GIODO

Generalny Inspektor
Ochrony Danych Osobowych

ZADANIA INSPEKTORÓW OCHRONY DANYCH

MONIKA MŁOTKIEWICZ
Departament Rejestracji ABI i Zbiorów Danych Osobowych

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Od administratora (bezpieczeństwa informacji) do inspektora (ochrony danych)

Do 1. 01. 2015.

„Administrator danych wyznacza administratora bezpieczeństwa informacji, nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust.1, chyba że sam wykonuje te czynności” (art.36 ust.3 uodo)

URZĘDNIK DS. OCHRONY DANYCH OSOBOWYCH - DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY 95/46/WE

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Motyw 49 i art. 18 ust. 2 Dyrektywy 95/46/WE przewiduje uprawnienie administratora danych do powołania „URZĘDNIKA DO SPRAW OCHRONY DANYCH OSOBOWYCH” (Personal Data Protection Official):

1. **odpowiedzialnego za zapewnienie wewnętrznego stosowania przepisów prawa krajowego**
2. **prowadzącego rejestr operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje określone w rejestrze organu nadzorczego**
3. **sprawującego swoją funkcję w sposób całkowicie niezależny**
4. **który jest lub nie jest pracownikiem administratora danych**

ZADANIA ABI

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zadaniem ABI jest **ZAPEWNIANIE** **przestrzegania przepisów o ochronie danych osobowych** (zgodnie z art. 36a ust. 2 pkt 1 u.o.d.o.), w szczególności przez:

1. **sprawdzanie** **zgodności przetwarzania danych osobowych** z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie **sprawozdania dla administratora danych oraz dla GIODO**,

2. **nadzorowanie** **opracowania i aktualizowania dokumentacji** opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych,

3. **zapewnianie** **zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami** o ochronie danych osobowych.

Zadaniem ABI jest również **prowadzenie rejestru zbiorów** **danych** przetwarzanych przez administratora danych (zgodnie z art. 36a ust. 2 pkt 2 u.o.d.o.), zawierającego nazwę zbioru oraz informacje, o których mowa w art. 41 ust. 1 pkt 2–4a i 7 u.o.d.o.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ZADANIA ABI

Zapewnienie przestrzegania przepisów o ochronie danych osobowych poprzez

- Prowadzenie lokalnego rejestru zbiorów danych (rozporządzenie MAiC)
- Zapewnienie zapoznania osób upoważnionych do przetwarzania z przepisami o ochronie danych osobowych
- Sprawdzanie zgodności przetwarzania (rozporządzenie MAiC)
- Opracowywanie sprawozdań ze sprawdzeń dla administratora danych (rozporządzenie MAiC)
- Nadzór w zakresie dokumentacji opisującej sposób przetwarzania i środki z art. 36 ust. 1 uodo (rozporządzenie MSWiA)
- Nadzór nad opracowaniem dokumentacji
- Nadzór nad wdrożeniem dokumentacji
- Nadzór nad przestrzeganiem zasad określonych w dokumentacji

Administrator bezpieczeństwa informacji **w planie sprawdzeń** uwzględnia, w szczególności, zbiory danych osobowych i systemy informatyczne służące do przetwarzania danych osobowych oraz **konieczność weryfikacji** zgodności przetwarzania danych osobowych:

1) **z zasadami, o których mowa w art. 23–27 i art. 31–35 ustawy;**

2) z zasadami **dotyczącymi zabezpieczenia danych osobowych**, o których mowa w art. 36, art. 37–39 ustawy oraz przepisach wydanych na podstawie art. 39a ustawy;

3) **z zasadami przekazywania danych osobowych**, o których mowa w art. 47–48 ustawy;

4) **z obowiązkiem** zgłoszenia zbioru danych do rejestracji i jego aktualizacji, jeżeli zbiór zawiera dane, o których mowa w art. 27 ust. 1 ustawy.

§ 5. 1. **Osoba odpowiedzialna za przetwarzanie danych osobowych**, której dotyczy sprawdzenie, **bierze udział** w sprawdzeniu lub **umożliwia administratorowi bezpieczeństwa informacji przeprowadzenie czynności w toku sprawdzenia.**

2. Administrator bezpieczeństwa informacji **zawiadamia kierownika jednostki organizacyjnej objętej sprawdzeniem o zakresie planowanych czynności** w terminie co najmniej 7 dni przed dniem przeprowadzenia czynności.

3. **Zawiadomienia nie przekazuje się w przypadku:**

1) sprawdzenia doraźnego, jeżeli niezwłoczne rozpoczęcie sprawdzenia jest niezbędne do przywrócenia stanu zgodnego z prawem lub weryfikacji, czy naruszenie miało miejsce;

§ 4. 1. Administrator bezpieczeństwa informacji **dokumentuje czynności przeprowadzone w toku sprawdzenia**, w zakresie niezbędnym do oceny zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz do opracowania sprawozdania.

