„ZATWIERDZAM”

Jan Śmiałowski

OBOWIĄZKI

Inspektora Ochrony Danych Osobowych

w Stowarzyszeniu
POLSKIE DRUŻYNY STRZELECKIE

ROZPOCZĘTO: *15.01.2020 r.*

ZAKOŃCZONO: .....

WARSZAWA

OBOWIĄZKI
Inspektora Ochrony Danych Osobowych *(w skrócie I ODO)*

Nowelizacja „starej" ustawy o ochronie danych osobowych, wprowadzona w 2015 roku miała przygotować Administratorów Danych Osobowych do RODO. Wprowadziła nową, niż dotychczasowa, rolę Administratora Bezpieczeństwa Informacji. Generalny Inspektor Ochrony Danych w wypowiedziach związanych z nowelizacją przepisów, podkreślał, że zmiany mają przygotować przedsiębiorców na projektowane Rozporządzenie o ochronie danych (R ODO).

Rolę i obowiązki ABI określono w rozdziale (Zabezpieczenie danych osobowych) „starej" ustawy o ochronie danych osobowych ***(Dz. U. 2016 poz. 922).***

Wśród obowiązków ABI było zapewnienie przestrzegania przepisów o ochronie danych osobowych, w szczególności poprzez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora danych,

b) nadzorowanie opracowania i aktualizowania dokumentacji oraz przestrzegania zasad w niej określonych,

c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

a także prowadzenie „Rejestru zbiorów danych" przetwarzanych przez Administratora Danych Osobowych. Sposób realizacji obowiązków ABI określały dwa Rozporządzenia wykonawcze do ustawy:

- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez Administratora bezpieczeństwa informacji
- Rozporządzenie Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez Administratora bezpieczeństwa informacji rejestru zbiorów danych

Jednocześnie ustawa dawała możliwość powierzenia ABI innych obowiązków, jeżeli nie naruszy to prawidłowego realizowania przez niego swoich głównych zadań, związanych z nadzorem nad zgodnością przetwarzania danych.

Mówiąc krótko, dotychczasowe przepisy dosyć szczegółowo określały zakres obowiązków ABI.

Jak wyglądają obowiązki nowego ABI, czyli Inspektora Ochrony Danych w świetle przepisów R ODO?

Zadania IOD zostały określone w artykule 39 R ODO:

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;
e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

Warto zwrócić uwagę, na punkt c, tzn.: udzielanie zaleceń **na żądanie ADO**. RODO w wielu miejscach podkreśla, że to Administrator danych jest odpowiedzialny za zapewnienie realizacji obowiązków właściwego przetwarzania danych osobowych:

Administrator oraz podmiot przetwarzający zapewniają, by Inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych (art. 38 ust. 3).

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 (art. 38 ust. 2).

To Administrator Danych Osobowych przeprowadza analizę ryzyka oraz ocenę skutków. I ODO jest włączany w te czynności na żądanie ADO. W praktyce oznacza to, że już na etapie określania zakresu obowiązków I ODO, Administrator danych powinien rozważyć, czy nie wpisać zaleceń co do oceny skutków do zakresu obowiązków I ODO. W końcu to I ODO jest profesjonalistą, który ma wspierać Administratora danych w jego działaniach i to on ma najlepszą wiedzę, jak postępować. Sam Administrator może nawet nie wiedzieć (co nie zwalnia go z odpowiedzialności) o tym, że I ODO włącza się w pewne działania, tylko na żądanie.

