Administrator bezpieczeństwa informacji, urzędnik do spraw ochrony danych osobowych, inspektor ochrony danych – analiza porównawcza

dr Grzegorz Sibiga

Dyrektywa 95/46/WE – „urzędnik ds. ochrony danych osobowych" *(data protection official)*

1) Możliwość dla państwa członkowskiego
2) Status: „całkowicie niezależny" sposób wykonywania funkcji

3) Zadania:

- zapewnienie (…) stosowania krajowych przepisów przyjętych na podstawie niniejszej dyrektywy,

- prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych („uproszczona rejestracja")

- przeprowadzanie kontroli wstępnej, współpracując z organem nadzoru.

4) **Źródła prawa**: motywy 49 i 54 preambuły, art. 18 i 20 dyrektywy 95/46/WE

Dyrektywa 95/46/WE - "urzędnik ds. ochrony danych osobowych" *(data protection official)*

Notyfikacja

18.2 Państwa członkowskie mogą wprowadzić uproszczenie procedury lub zwolnienie z obowiązku powiadomienia tylko w następujących sytuacjach oraz na następujących warunkach:

(…)

- jeżeli administrator danych, zgodnie z dotyczącymi go przepisami krajowymi, powoła **urzędnika do spraw ochrony danych osobowych**, odpowiedzialnego w szczególności:
  - za zapewnienie w niezależny sposób wewnętrznego stosowania krajowych przepisów przyjętych na podstawie niniejszej dyrektywy,
  - za prowadzenie rejestru operacji przetwarzania danych wykonywanych przez administratora danych i zawierających informacje, o których mowa w art. 21 ust. 2, zapewniając przy tym, że nie zostaną naruszone prawa i wolności osób, których dane dotyczą.

Dyrektywa 95/46/WE - "urzędnik ds. ochrony danych osobowych"
(data protection official)

Artykuł 20 Dyrektywy:

1) Państwa Członkowskie definiują operacje przetwarzania danych mogące stwarzać określone zagrożenia dla praw i wolności osób, których dane dotyczą oraz kontrolują, czy dane te są badane przed ich rozpoczęciem.

2) Kontrole wstępne są przeprowadzane przez organ nadzorczy po przyjęciu od administratora danych lub urzędnika odpowiedzialnego za ochronę danych zawiadomienia, którzy w razie wątpliwości powinni zasięgać opinii organu nadzorczego.

(…)

POLSKIE PRZEPISY O OCHRONIE DANYCH OSOBPOWYCH - STAN PRAWNY SPRZED 1.5.2004 r.

Podstawa prawna:

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz.U. Nr 80, poz. 521)

ABI – wyznaczona przez ADO osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznym, w tym w szczególności za przeciwdziałanie dostępowi osób niepowołanych do systemu, w którym przetwarzane sa dane osobowe, oraz za podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń (§3).

STAN PRAWNY SPRZED 1.5.2004 r.

W przypadkach naruszenia ochrony danych osobowych osoba przetwarzająca te dane była zobligowana niezwłocznie powiadomić o tym administratora bezpieczeństwa informacji lub inna upoważniona przez niego osobę (§6 ust.3).

Oprócz tego administrator bezpieczeństwa informacji był odpowiedzialny za właściwy nadzór nad funkcjonowaniem mechanizmów uwierzytelnienia użytkownika w systemie informatycznym oraz kontroli dostępu w nim do danych osobowych (§ 14 ust.2).

Administrator bezpieczeństwa informacji (obecny stan aktualny)

Administrator danych wyznacza administratora bezpieczeństwa informacji nadzorującego przestrzeganie zasad ochrony, o których mowa w art. 36 ust.1 (bezpieczeństwo techniczne i organizacyjne), chyba że sam wykonuje te czynności (**art. 36 ust.3** u.o.d.o.)