2. Dokumentowanie czynności w toku sprawdzenia może polegać, w szczególności, na **utrwaleniu danych z systemu informatycznego** służącego do przetwarzania lub zabezpieczania danych osobowych **na informatycznym nośniku danych lub dokonaniu wydruku tych danych** oraz na:

1) **sporządzeniu notatki** z czynności, w szczególności z zebranych **wyjaśnień, przeprowadzonych oględzin oraz z czynności związanych z dostępem do urządzeń**, nośników oraz systemów informatycznych służących do przetwarzania danych osobowych;

2) **odebraniu wyjaśnień osoby**, której czynności objęto sprawdzeniem;

3) **sporządzeniu kopii otrzymanego dokumentu**;

Par. 3 ust. 5 Plan sprawdzeń jest przygotowywany przez administratora bezpieczeństwa informacji **na okres nie krótszy niż kwartał i nie dłuższy niż rok.** Plan sprawdzeń jest przedstawiany administratorowi danych **nie później niż na dwa tygodnie przed dniem rozpoczęcia okresu objętego planem**. Plan sprawdzeń obejmuje co najmniej jedno sprawdzenie.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ZADANIA IOD

1. wykonywane z uwzględnieniem ryzyka,

2. podejście systemowe i procesowe,

3. możliwość przyporządkowania zadań 3 rolom: doradczej, audytorskiej i „łącznikowej”.

WYPEŁNIANIE ZADAŃ „Z NALEŻYTYM UWZGLĘDNIENIEM RYZYKA”

GIODO
Generalny Inspektor Ochrony Danych Osobowych

DPO ma ustalać priorytety w swojej pracy i koncentrować się na aspektach pociągających za sobą większe ryzyko.

Wypełnianie zadań „z należytym uwzględnieniem ryzyka”

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 39 ust. 2 Inspektor ochrony danych wypełnia swoje zadania **z należytym uwzględnieniem ryzyka** związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

art. 24 RODO administratorzy i podmioty przetwarzające, są zobowiązani **uwzględniać charakter, zakres, kontekst i cele przetwarzania** oraz **ryzyko** naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, i **odpowiednio do nich - dobierać i wdrażać środki techniczne i organizacyjne**, tak, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby móc to wykazać.

WYPEŁNIANIE ZADAŃ „Z NALEŻYTYM UWZGLĘDNIENIEM RYZYKA”

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Takie podejście powinno ułatwić DPO doradzenie administratorowi np.:

- na które operacje przetwarzania należy przeznaczyć więcej czasu i zasobów
- które obszary powinny zostać poddane wewnętrznemu albo zewnętrznemu audytowi
- jakie szkolenia należy przeprowadzić dla pracowników lub kierowników odpowiedzialnych za przetwarzanie danych

WEWNĘTRZNE REGUŁY DOTYCZĄCE FUNKCJONOWANIA IOD (I ZOBOWIĄZANIE DO ICH PRZESTRZEGANIA)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Przykłady:

- inspektor **działa w sposób niezależny i nie może przyjmować żadnych instrukcji dotyczących sposobu wykonywania obowiązków.**
- musi być **w stanie zademonstrować zdolność do właściwego osądu oraz do zachowania bezstronnego i obiektywnego podejścia**
- inspektor **może wydawać zalecenia i udzielać porad kierownictwu i osobom upoważnionym do przetwarzania danych**
- może **prowadzić dochodzenia, na wniosek albo z własnej inicjatywy**, w sprawach dotyczących bezpośrednio jego zadań oraz składać sprawozdanie osobie, która zleciła dochodzenie,
- jeżeli **wnioskodawca jest osobą fizyczną (w tym pracownikiem) lub działa w imieniu takiej osoby, inspektor musi, w najszerszym możliwym zakresie**, zapewnić **poufność wniosku,** chyba że osoba, której dotyczą dane, udzieli mu wyraźnej zgody na inne traktowanie tego wniosku.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- może **wnioskować o opinię prawną służby prawnej**
- inspektor **ma nieustanny dostęp do danych będących przedmiotem operacji przetwarzania i do wszystkich biur, instalacji przetwarzających dane i nośników danych.**
- Inspektor **prowadzi spis wszystkich operacji przetwarzania danych osobowych** prowadzonych przez Komisję, **do którego koordynatorzy wpisują** w imieniu swoich dyrekcji generalnych **wszystkie operacje przetwarzania, które należy zgłosić.** Koordynatorzy **powinni także wskazywać kontrolerów odpowiedzialnych za takie operacje przetwarzania danych**. Inspektor **pomaga** kontrolerowi, **ocenić ryzyko podlegającej mu operacji przetwarzania danych i monitorować wykonywanie rozporządzenia w ramach Komisji**

