Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Nowe obowiązki zabezpieczenia danych osobowych po nowelizacji ustawy o ochronie danych osobowych – fakty i mity

Maciej Byczkowski

Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Zmiana obowiązków zabezpieczania danych osobowych

- Nowelizacja ustawy o ochronie danych osobowych z 7 listopada 2014 r. zmieniła obowiązki wykonywania nadzoru nad przestrzeganiem zasad ochrony danych osobowych:
  - Zmiana w rozdziale V „Zabezpieczenie danych osobowych”
  - Dodanie Art. 36a i 36b
- Nowe obowiązki dotyczące zapewniania przestrzegania przepisów o ochronie danych osobowych musi realizować każdy ADO oraz procesor.

Nowe obowiązki zabezpieczania danych osobowych

- Zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:
  - sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych *oraz opracowanie w tym zakresie sprawozdania dla administratora danych*
  - nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,
  - zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych.

Zabezpieczenie danych osobowych

Wymóg: Art. 36 ust. 1

- Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do:
  - zagrożeń
  - kategorii danych objętych ochroną

Zabezpieczenie danych osobowych

Wymóg: Art. 36 ust. 1

- Administrator danych w szczególności powinien zabezpieczyć dane przed:
  - ich udostępnieniem osobom nieupoważnionym,
  - zabraniem przez osobę nieuprawnioną,
  - przetwarzaniem z naruszeniem ustawy
  - zmianą, utratą, uszkodzeniem lub zniszczeniem.

Zabezpieczenie danych osobowych

Wymóg: Art. 36 ust. 2

- Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w art. 36 ust. 1 (techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych)

Realizacja nowych obowiązków zabezpieczania danych osobowych

- ADO ma wybór dotyczący sposobu realizacji nowych obowiązków:
  - Albo powoła do tego ABI na niezależnym stanowisku (zgodnie z art. 36a)
  - Albo sam będzie realizował te obowiązki – wyznaczając do tego inne osoby (zgodnie z art. 36b)
- ADO, który powoła ABI jest zwolnieny z obowiązku zgłaszania zbiorów do rejestracji GIODO (z wyjątkiem zbiorów danych wrażliwych)
- Ustawa wprowadza nowy status ABI, w tym niezależność jego stanowiska.

Realizacja nowych obowiązków bez powołania ABI

- Wybór wariantu zapewniania przestrzegania przepisów o ochronie danych bez powołania ABI nie oznacza obniżenia wymagań związanych z ochroną przetwarzanych danych osobowych.
- Nowe zadania powinny być prawidłowo realizowane, co wymaga zorganizowanego i uporządkowanego podejścia ze strony administratora danych lub procesora.

Nowy status ABI od 2015 r.

- Powołanie ABI (art. 36a ust. 1)
- Zakres zadań ABI (art. 36a ust. 2)
- Wymagane kwalifikacje do pełnienia funkcji ABI (art. 36a ust. 5)
- Zapewnienie niezależności stanowiska ABI (art. 36a ust. 7 i 8)
- Rejestracja ABI przez GIODO (art. 46b)
- Rola ABI w kontroli GIODO (art. 19b)

Okres przejściowy na powołanie ABI – fakty i mity

- Dotyczy “starych” ABI
- ABI wyznaczony przed 1 stycznia 2015 r., na podstawie uchylonego art. 36 ust. 3, pełni swoją funkcję w rozumieniu art. 36a ust. 1, do czasu zgłoszenia go do rejestracji, **nie dłużej jednak niż do dnia 30 czerwca 2015 r.**
- Po 30 czerwca ABI można powołać w dowolnym momencie.
- GIODO nie nakłada kar za brak powołania ABI czy brak jego zgłoszenia do rejestracji do 30.06.15

Nowy status ABI - mity

- Nowelizacja wprowadza obowiązek powołania ABI przez każdego ADO
- 30 czerwca 2015 r. to ostateczny termin zgłoszenia ABI do rejestracji GIODO
- Ryzyko grzywny 200 tys. pln za brak zgłoszenia ABI do rejestracji do 30.06.15 (lub zbiorów danych…)
- Aby móc pełnić funkcję ABI, trzeba posiadać odpowiedni certyfikat potwierdzający kwalifikacje zawodowe. Certyfikat taki jest wymagany przez GIODO przy rejestracji ABI

Nowy status ABI - mity

- Sprawozdania ze sprawdzeń zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych wykonywanych okresowo przez ABI dla ADO muszą być wysyłane obowiązkowo co roku do GIODO
- GIODO może nakazać każdemu ADO wykonanie sprawdzenia zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych w trybie art. 19b

Akcje propagujące mity

"Do Szanownej Dyrekcji,

Zgodnie z nowelizacją ustawy o ochronie danych z 2015 r., podmioty, które przetwarzają dane podlegające zgłoszeniu do GIODO (np. zbiory Klientów) są zobowiązane do zgłoszenia ABI - Administratora Bezpieczeństwa Informacji do GIODO nie później niż do 30 czerwca 2015 roku lub pozostania przy rejestracji zbiorów.