Administrator bezpieczeństwa informacji – podstawowe problemy

Status i zadania ABI

- Forma wyznaczenia
- Charakter obowiązków ABI
- Usytuowanie w strukturze organizacyjne

Niejednolitość w skali kraju wykonywania funkcji ABI

Projekt rozporządzenia Parlamentu Europejskiego i Rady - ogólne rozporządzenie o ochronie danych (art. 35-37)

1) Zakres obowiązku wyznaczenia inspektora ochrony danych. Wymogi kwalifikacyjne wobec inspektora.

2) Status inspektora ochrony danych

3) Zadania inspektora ochrony danych

Projekt rozporządzenia Parlamentu Europejskiego i Rady - ogólne rozporządzenie o ochronie danych (art. 35-37)

1) Zakres obowiązku wyznaczenia inspektora ochrony danych.

a) przetwarzania dokonuje organ lub podmiot publiczny; lub

b) przetwarzania dokonuje przedsiębiorstwo zatrudniające 250 osób lub więcej; lub

c) główna działalność administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania podmiotów danych

2) Inspektor dla grupy administratorów

Projekt rozporządzenia Parlamentu Europejskiego i Rady - ogólne rozporządzenie o ochronie danych (art. 35-37)

Wyznaczenia inspektora ochrony danych

- Wymóg kwalifikacji zawodowych oraz w szczególności jego wiedzy specjalistycznej z zakresu prawa ochrony danych, praktyki i zdolności do wykonywania jego zadań.
- Inne obowiązki zawodowe inspektora ochrony danych muszą być zgodne z zadaniami i obowiązkami tej osoby jako inspektora ochrony danych i by nie skutkowały one konfliktem interesów.
- Kadencyjność inspektora (co najmniej 2 lata). Inspektora ochrony danych można odwołać w czasie trwania kadencji jedynie wtedy, gdy przestał spełniać warunki niezbędne do pełnienia przez niego obowiązków.
- Podstawa - zatrudnienie lub wykonywanie zadań na podstawie umowy o świadczenie usług.
- Niezależność wykonywania zadań (brak możliwości otrzymywania poleceń dotyczących pełnienia swojej funkcji). Inspektor ochrony danych podlega bezpośrednio kierownictwu administratora lub podmiotu przetwarzającego
- Zapewnienie przez ADO personelu, pomieszczeń, sprzętu i zasobów niezbędnych do wykonywania obowiązków i zadań inspektorów

Projekt rozporządzenia - zadania

- informowanie administratora lub podmiotu przetwarzającego o ich obowiązkach wynikających z niniejszego rozporządzenia oraz dokumentowanie tej działalności i uzyskiwanych odpowiedzi;
- monitorowanie wykonania i stosowania polityk administratora lub podmiotu przetwarzającego w zakresie ochrony danych osobowych, w tym przydział obowiązków, szkolenie personelu zaangażowanego w operacje przetwarzania oraz powiązane kontrole;
- monitorowanie wykonania i stosowania niniejszego rozporządzenia, w szczególności jeśli chodzi o wymogi dotyczące uwzględnienia ochrony danych już w fazie projektowania, ochrony danych jako opcji domyślnej i bezpieczeństwa danych oraz informowania podmiotów danych, a także wniosków w ramach wykonywania praw przysługujących im na mocy niniejszego rozporządzenia.
- zapewnienie prowadzenia dokumentacji, o której mowa w art. 28;
- monitorowanie dokumentacji, zgłoszeń i zawiadomień dotyczących naruszeń ochrony danych osobowych na mocy art. 31 i 32;
- monitorowanie przeprowadzenia oceny skutków w zakresie ochrony danych przez administratora lub podmiot przetwarzający oraz wniosków o uprzednie zezwolenie lub uprzednią konsultację, jeśli są one wymagane na mocy art. 33 i art. 34;
- monitorowanie odpowiedzi na wnioski organów nadzorczych oraz, w ramach kompetencji inspektora ochrony danych, współpraca z organem nadzorczym na wniosek tego organu lub z inicjatywy inspektora ochrony danych;
- pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem oraz zasięganie opinii organu nadzorczego, w odpowiednich przypadkach, z inicjatywy inspektora ochrony danych.

Dziękuję za uwagę.

gsibiga@inp.pan.pl