DECYZJA KOMISJI Wspólnot Europejskich z dnia 3 czerwca 2008 r. **w sprawie przyjęcia przepisów wykonawczych w zakresie inspektora ochrony danych** zgodnie z art. 24 ust. 8 rozporządzenia (WE) nr 45/2001 o ochronie osób fizycznych **w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych** (2008/597/WE)

TWORZENIE SKUTECZNEGO SYSTEMU OCHRONY DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Podejście systemowe i procesowe

ROZLICZALNOŚĆ - SYSTEMATYCZNY PROGRAM ZGODNOŚCI I SKUTECZNOŚCI

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- Bezpośrednie zaangażowanie kierownictwa najwyższego szczebla i zapewnienie nadzoru (wskazanie osoby nadzorującej)
- Prowadzenie ciągłego procesu oceny ryzyka (ryzyko naruszenia praw i wolności, ale i ryzyka dla organizacji)
- Polityki i procedury
- Privacy by design
- Zasada przejrzystości
- Szkolenia
- Monitorowanie, weryfikowanie przestrzegania wprowadzonych zasad
- Skargi, naruszenia, egzekwowanie odpowiedzialności

TWORZENIE SKUTECZNEGO SYSTEMU OCHRONY DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- przebudowanie myślenia:

➢ ochrona danych strategii działania **instytucji i jej przywództwa**

➢ wpisanie ochrony danych **w proces zarządzania organizacją**

➢ przestrzeganie przepisów o ochronie danych osobowych - **wysiłkiem i odpowiedzialnością wszystkich pracowników**

➢ zapewnienie zgodności **nie jest działaniem jednorazowym, wymaga monitorowania**

➢ minimalizowanie ryzyka prawnego, finansowego i reputacyjnego

ROLA IOD W TWORZENIU SKUTECZNEGO SYSTEMU OCHRONY DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Osoby fizyczne (interesanci) są coraz bardziej świadomi swoich praw w zakresie ochrony danych osobowych i oczekują, że instytucje publiczne:

- będą postępować z ich danymi w sposób zgodny z prawem, odpowiedzialny i przejrzysty (to jest ważne również na etapie tworzenia przepisów prawa)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- zasada rozliczalności nabiera innego sensu
- chronimy dane nie tylko dlatego, że wymagają od nas tego przepisy prawa ale dlatego, że to jest racjonalne i korzystne zarówno dla organizacji, jak i jej interesantów
- ochrona danych zakorzenia się w myśleniu każdego w organizacji
- zyskujemy autentyczne przestrzeganie przepisów, które dużo łatwiej nam wykazać

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

Jak rozumieć i stosować podejście oparte na ryzyku? – poradnik GIODO

Metadane

Zgodnie z RODO, każdy podmiot musi samodzielnie oceniać ryzyko, jakie przetwarzanie danych osobowych może spowodować dla praw i wolności osób, których te dane dotyczą. To właśnie te wartości należy przede wszystkim brać pod uwagę.

Ogólne rozporządzenie o ochronie danych (RODO) nie odnosi się wprost do procesu zarządzania ryzykiem i nie wskazuje konkretnej metody przeprowadzania oceny w tym zakresie. Każdy podmiot musi dokonywać jej samodzielnie, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne czy zakres i rodzaj danych oraz cel ich przetwarzania. Jednym ze skutecznych systemowych sposobów dokonywania oceny ryzyka jest wdrożenie w danej jednostce procesu zarządzania ryzykiem.

Dla ułatwienia przyjęcia w tym zakresie właściwych rozwiązań, Generalny Inspektor Ochrony Danych Osobowych (GIODO), przygotował dwuczęściowy poradnik.

SPIS TREŚCI

Proces zarządzania ryzykiem powinien być wpisany w proces zarządzania organizacją. Spełnienie tego warunku wymaga ustalenia wszystkich procesów zachodzących w organizacji (w tym dotyczących przetwarzania danych osobowych)**, uwarunkowań wewnętrznych i zewnętrznych dotyczących środowiska, w którym ona funkcjonuje.** Kluczowym elementem w stosowaniu podejścia opartego na ryzyku jest przyjęcie przez organizację określonej **systematyki i kolejności działań**.

