwa informacji może być osoba, która:

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

2) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych;

3) nie była karana za umyślne przestępstwo.

IOD/DPO

Art. 37 5. Inspektor ochrony danych jest wyznaczany

1)na podstawie kwalifikacji zawodowych,

2) wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych

3)umiejętności wypełnienia zadań, o których mowa w art. 39

Artykuł 39
Zadania inspektora ochrony danych

1. **Inspektor ochrony danych ma następujące zadania:**

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

- b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich 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;

- c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;
- d) współpraca z organem nadzorczym; GIODO
- e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Artykuł 38
Status inspektora ochrony danych

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

2. Administrator oraz podmiot przetwarzający wspierają inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39, 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.

- 3. Administrator oraz podmiot przetwarzający zapewniają, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.

4. 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 niniejszego rozporządzenia.

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

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

Przepisy Karne UoDO

Rozdział 8 Przepisy karne

Art. 49

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.**

2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca **podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.**

Przepisy Karne w RODO

- Artykuł 82

Prawo do odszkodowania i odpowiedzialność

1. Każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

- Artykuł 83

Ogólne warunki nakładania administracyjnych kar pieniężnych Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 10 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa: Naruszenia przepisów dotyczących następujących kwestii podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:

Przepisy Karne

- Wysokość kary uzależniona od szeregów czynników i konkretnego przypadku

Co ADO musi wiedzieć o RODO

1) Termin obowiązywania

Przepisy rozporządzenia ogólnego już weszły w życie

Do 25 maja 2018 roku musisz wykazać zgodność działań ze wszystkimi przepisami RODO

Nie ma okresu przejściowego

Co ADO musi wiedzieć o RODO

2. Kto będzie musiał stosować RODO

Prowadzisz działalność w UE , będziesz musiał stosować RODO

RODO będzie obowiązywało sektor publiczny i prywatny

Co ADO musi wiedzieć o RODO

3. Nowe obowiązki ADO,DPO

ocena skutków dla ochrony danych *

(privacy impact assessment)

uwzględnianie prywatności w fazie projektowania (privacy by design)

w ustawieniach domyślnych (privacy by default)

uwzględnianie prywatności w fazie projektowania (privacy by design)

- Na etapie projektowania urządzenia, systemu lub oprogramowania (np. aplikacji bądź platformy internetowej), w wyniku używania którego dochodzić będzie do przetwarzania danych osobowych, należy uwzględniać potrzebę zapewnienia ochrony tym danym, wdrażając w tym celu odpowiednie środki techniczne i organizacyjne (np. minimalizacja danych czy odpowiednie zabezpieczenia).

w ustawieniach domyślnych (PRIVACY BY DEFAULT)

Obowiązkiem jest wdrożenie takich środków technicznych i organizacyjnych, które zapewnią, aby domyślnie zbierane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu.

Stosowanie tego obowiązku ograniczyć ma ilość zbieranych danych, zakres ich przetwarzania, okres przechowywania oraz ich dostępność.

Co ADO musi wiedzieć o RODO

3. cd. Nowe obowiązki ADO,DPO

Analiza ryzyka

Rejestrowanie czynności przetwarzania

Współpraca z organem nadzorczym- GIODO

Odpowiednie zabezpieczenie danych

Zgłaszanie naruszeń do organu nadzorczego- GIODO
(72 godziny od stwierdzenia naruszenia)

ADO musi poinformować GIODO ,że doszło do naruszenia ochrony danych w Twojej strukturze

Zawiadomienie podmiotów danych o naruszeniu

Ocena skutków dla ochrony danych

Uprzednie konsultacje

Co należy uwzględnić wdrażając środki zabezpieczające dane osobowe:

- aktualny stan wiedzy technicznej
- koszt wdrażania środka
- charakter, zakres, kontekst i cele przetwarzania danych osobowych
- ryzyko naruszenia praw i wolności osób fizycznych o rożnym prawdopodobieństwie wystąpienia i wadze zagrożenia
- ryzyko wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych

PRZYKŁADOWE ŚRODKI BEZPIECZEŃSTWA WEDŁUG RODO:

- pseudonimizacja i szyfrowanie danych osobowych
- środki zdolne do ciągłego zapewniania poufności, integralności, dostępności i odporności systemów i usług przetwarzania
- środki zdolne do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania

Obowiązująca dokumentacja

Zgodnie z ustawą oraz przepisami wykonawczymi na dokumentację przetwarzania składają się:

- polityka bezpieczeństwa;
- instrukcja zarzadzania systemem informatycznym służącym do przetwarzania danych osobowych;
- imienne upoważnienia do przetwarzania danych osobowych;
- ewidencja nadanych upoważnień do przetwarzania danych osobowych;
- rejestr zbiorów danych osobowych prowadzony przez ABI (w przypadku jego powołania).