Kary grzywien za niewykonanie decyzji administracyjnych związanych z przetwarzaniem danych wynoszą do 50 tys. dla os. fizycznych i do 200 tys zł dla os. prawnych.

Poniżej proponujemy Państwu warianty wdrożeń systemu ochrony danych - od wzorów do kompleksowego audytu z wdrożeniem i szkoleniem." (cytat z e-maila)

Akcje propagujące mity

Zaproszenie na szkolenie:

"Nowy Obowiązek Prawny w każdej firmie i urzędzie!

Administrator Bezpieczeństwa Informacji

Jak spełnić nowe wymogi w nieprzekraczalnym terminie do 30.06.2015?"

(zaproszenie od Forum Media Polska)

Akcje propagujące mity

"Uwaga! Do 30.06.2015 trzeba wdrożyć nowe procedury dotyczące ochrony danych osobowych i wyznaczyć ABI. W przypadku uchybień to szef firmy ponosi odpowiedzialność!

Do 30 czerwca 2015 każdy szef firmy musi:

- *powołać i zgłosić ABI do GIODO, zgodnie z najnowszymi zmianami ustawy o ochronie danych osobowych z 2015 r., nawet jeżeli zatrudniasz 1 pracownika, a w bazie firmy przechowywane są tylko dane klientów w celu wystawienia faktury,*
- *w ciągu 2 miesięcy przeprowadzić audyt bezpieczeństwa informacji w firmie, by sprawdzić, które obszary ochrony danych trzeba natychmiast poprawić,*
- *przygotować się do kontroli GIODO zapowiedzianych na konferencji z dnia 28.01.2015 – za nieprzestrzeganie przepisów grozi kara grzywny 200 000 zł lub pozbawienie wolności do 2 lat*

Z naszym szkoleniem, które uwzględnia wytyczne nowych rozporządzeń do ustawy, szybko wychwycisz wszelkie uchybienia i zagwarantujesz pełną ochronę danych osobowych"

Mity na stronach www

<u>Przykładowe cytaty ze stron www</u>:

- *"JUŻ 30 CZERWCA 2015 ROKU MIJA TERMIN REJESTRACJI ABI DO GIODO" (www.rbdo.com.pl)*
- *"Przed nowelizacją informowaliśmy GIODO o zamiarze powierzenia danych osobowych do swoich kontrahentów, aktualnie będziemy musieli ich wskazać do GIODO i przeprowadzić u nich kontrole zakończone pisemnym raportem (tak wynika z projektu rozporządzenia)" (www.fundacjapb.pl)*

Nowe rozporządzenia wykonawcze

- Rozporządzenie MAiC z 10 grudnia 2014 r. w sprawie wzoru zgłoszenia powołania i odwołania administratora bezpieczeństwa informacji do rejestracji Generalnemu Inspektorowi Ochrony Danych Osobowych (Dz. U. 2014, poz. 1934)
- Rozporządzenie MAiC z 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji (Dz. U. 2015, poz. 719)
- Rozporządzenie MAiC z 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych osobowych (Dz. U. 2015, poz. 745)

Korzyści dla ADO z powołania ABI

- Zapewnienie przestrzegania przepisów o ochronie danych osobowych:
  - Przez właściwie przygotowaną do tego osobę
  - W uporządkowany sposób, w tym: nadzór nad dokumentacją, wykonywanie sprawdzeń, minimalizacja ryzyk, zapoznawanie osób z przepisami.
- Uproszczona procedura rejestracji zbiorów danych – zgłoszenie zbiorów do ABI
- Uproszczona forma kontroli przez GIODO - sprawdzenie realizowane przez ABI
- Przygotowanie do realizacji wymagań nowego Rozporządzenia PE i Rady:
  - Nowa funkcja Inspektora ochrony danych (DPO)