W dużych organizacjach o złożonej strukturze może być **potrzebne wyznaczenie zespołu odpowiedzialnego za proces zarządzania ryzykiem**. W skład zespołu zwykle **powołuje się przewodniczącego** (np. prezesa/wiceprezesa lub innego członka zarządu), koordynatora tego zespołu (menedżera ds. ryzyka), **właścicieli procesów biznesowych oraz aktywów** (np. dyrektorów departamentów), ekspertów dziedzinowych (np. ekspertów ds. bezpieczeństwa informacji, ekspertów ds. bezpieczeństwa fizycznego itp.), a następnie **przypisuje się im określony zakres uprawnień i odpowiedzialności, czyli rolę w całym procesie.**

Ponieważ zarządzanie ryzykiem obejmuje wszystkie szczeble organizacji, a także to, że **proces zarządzania ryzykiem powinien być częścią procesu zarządzania organizacją**, osoby wybrane do zespołu powinny mieć **odpowiednio wysokie umocowanie**.

Raporty oraz pojawiające się nieprawidłowości powinny być zgłaszane bezpośrednio najwyższemu kierownictwu administratora, np. członkom zarządu.

Włączenie w ten proces wszystkich pracowników i ścisła współpraca z nimi. Pracownicy stanowią **cenne źródło informacji, jeżeli chodzi o określanie źródeł ryzyka**. Z tego powodu warto stworzyć dla nich **efektywną ścieżkę służącą zgłaszaniu wszystkich zauważonych w tym zakresie problemów**, w **tym naruszeń, oraz propozycji rozwiązań**. Muszą oni **zostać poinformowani, komu i w jaki sposób mogą dokonać tego typu zgłoszenia oraz z kim mogą się w tej sprawie w razie wątpliwości kontaktować**. Warto również (np. w formie ankiet) okresowo **zwracać się do nich z prośbą o wskazanie zauważonych problemów.** Pracownikom powinny być **ponadto przedstawiane wnioski z analizy ryzyka oraz związane z tymi wnioskami rekomendacje.**

- Szacowanie ryzyka należy traktować **jako proces ciągły.**
- Ochrona danych osobowych powinna **być zapewniona na każdym etapie procesu przetwarzania danych i na każdym etapie powstawania systemu przetwarzania danych (tj. podczas całego cyklu życia informacji, od momentu zbierania danych aż do ich usunięcia)**
- konieczne jest **wbudowanie zasad ochrony danych osobowych w każdy projekt zakładający przetwarzanie danych osobowych**, zgodnie z zasadą **uwzględniana ochrony danych w fazie projektowania (ang. *privacy by design*)** tj. od momentu pojawienia się koncepcji systemu przetwarzania, przez budowę projektu, stworzenie systemu, następnie jego wdrożenie i eksploatację, kończąc na usunięciu danych.
- **Skuteczność wdrożonych środków ochrony powinna być monitorowana i doskonalona.**

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

3 role inspektora:

- doradcza
- audytorska
- łącznikowa

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)

ZADANIA DPO

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

1. INFORMOWANIE I DORADZANIE W ZAKRESIE OBOWIĄZKÓW CIĄŻĄCYCH NA ADMINISTRATORZE, PODMIOCIE PRZETWARZAJĄCYM I PRACOWNIKACH

- ochrona danych w fazie projektowania („privacy by design”)

- domyślna ochrona danych w systemach IT („privacy by default”)

DORADZANIE I INFORMOWANIE

GIODO
Generalny Inspektor Ochrony Danych Osobowych

PRIVACY BY DESIGN „ochrona prywatności w fazie projektowania”

Narzędzia i usługi powinny być tak konstruowane, by od samego początku uwzględniały potrzebę ochrony prywatności obywateli. Perspektywa ta zakłada więc działania o charakterze proaktywnym i prewencyjnym. Administratorzy danych nie mają jedynie odpowiadać na pojawiające problemy, ale również je przewidywać. Ochrona prywatności staje się wówczas nie tylko dodatkiem do produktu, ale jego integralną częścią.

PRIVACY BY DEFAULT „domyślna ochrona danych”

Domyślne ustawienia mają chronić prywatność użytkowników

Domyślnie przetwarzane są tylko niezbędne dane

Prywatność chroniona mimo braku działań użytkownika

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Motyw 78 cd Jeżeli opracowywane, projektowane, wybierane i użytkowane są aplikacje, usługi i produkty, które opierają się na przetwarzaniu danych osobowych należy **zachęcać wytwórców tych produktów, usług i aplikacji,** by podczas opracowywania i projektowania takich produktów, usług i aplikacji **wzięli pod uwagę prawo do ochrony danych osobowych** i z należytym uwzględnieniem stanu wiedzy technicznej zapewnili administratorom i podmiotom przetwarzającym możliwość wywiązania się ze spoczywających na nich obowiązków ochrony danych.

Zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę **w przetargach publicznych.**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

(77) Wskazówki co do tego, jak wdrożyć odpowiednie środki oraz wykazać przestrzeganie prawa przez administratora lub podmiot przetwarzający dane – w szczególności jeżeli **chodzi o identyfikowanie ryzyka związanego z przetwarzaniem, o jego ocenę** pod kątem źródła, charakteru, prawdopodobieństwa i wagi zagrożenia **oraz o najlepsze praktyki pozwalające zminimalizować to ryzyko –** mogą być przekazane w szczególności w formie zatwierdzonych kodeksów postępowania, zatwierdzonej certyfikacji, wytycznych Europejskiej Rady Ochrony Danych lub **poprzez sugestie inspektora ochrony danych. (…)**

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Konieczność regularnego testowania, mierzenia i oceniania skuteczności wdrożonych środków technicznych i organizacyjnych, które mają zapewnić bezpieczeństwo przetwarzania danych (art. 24 ust 1, art. 32 ust 1 lit. d RODO)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ZADANIA DPO

2. MONITOROWANIE PRZESTRZEGANIA PRZEPISÓW I POLITYK W DZIEDZINIE OCHRONY DANYCH OSOBOWYCH

- PODZIAŁ OBOWIĄZKÓW
- AUDYTY
- DZIAŁANIA ZWIĘKSZAJĄCE ŚWIADOMOŚĆ
- SZKOLENIA

MONITOROWANIE - POLITYKI

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

MOTYW 78 Ochrona praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych wymaga wdrożenia odpowiednich środków technicznych i organizacyjnych, by zapewnić spełnienie wymogów niniejszego rozporządzenia. **Aby MÓC WYKAZAĆ przestrzeganie niniejszego rozporządzenia, administrator powinien przyjąć wewnętrzne polityki i wdrożyć środki**, które są zgodne w szczególności z zasadą uwzględniania ochrony danych w fazie projektowania oraz z zasadą domyślnej ochrony danych..

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

cja Współpraca Wydarzenia Serwis prasowy Odpowiedzi na pytania Kontakt

» Porady i wskazówki » Wskazówki dla Administratorów Danych

Nie wolno ujawniać dokumentacji związanej z zabezpieczaniem informacji i danych osobowych

Metadane

Polityka bezpieczeństwa i Instrukcja zarządzania systemem informatycznym to dokumenty wewnętrzne, które powinny być udostępniane jedynie ograniczonemu kręgowi osób.

Wiele podmiotów często myli dokumenty określające politykę przetwarzania danych osobowych z dokumentami wewnętrznymi określającymi politykę bezpieczeństwa. Tymczasem to dwa różne zestawy informacji, służące zupełnie innym celom.

Polityka przetwarzania danych osobowych (Polityka prywatności)

Polityka przetwarzania danych nazwana tutaj „Polityką przetwarzania danych osobowych" to dokument, w którym

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

DZIAŁANIA ZWIĘKSZAJĄCE ŚWIADOMOŚĆ

SZKOLENIA

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

AUDYTY

MONITOROWANIE ZGODNOŚCI Z RODO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Np.

- zbieranie informacji w celu identyfikacji procesów przetwarzania

- analizowanie i sprawdzanie zgodności przetwarzania

- rekomendowanie określonych działań

PRZYKŁADOWE WYSTĄPIENIE O SPRAWDZENIE GIODO – ABI- informator

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ABC Sprawdzenia

- Wystąpienie GIODO
- Sprawdzenie
- Sprawozdanie
- Przesłanie sprawozdania do GIODO
- Co dalej?

Przepisy

Ważne!

Na czym polega?

Kto dokonuje?

Termin i zakres

Sprawozdanie

ABC Sprawdzenia

Wystąpienie GIODO

GIODO zwraca się w formie pisemnej do ABI o dokonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych określając zakres i termin sprawdzenia.

Zakres sprawdzenia może dotyczyć określonego przez GIODO zagadnienia (np. monitoringu wizyjnego), kategorii danych osobowych (np. danych biometrycznych, danych tzw. wrażliwych), realizacji określonego obowiązku wynikającego z przepisu prawa (np. realizacji obowiązku informacyjnego), konkretnego zbioru danych osobowych (np. zbioru kadrowo-płacowego, zbioru klientów) lub systemu informatycznego.

GIODO określa termin, w którym sprawozdanie ze sprawdzenia powinno zostać przedstawione.

GIODO umieszcza również pouczenie dotyczące sposobu dokonania sprawdzenia.