Drugim istotnym aspektem jest **właściwe i niezwłoczne włączanie** Inspektora w procesy przetwarzania. Nie wystarczy wpisać w obowiązki Inspektora, że ma monitorować i dawać zalecenia w sprawach związanych z ochroną danych osobowych. Należy dać mu odpowiednie „narzędzia" lub stworzyć odpowiednie procedury, aby był on automatycznie we wszystko włączany. Dobrym rozwiązaniem jest umieszczenie I ODO w łańcuchu akceptacji projektów/czynności. Jeżeli dotychczas wystarczyła akceptacja przełożonego, to zgodnie z nową procedurą powinno być także konieczne uzyskanie akceptacji I ODO. Oczywiście procedura powinna być rozsądna, tzn.: dotyczyć nowych projektów i czynności, a nie powtarzalnych działań, dla których zostały już przyjęte działające rozwiązania. Jeżeli Administrator danych nie zadba o odpowiednie włączenie Inspektora w sprawy związane z przetwarzaniem danych, nie można wymagać od Inspektora, aby sprawował skutecznie nadzór.

Poprzez informowanie, o którym mowa w punkcie „a", można w szczególności rozumieć wprowadzenie w zasady zachowania poufności obowiązujące w firmie, w tym odebranie „Oświadczenia…" o zachowaniu poufności (lub podpisanie umowy o zachowaniu poufności). Inspektor Ochrony Danych Osobowych powinien być jedną z pierwszych osób, z którą styka się nowy pracownik, dzięki czemu w jego świadomości pozostanie skojarzenie, że w Polskich Drużynach Strzeleckich (PDS) jest ktoś odpowiedzialny za nadzór nad bezpieczeństwem danych, do kogo można zwrócić się ze wszystkimi pytaniami i problemami w tej sprawie.

Spotkać się można wielokrotnie z tym, że pracownicy nie wiedzą, że jest w ich Firmie ktoś odpowiedzialny za nadzór.

Ważnym obowiązkiem jest przygotowywanie zaleceń działań, do procesów przetwarzania, o których I ODO ma wiedzę. Tutaj należy podkreślić, że Inspektor nie powinien czekać na „specjalne zaproszenie / oficjalne włączenie" do procesu przetwarzania, o którym ma wiedzę. Jeżeli przebywa w organizacji, rozmawia z pracownikami, to bardzo szybko dowiaduje się, o pewnych działaniach, które mają miejsce w Firmie. Jego obowiązkiem w takiej sytuacji jest zgłaszanie Administratorowi danych wszelkich nieprawidłowości i ryzyka, a także zaleć w celu ich naprawy lub minimalizacji ryzyka.

Inspektor Ochrony Danych nie jest wykonawcą swoich zaleceń.

Wielu Administratorów danych, oczekuje, że I ODO będzie multifunkcyjny, tzn.: znajdzie problem, rozwiąże go, a następnie jeszcze zrobi audyt, aby potwierdzić, że jego praca była skuteczna. Jeżeli I ODO sam ma wykonywać swoje zalecenia lub doprowadzać do ich realizacji, to nadzorowanie, czy proces jest zgodny z przepisami RODO stanowi konflikt interesów. Obowiązkiem I ODO nie jest wdrażanie rozwiązań. Obowiązkiem I ODO jest dawanie zaleceń oraz nadzór nad ich realizacją. W szczególności może proponować konkretne procedury i zmiany w dokumentacji.

Najważniejszym obowiązkiem jest przeprowadzanie audytów (czyli monitorowanie, o którym mowa w punkcie b). RODO nie daje konkretnych wytycznych, w jaki sposób Inspektor ma monitorować przestrzeganie. W szczególności nic nie stoi na przeszkodzie, żeby robił to metodami, które stosował dotychczasowy ABI, w oparciu o przepisy *Rozporządzenia Ministra Administracji i Cyfryzacji z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych...*

W tej konkretnej sytuacji, jak „monitorowanie" będzie także wiązało się z oceną ryzyka naruszenia praw i wolności osób, których dane dotyczą. Jeżeli I ODO ma wspierać Administratora oraz dawać mu zalecenia, to powinien w szczególności być w stanie określić stopień ryzyka.

