Propozycje SABI w zakresie doprecyzowania statusu ABI

Maciej Byczkowski, Grzegorz Sibiga, Stefan Szyszko

Warszawa 10.10.2011

Projekt SABI – proponowany zakres zmian

- Status ABI
- Rejestracja zbiorów danych osobowych
- Zasady przeprowadzenia kontroli

- Pytania i wątpliwości

Propozycja zmian Statusu ABI – Projekt SABI

- **Punkty kierunkowe:**
  - **Powołanie ABI**
  - **Niezależne stanowisko i możliwość wykonywania obowiązków**
  - **Kwalifikacje ABI**
  - **Zakres obowiązków ABI**
  - **Korzyści dla ADO z wyznaczenia ABI**

Powołanie ABI

- Administrator danych osobowych powołuje ABI, chyba że sam wykonuje zadania, określone w ustawie
- Administrator danych może powołać zastępcę ABI, który spełnia określone w ustawie warunki (kwalifikacje)

Niezależność stanowiska

- ABI podlega bezpośrednio kierownikowi jednostki organizacyjnej, który zapewnia:
  - niezbędne środki do wykonywania zadań
  - organizacyjną odrębność ABI w niezależnym wykonywaniu zadań, określonych w przepisach o ochronie danych osobowych.

Zgłaszanie ABI do GIODO

- Administrator danych zawiadamia GIODO o:
  - powołaniu ABI,
  - odwołaniu ABI wraz z podaniem przyczyn takiego odwołania
- GIODO prowadzi ogólnokrajowy, jawny rejestr ABI
- Kompetencja do wykreślenia ABI z rejestru, gdy powołanie lub działalność narusza ustawowe zasady (wówczas ADO nie może korzystać z korzyści związanych z powołaniem ABI)

Zadania ABI

- Przeprowadzanie kontroli przestrzegania przepisów o ochronie danych osobowych w jednostce organizacyjnej oraz opracowanie w tym zakresie sprawozdania dla administratora danych
- Zapewnienie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust.2, oraz nadzorowanie przestrzegania zasad w niej określonych

Zadania ABI

- Prowadzenie rejestru zbiorów danych przetwarzanych w jednostce organizacyjnej
- Zaznajamianie osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych
- ADO może powierzyć ABI wykonywanie innych zadań, które nie naruszałyby prawidłowego wykonywania jego obowiązków, określonych w ustawie

Kwalifikacje ABI

- ABI może być osoba, która:
  - ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych
  - posiada wykształcenie wyższe
  - posiada odpowiednią wiedzę z zakresu ochrony danych osobowych
  - nie była karana za przestępstwo popełnione z winy umyślnej

Propozycja zmian w zakresie rejestracji zbiorów

- Uproszczona rejestracja – prowadzenie własnego, wewnętrznego rejestru zbiorów danych przez ABI, powoduje zwolnienie z obowiązku zgłoszenia zbioru do GIODO
- Udział ABI w kontroli wstępnej zbiorów danych zawierających dane wrażliwe
- Konsekwencje wykreślenia ABI z rejestru prowadzonego przez GIODO

Rejestracja

- Administrator danych, który powołał ABI jest zwolniony ze zgłoszenia do rejestracji/aktualizacji swoich zbiorów (za wyjątkiem zbiorów danych wrażliwych)
- W przypadku zgłoszenia zbiorów danych, pozytywna opinia ABI umożliwia rozpoczęcie przetwarzania danych bez potrzeby rejestracji przez GIODO

Propozycja zmian w zakresie przeprowadzania kontroli

- Założenie: ABI jako niezależny kontroler wewnętrzny może przejąć zadania kontrolne GIODO, bez ograniczania kompetencji samego organu ochrony danych osobowych

Przeprowadzenie kontroli

- Jeżeli nie sprzeciwia się to celowi kontroli, GIODO może odstąpić od czynności kontrolnych, o których mowa w art. 14-16 i zwrócić się do ABI (zgłoszonego do rejestru GIODO) o przeprowadzenie kontroli w określonym terminie.
- Po przeprowadzeniu kontroli ABI przedstawia GIODO sprawozdanie
- Przeprowadzenie kontroli przez ABI nie wyłącza prawa GIODO do późniejszej kontroli

Korzyści dla ADO z wyznaczenia ABI

- Uproszczona procedura rejestracji zbiorów danych – ich zgłaszanie do ABI, zamiast do GIODO
- Zwolnienie z procedury uprzedniej kontroli przy rejestracji zbiorów z danymi wrażliwymi
- Uproszczona forma kontroli przez GIODO

Zmiany rozdziału 5 Ustawy ODO - zabezpieczenia

- Określanie zabezpieczeń w odniesieniu do ryzyka przetwarzania danych
- Dokumentacja – rejestr operacji na danych
- ABI – ustalenie statusu
- Kwestie upoważnienia do przetwarzania danych - zakres i forma nadania
- Określenie kontroli – art. 38
- Delegacja do Rozporządzenia

Przewidywane zmiany dot. ABI w Dyrektywie 96/46/WE wskutek jej nowelizacji

- Wzmocnienie roli ABI – wzorem większości państw, gdzie funkcja ta została wprowadzona:
  - ABI OCENIANY JEST JAKO POZYTYWNIE WPŁYWAJĄCY NA POZIOM ODO
- Dodatkowe gwarancje dla niezależności sprawowania funkcji ABI
- Doprecyzowanie wymagań, jakie musi spełniać osoba pełniąca funkcję ABI
- Doprecyzowanie zasad współpracy z organem nadzoru

WĄTPLIWOŚCI I WYZWANIA

- **ZJAWISKA OBIEKTYWNE:**
  - Wzrost komplikacji przepływów danych w dużych organizacjach
  - Wzrost komplikacji zasad współpracy z mechanizmami kontroli, audytu, *compliance*, IT, bezpieczeństwa teleinformatycznego, etc. w dużych organizacjach
  - Systematyczny wzrost delegowania istotnych części przetwarzania danych do podmiotów zewn.:
    - **Wyzwania ze strony modelu usługowego CLOUD COMPUTING**
  - Dodatkowe zadania nakładane na ADO w związku z Programem / Polityką Ochrony Cyberprzetrzeni

PYTANIA O REALIZACJĘ ZADAŃ ABI

- Jakie zadanie mogą być faktycznie zrealizowane przez ABI:
  - Zadania nadzorcze?
  - Zadania o charakterze wykonawczym?
  - Czy w ogóle zasadny i racjonalny jest model ABI, niezależny od wielkości organizacji?
- ZASOBY !!!
  - Bez zagwarantowania zasobów: syndrom ODPOWIEDZIALNOŚCI BEZ WŁADZY
  - Konieczność zagwarantowania synchronizacji listy zadań z przyznanymi zasobami
- KORELACJA Z INNYMI FUNKCJAMI O PODOBNYM CHARAKTERZE W DUŻYCH ORGANIZACJACH:
  - Information Security Officer z norm ISO-27000
  - Pełnomocnik Ochrony Informacji Niejawnych
  - Administrator (?) ds. Ochrony Cyberprzestrzeni

Dziękujemy za uwagę

Dyskusja