Załączone dokumenty:

- Przykładowe wystąpienia GIODO – dotyczy systemu monitoringu
- Przykładowe wystąpienia GIODO – dotyczy zastosowanych środków bezpieczeństwa

WNIOSKI W ZAKRESIE PRAWIDŁOWOŚCI PRZEDSTAWIONYCH SPRAWOZDAŃ

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- brak wszystkich niezbędnych informacji (odniesienia się do pytań zawartych w wystąpieniu) i dowodów potwierdzających dokonane ustalenia

- brak spójności pomiędzy ustaleniami a załącznikami (ABI oświadcza, iż nie stwierdził nieprawidłowości, a z analizy dokumentacji wynika, iż takie nieprawidłowości są)

- brak wskazania, które z załączonych dokumentów dotyczą poszczególnych ustaleń

WNIOSKI W ZAKRESIE PRAWIDŁOWOŚCI PRZEDSTAWIONYCH SPRAWOZDAŃ

GIODO
Generalny Inspektor Ochrony Danych Osobowych

- brak wskazania planowanych lub podjętych działań przywracających stan zgodny z prawem (art. 36c pkt 7 uodo)
- przesłanie sprawozdania bez wymaganego pośrednictwa administratora danych (brak podpisu administratora danych na sprawozdaniu lub w piśmie przewodnim) (art. 19b ust. 2 uodo)
- brak podpisu ABI lub brak jego parafy na każdej stronie sprawozdania (art. 36c pkt 9 uodo)

ZADANIA DPO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

3. ZALECENIA I KONSULTACJE CO DO OCENY SKUTKÓW DLA OCHRONY DANYCH I MONITOROWANIE JEJ WYKONANIA

W art. 35 RODO na administratora danych nałożony został obowiązek dokonywania oceny oraz konsultowania się przy dokonywaniu oceny *z inspektorem ochrony danych, jeżeli został on wyznaczony.*
Przepis ten określa, kiedy i jak należy dokonywać oceny skutków dla ochrony danych.

Monitorowanie – art. 35 ust. 11 RODO - W razie potrzeby, przynajmniej gdy zmienia się ryzyko wynikające z operacji przetwarzania, **administrator dokonuje przeglądu, by stwierdzić, czy przetwarzanie odbywa się zgodnie z oceną skutków dla ochrony danych.**

ROLA DPO W OCENIE SKUTKÓW DLA OCHRONY DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

GR zaleca administratorowi konsultowanie z DPO m.in. następujących kwestii:

- ❑ **czy należy przeprowadzić ocenę skutków dla ochrony danych**
- ❑ **metodologii przeprowadzenia oceny skutków dla ochrony danych**
- ❑ **czy należy przeprowadzić wewnętrzną ocenę, czy też zlecić ją podmiotowi zewnętrznemu**
- ❑ **zabezpieczeń zastosowanych, żeby złagodzić ryzyko naruszenia praw i interesów osób, których dane dotyczą**
- ❑ **prawidłowości przeprowadzonej oceny i zgodności jej wyników z RODO tzn. czy należy kontynuować przetwarzanie czy też nie oraz jakie jeszcze zabezpieczenia należy zastosować).**

Jeśli administrator nie zgadza się z zaleceniami DPO, dokumentacja oceny powinna zawierać pisemne uzasadnienie nieuwzględnienia tych zaleceń.

ZADANIA DPO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

4. WSPÓŁPRACA Z ORGANEM NADZORCZYM

Artykuł 31

Współpraca z organem nadzorczym

Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ZADANIA DPO

5. PEŁNIENIE FUNKCJI PUNKTU KONTAKTOWEGO DLA ORGANU NADZORCZEGO w tym w zakresie uprzednich konsultacji z art. 36 i konsultacji we wszelkich innych sprawach

DPO ma pełnić funkcję punktu kontaktowego **by umożliwić** organowi nadzorczemu dostęp do dokumentów i informacji w celu realizacji zadań, o których mowa w art. 57, jak również wykonywania uprawnień w zakresie prowadzonych postępowań, uprawnień naprawczych, uprawnień w zakresie wydawania zezwoleń oraz uprawnień doradczych, zgodnie z art. 58.

ZADANIA IOD

GIODO
Generalny Inspektor Ochrony Danych Osobowych

6. PEŁNIENIE FUNKCJI PUNKTU KONTAKTOWEGO DLA OSÓB, KTÓRYCH DANE DOTYCZĄ

- art. 38 ust. 4 RODO, 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 RODO .

UŁATWIANIE OSOBOM WYKONYWANIA SWOICH PRAW

GIODO
Generalny Inspektor Ochrony Danych Osobowych

59. ***Należy przewidzieć procedury ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy niniejszego rozporządzenia (…)– w szczególności dostępu do danych osobowych i ich sprostowania lub usunięcia oraz możliwości wykonywania prawa do sprzeciwu***. (…). Administrator powinien być **zobowiązany udzielić odpowiedzi na żądania osób, których dane dotyczą, bez zbędnej zwłoki – najpóźniej w terminie miesiąca**, a jeżeli nie zamierza spełnić takiego żądania – podać tego przyczyny.