Rolą Inspektora w organizacji jest także dbanie o świadomość pracowników w zakresie prawidłowego przetwarzania danych, zgodnie z przepisami. Tutaj należy zwrócić uwagę na ogromną ilość „absurdów dookoła RODO" oraz to, że prawidłowa edukacja personelu jest bardzo ważna. Nie wystarczy, że Inspektor będzie cytował przepisy, musi być w stanie także przełożyć je na praktykę. Nie wystarczy powiedzieć „musicie zabezpieczyć dane wysyłane e-mailem", należy pokazać jak to robić. Rolą Inspektora jest przekładanie przepisów na ludzki język i podnoszenie świadomości pracowników, prowadzące do skutecznych i właściwych działań po ich stronie.

Inspektor jest punktem kontaktowym dla Komendanta PDS oraz osób, których dane dotyczą. Jest to bardzo dobre rozwiązanie. Po pierwsze przyśpieszy odpowiedzi na ewentualne pytania, czy żądania, po drugie gwarantuje Administratorowi, że będą realizowane właściwe czynności (w końcu I ODO jest specjalistą).

Podsumowując, oto lista obowiązków I ODO:

1. Monitorowanie przestrzegania przepisów o ochronie danych osobowych oraz wewnętrznych dokumentów, procedur w Polskich Drużynach Strzeleckich i zaleceń dla przetwarzania danych, a także bieżące informowanie kierownictwa o wnioskach.
2. Przeprowadzanie audytów zgodności przetwarzania danych osobowych z przepisami oraz opracowywanie sprawozdań i zaleceń dla kierownictwa.

3. Informowanie pracowników oraz współpracowników o ich obowiązkach wynikających z przepisów o ochronie danych oraz przyjmowanie od nich „OŚWIADCZENIA…" o zachowaniu poufności.
4. Informowanie kierownictwa o obowiązkach wynikających z przepisów o ochronie danych, w tym aktywne doradzanie, jakie działania powinny być podejmowane.
5. Przeprowadzanie analizy ryzyka i zagrożeń oraz przedstawianie wniosków i zaleceń kierownictwu.
6. W przypadku konieczności przeprowadzania oceny skutków, aktywne wspieranie kierownictwa w jej realizacji.
7. Organizowanie szkoleń wstępnych i okresowych z ochrony danych osobowych.
8. Bieżące doradzanie oraz podnoszenie świadomości osób przetwarzających danych, dla których Administratorem jest Komendant Polskich Drużyn Strzeleckich lub które zostały jej powierzone.
9. Doradzanie w kwestiach związanych z powierzeniem danych.
10. Pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, w tym przygotowywanie odpowiedzi na ich żądanie i udzielanie odpowiedzi.
11. Wsparcie Administratora oraz pracowników w realizacji żądań osób, których dane dotyczą.
12. Monitorowanie udostępnień danych osobowych, w tym wydawanie opinii w zakresie realizacji wniosku o udostępnienie.
13. Pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych
14. Aktywne wsparcie kierownictwa w przypadku naruszenia poufności poprzez przygotowanie odpowiednich zaleceń działań, określenie poziomu ryzyka dla naruszenia praw i wolności, przeprowadzenie audytu, wsparcie przy zgłoszeniu naruszenia oraz udzielaniu wyjaśnień z tym związanych.
15. Aktywne włączenie się we wszelkie sprawy związane z przetwarzaniem danych osobowych.
16. Nadzór nad aktualnością dokumentacji i wewnętrznych procedur zarządzania bezpieczeństwem danych osobowych, w tym proponowanie nowych procedur.

Opracowano na podstawie tekstu Sylwii CZUB-KIEŁCZEWSKEJ, specjalisty ds. ochrony danych osobowych certyfikowanego audytora wewnętrznego ISO 27001

Warszawa, dnia 15. 01. 2020 r.

Wykonano w 1 Egz.
- do powielenia w ilości egzemplarzy – wg potrzeb.

OBOWIĄZKI

Inspektora Ochrony Danych…

zawierają 6

(sześć) stron
(słownie)

ponumerowanych.

Warszawa, 15.01.2020 r.
(Miejscowość i data)