Co ADO musi wiedzieć o RODO

4. Czego już nie będzie

Sformalizowanej dokumentacji : Polityki, Instrukcji, rejestru, itp.

Zgłaszania zbiorów

Rejestru zbiorów ABI

Zmiany haseł co 30 dni

RODO Obowiązująca dokumentacja

1. Zatwierdzony kodeks postępowania

2. Certyfikaty, znaki jakości i inne oznaczenia

Ad1. KTO OPRACOWYWUJE: Zrzeszenia i inne podmioty (np. związki, stowarzyszenia) reprezentujące określone kategorie administratorów lub podmiotów przetwarzających (np. z określonej branży). (**WAŻNA ROLA OSKKO)**

TREŚĆ: Kodeks powinien doprecyzowywać zasady stosowania RODO, przy uwzględnieniu specyfiki działalności podmiotów, na rzecz których jest tworzony.

- **KTO ZATWIERDZA**: Projekt kodeksu zatwierdza krajowy organ nadzorczy. Po zatwierdzeniu kodeksu postępowania krajowy organ nadzorczy rejestruje go i publikuje. Jeżeli kodeks dotyczy czynności przetwarzania prowadzonych w kilku państwach członkowskich, krajowy organ nadzorczy przed jego zatwierdzeniem przedkłada projekt Europejskiej Radzie Ochrony Danych, która wydaje opinię o jego zgodności z RODO.

Istotną nowością jest również rezygnacja z wymogu prowadzenia wykazu zbiorów danych jako elementu polityki bezpieczeństwa oraz obowiązku zgłaszania zbiorów danych do rejestracji GIODO.

Na gruncie RODO zostały one zastąpione obowiązkiem

REJESTROWANIA CZYNNOŚCI PRZETWARZANIA DANYCH.

Prawa podmiotów danych

Prawo do bycia zapomnianym

Prawo do przenoszenia danych

Prawo sprzeciwu

Prawo dostępu do danych i uzyskania kopii

Prawo do niepodlegania profilowaniu

Zgoda dziecka na przetwarzanie danych osobowych w świetle ogólnego rozporządzenia o ochronie danych

Ogólne rozporządzenie o ochronie danych osobowych, które od 25 maja 2018 r. ujednolici zasady ochrony danych osobowych we wszystkich państwach członkowskich UE, stanowi, że korzystanie przez dzieci poniżej 16 roku życia z usług społeczeństwa informacyjnego, a więc m.in. portali społecznościowych i innych usług internetowych, będzie możliwe dopiero po wyrażeniu lub zaaprobowaniu takiej zgody przez rodziców albo opiekunów prawnych. Przewiduje jednak, że państwa członkowskie mogą w swoim prawie ustanowić niższą granicę wiekową – musi ona jednak wynosić co najmniej 13 lat.

UWAGA – NA KORESPONDENCJĘ Z „KANCELARII KONSUMENCKIEJ" „KANCELARII LIBERTY”, „BĄDŹMY LEGALNI” I „LEGALNI Z PRAWEM”

GIODO skierował do organów ścigania zawiadomienie o podejrzeniu popełnienia przestępstwa oszustwa.

NIE WSZYSTKIE SPRAWOZDANIA ZE SPRAWDZEŃ NALEŻY PRZESYŁAĆ DO GIODO

- Generalnemu Inspektorowi Ochrony Danych Osobowych nie należy przesyłać sprawozdań z planowych i doraźnych sprawdzeń realizowanych przez ABI.
- Do Biura Generalnego Inspektora Ochrony Danych Osobowych wpływają sprawozdania z przygotowywanych przez administratorów bezpieczeństwa informacji (ABI) sprawdzeń planowych i doraźnych. Ich opracowywanie jest jednym z ich zadań wynikającym z przepisów ustawy o ochronie danych osobowych (art. 36c w związku z art. 36a ust. 2 pkt 1 lit. a), lecz są one tworzone przede wszystkim na użytek danego podmiotu i nie powinny być przesyłane do GIODO.

- Obowiązek przedstawienia Generalnemu Inspektorowi Ochrony Danych Osobowych – za pośrednictwem administratora danych osobowych – sprawozdania ze sprawdzenia, dotyczy wyłącznie sprawdzeń realizowanych na wniosek GIODO (a więc przypadków określonych w art. 19b ustawy).

Dziękuję z uwagę Tomasz Paprocki

www.abifusion24.pl

Ten i inne materiały konferencyjne XIV Konferencji OSKKO znajdziesz na stronie: www.oskko.edu.pl/konferencjaoskko2017

w zakładce *materiały do pobrania.*