60. Zasady rzetelnego i przejrzystego przetwarzania wymagają, **by osoba, której dane dotyczą, była informowana o prowadzeniu operacji przetwarzania i o jej celach.** Ponadto należy poinformować osobę, której dane dotyczą, o fakcie profilowania oraz o konsekwencjach takiego profilowania.

UDZIELANIE INFORMACJI I POMOCY PODMIOTOM DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 12 RODO

ust. 2 **Administrator ułatwia osobie**, której dane dotyczą, **wykonanie praw** przysługujących jej na mocy art. 15–22.

ust 3. Administrator bez zbędnej zwłoki – a w każdym razie w terminie miesiąca od otrzymania żądania – **udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem** na podstawie art. 15–22.

UDZIELANIE INFORMACJI I POMOCY PODMIOTOM DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 12 RODO

ust. 4. Jeżeli administrator **nie podejmuje działań w związku z żądaniem osoby,** której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – **informuje osobę**, której dane dotyczą, **o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego** oraz skorzystania ze środków ochrony prawnej przed sądem.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

ZADANIA DPO

7. REJESTROWANIE CZYNNOŚCI (kategorii czynności) PRZETWARZANIA

W JAKIM CELU? - MOTYW 82

Dla zachowania **zgodności** z niniejszym rozporządzeniem

W ramach **współpracy** z organem nadzorczym, na jego żądanie **udostępniać mu rejestry** w celu monitorowania operacji przetwarzania.

KTO I W JAKI SPOSÓB MA PROWADZIĆ? – ART. 30

Administrator prowadzi REJESTR CZYNNOŚCI.

Podmiot przetwarzający prowadzi rejestr wszystkich KATEGORII CZYNNOŚCI DOKONYWANYCH W IMIENIU ADMINISTRATORA

WYŁĄCZENIA Z OBOWIĄZKU

Obowiązek nie dotyczy podmiotów zatrudniających mniej niż 250 osób, chyba że:

przetwarzanie może powodować ryzyko naruszenia praw i wolności podmiotów danych,

przetwarzanie nie ma charakteru sporadycznego,

Przetwarzanie obejmuje szczególne kategorie danych osobowych lub dane dotyczące wyroków skazujących i naruszeń prawa

Lp.	Zawartość rejestru czynności przetwarzania prowadzonego przez ADO	Zawartość rejestru czynności przetwarzania prowadzonego przez podmiot przetwarzający
1.	imię i nazwisko lub nazwa oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych	imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;
2.	cele przetwarzania	kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
3.	opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych	
4.	kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych	
5.	gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;	gdy ma to zastosowanie – przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń
6.	jeżeli jest to możliwe – planowane terminy usunięcia poszczególnych kategorii danych	
7.	jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rodo	jeżeli jest to możliwe – ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 rodo

ROLA DPO W EWIDENCJONOWANIU

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Prowadzenie rejestru „czynności przetwarzania” to obowiązki administratora albo podmiotu przetwarzającego.

Katalog zadań DPO wskazany w art. 39 nie jest zamknięty i na mocy od dawna ustalonej praktyki to DPO tworzy i prowadzi zwykle rejestry w oparciu o dane otrzymane od pozostałych komórek organizacji.

GIODO
Generalny Inspektor
Ochrony Danych Osobowych

W jaki sposób działania IOD i organów nadzorczych będą się uzupełniać?

MONITOROWANIE PRZESTRZEGANIA OGÓLNEGO ROZPORZĄDZENIA O OCHRONIE DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Organ nadzorczy	DPO
• monitoruje i egzekwuje stosowanie RODO; • monitoruje zmiany w stosownych dziedzinach, o ile zmiany te mają wpływ na ochronę danych osobowych, w szczególności monitoruje rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;	• monitoruje przestrzeganie RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych; • monitoruje wykonanie zaleceń w zakresie oceny skutków dla ochrony danych zgodnie z art. 35 RODO;

MONITOROWANIE PRZESTRZEGANIA USTAWY O OCHRONIE DANYCH OSOBOWYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zadaniem **zarejestrowanych** administratorów bezpieczeństwa informacji jest **zapewnianie przestrzeganie przepisów,** m.in.

- poprzez dokonywanie sprawdzeń i sporządzanie sprawozdań (w tym na zlecenie GIODO)
- oraz nadzorowanie wdrożenia wymaganej przepisami dokumentacji.

PODNOSZENIE POZIOMU ŚWIADOMOŚCI PRAWNEJ EDUKOWANIE ADO I PODMIOTÓW PRZETWARZAJĄCYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Organ nadzorczy	DPO
• upowszechnia w społeczeństwie wiedzę o ryzyku, przepisach, zabezpieczeniach i prawach związanych z przetwarzaniem oraz rozumienie tych zjawisk. Szczególną uwagę poświęca działaniom skierowanym do dzieci; • upowszechnia wśród administratorów i podmiotów przetwarzających wiedzę o obowiązkach spoczywających na nich na mocy rozporządzenia;	• informuje administratora, podmiot przetwarzający 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 doradza im w tej sprawie; • prowadzi działania zwiększające świadomość dotyczącą ochrony danych osobowych, tj. szkolenia

Podnoszenie poziomu świadomości prawnej
Edukowanie ADO i podmiotów przetwarzających

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zadania ABI/DPO

Art. 36a ust. 2 lit. c UODO:

- zapewnianie **zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami** o ochronie danych osobowych

UDZIELANIE INFORMACJI I POMOCY PODMIOTOM DANYCH

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Organ nadzorczy	DPO
• udziela osobie, której dane dotyczą, na jej żądanie informacji o wykonywaniu praw przysługujących im na mocy RODO , a w stosownym przypadku współpracuje w tym celu z organami nadzorczymi innych państw członkowskich;	pełni rolę punktu kontaktowego dla osób, których dane dotyczą, art. 38 ust. 4 RODO, 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 RODO .

WSPÓŁPRACA I WZAJEMNA POMOC

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 39 ust. 1 Inspektor ochrony danych ma zadanie:

d) współpracy z organem nadzorczym

Artykuł 31

Współpraca z organem nadzorczym

Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.

WSPÓŁPRACA I WZAJEMNA POMOC

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 39 ust. 1 lit. d RODO

Inspektor ochrony danych ma za zadanie: współpracę z organem nadzorczym

art. 57. ust 3 RODO Zadania organu nadzorczego

KAŻDY ORGAN NADZORCZY WYPEŁNIA ZADANIA NA RZECZ OSOBY, KTÓREJ DANE DOTYCZĄ, I – **GDY MA TO ZASTOSOWANIE – INSPEKTORA OCHRONY DANYCH BEZPŁATNIE.**

DPO **może również konsultować się z organem nadzorczym** w stosownych przypadkach.

Współpraca - komunikowanie się w jednym języku

GIODO
Generalny Inspektor Ochrony Danych Osobowych

DPO powinien mieć możliwość sprawnego komunikowania się z osobami, których dane dotyczą **i współpracy z organem nadzorczym.**

Oznacza to, że **komunikacja musi odbywać się w języku lub językach używanych przez organy nadzorcze** i osób, których dane dotyczą.

Współpraca z DPO - postępowania kontrolne

GIODO
Generalny Inspektor Ochrony Danych Osobowych

art. 58 ust 1 Każdemu organowi nadzorczemu przysługują wszystkie następujące uprawnienia w zakresie prowadzonych postępowań:

b) prowadzenie **postępowań w formie audytów ochrony danych;**

e) **uzyskiwanie od administratora i podmiotu przetwarzającego dostępu do wszelkich danych osobowych** i wszelkich informacji niezbędnych organowi nadzorczemu do realizacji swoich zadań;

OCENA SKUTKÓW DLA OCHRONY DANYCH – ZADANIA GIODO

GIODO
Generalny Inspektor Ochrony Danych Osobowych

art. 57 ust 1 lit k organ nadzorczy ustanawia i prowadzi wykaz rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych

art. 57 ust 1 lit l udziela zaleceń, o których mowa w art. 36 ust. 2, dotyczących operacji przetwarzania

Współpraca - wymiana poglądów i doświadczeń

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art.12 UODO zadania GIODO:

• opiniowanie projektów ustaw i rozporządzeń dotyczących ochrony danych osobowych;
• inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych;

Art. 57 RODO zadania GIODO:

- upowszechnia wiedzę
- doradza parlamentowi narodowemu, rządowi oraz innym instytucjom i organom w sprawie aktów prawnych
- monitoruje zmiany w stosownych dziedzinach, w szczególności rozwój technologii informacyjno-komunikacyjnych i praktyk handlowych;
- wypełnia inne zadania związane z ochroną danych osobowych.

PUNKT KONTAKTOWY - konsultacje we wszelkich innych sprawach.

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Art. 33 ust 3 lit. b RODO
Zgłoszenie, naruszenia danych, musi zawierać m.in. co najmniej imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, **od którego można uzyskać więcej informacji**

GIODO

Generalny Inspektor
Ochrony Danych Osobowych

Dziękuję za uwagę!

20-LECIE PRAWA
DO OCHRONY DANYCH
OSOBOWYCH W POLSCE

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl