

Zarządzanie bezpieczeństwem danych osobowych

- Praktyka wykonywania zadań ABI oraz konieczne zmiany statusu ABI i wymagań dotyczących bezpieczeństwa danych

Maciej Byczkowski

Agenda

- ❖ **Działania SABI w sprawie zmiany statusu ABI**
- ❖ **Praktyka wykonywania zadań ABI:**
 - **Miejsce w strukturze organizacyjnej**
 - **Zakres kompetencji i uprawnień**
 - **Zakres zadań i obowiązków ABI**
- ❖ **Konieczne zmiany dotyczące zabezpieczenia danych osobowych**

Cel działań SABI związany ze zmianą statusu ABI

- ❖ **Podniesienie statusu zawodowego ABI**
- ❖ **Stworzenie Kodeksu Etyki zawodowej ABI**
- ❖ **Umożliwienie rozwoju zawodowego i podnoszenia kwalifikacji ABI**
- ❖ **Zwiększenie roli kontrolnej ABI w polskich organizacjach – ranga i ważność stanowiska**
- ❖ **Zapewnienie skutecznej realizacji ochrony danych wewnątrz organizacji**
- ❖ **Poprawa skuteczności ochrony danych osobowych w Polsce**

Wykonane działania SABI

- ❖ **Stworzenie Kodeksu Etyki Zawodowej ABI**
- ❖ **Opracowanie projektu nowelizacji ustawy o ochronie danych osobowych w zakresie zmian statusu ABI**
- ❖ **Przedstawienie projektu na forum sejmowym i rządowym**
- ❖ **Przedstawienie propozycji zmian Statusu ABI w Dyrektywie KE**



Praktyka wykonywania zadań ABI w Polsce

Praktyka ABI – ponad 12 lat doświadczeń

- ❖ **Faktyczny zakres zadań:**
 - **Nadzór zgodnie z ustawą**
 - **Wykonywanie prac związanych z realizacją obowiązków ADO**
 - **Zarządzanie systemem IT**
 - **Inne**

Praktyka wykonywania zadań ABI

- ❖ **Kogo wyznacza się na ABI:**
 - **Dedykowana osoba – niezależne stanowisko**
 - **Stanowisko łączone:**
 - **Dyrektor IT, Administrator systemu IT**
 - **Dyrektor Kadr**
 - **Audytor wewnętrzny – role kontrolne**
 - **Radca prawny**
 - **Stanowiska przypadkowe**
 - **Brak wyznaczenia ABI**

Różnice w wykonywaniu zadań ABI

- ❖ **Specyfika branży lub rodzaju podmiotu**
 - Różne wymagania prawne związane z przetwarzaniem danych
 - Różne cele biznesowe w pozyskiwaniu danych
- ❖ **Podział zadań przy przetwarzaniu danych:**
 - Role zarządcze, wykonawcze i kontrolne
- ❖ **Umiejscowienie ABI w strukturze:**
 - Łączenie stanowisk
 - Samodzielne stanowisko

Różnice w wykonywaniu zadań ABI

- ❖ **Złożoność problemu przetwarzania:**
 - Różne zbiory danych
 - Kanały zbierania danych
 - Akcje marketingowe
 - Powierzanie danych procesorom
 - Udostępnianie danych
- ❖ **Miejsca agregowania danych:**
 - System IT
 - Archiwa papierowe

ABI a inne role kontrolne

- ❖ **ABI nadzorca, kontroler czy audytor?**
- ❖ **ABI a audytor wewnętrzny (SZJ, SZBI, audyt/kontrola wewnętrzna)**
- ❖ **ABI a Pełnomocnik ds. ochrony informacji niejawnych**
- ❖ **ABI a Pełnomocnik ds. bezpieczeństwa informacji**
- ❖ **ABI a Inspektor Bezpieczeństwa Teleinformatycznego**
- ❖ **ABI a IT Security Officer (ABSI)**

Potrzeba określenia miejsca ABI w strukturze organizacji

- ❖ Zapewnienie niezależności
- ❖ Zapewnienie wykonywania zadań nadzoru/audytu przetwarzania danych
- ❖ Miejsce w strukturze - funkcjonalny pion kontrolny
- ❖ Samodzielne stanowisko
 - Lub pion ABI w dużych strukturach
- ❖ Pełnomocnik Zarządu ds. ochrony danych

Potrzeba podziału zadań w zarządzaniu bezpieczeństwem (przykład z Metodyki PBDO – ENSI)



Potrzeba określenia zakresu odpowiedzialności ABI

- ❖ **ABI nadzorca, audytor czy wykonawca?**
- ❖ **Podział roli na ABI i ABSI – w zależności od kompetencji**
- ❖ **Hierarchia ABI – Centrala a oddziały**
- ❖ **Outsourcing ABI**

Potrzeba kompetencji ABI

- ❖ **Propozycja zakresu kompetencji:**
 - **Wiedza dotycząca aspektów prawnych związanych z ochroną informacji**
 - **Umiejętności z zakresu prowadzenia audytu wewnętrznego**
 - **Wiedza z zakresu zarządzania (procesami) – w tym zarządzania ryzykiem**
 - **Wiedza dotycząca funkcjonowania systemu informatycznego**
 - **Umiejętności związane z opracowywaniem dokumentacji**
 - **Umiejętności związane z prowadzeniem szkoleń**

Potrzeba określenia zakresu uprawnień ABI

- ❖ **Możliwość wykonywania nadzoru i audytu w komórkach organizacyjnych przetwarzających dane**
- ❖ **Prawo żądania wglądu w dokumentację dotyczącą przetwarzania danych**
- ❖ **Prawo wglądu do systemu informatycznego przetwarzającego dane**
- ❖ **Prawo wykonywania kontroli u procesorów – zgodnie z umowami powierzenia**

Potrzeba określenia zadań ABl

- ❖ Nadzór nad przestrzeganiem zasad ochrony danych osobowych
- ❖ Przeprowadzanie audytu zgodności przetwarzania danych osobowych z u.o.d.o.
- ❖ Prowadzenie dokumentacji opisującej sposób przetwarzania danych osobowych oraz środki techniczne i organizacyjne zabezpieczenia danych osobowych
- ❖ Prowadzenie lub nadzór nad prowadzeniem ewidencji osób upoważnionych do przetwarzania danych osobowych

Potrzeba określenia zadań ABl

- ❖ Prowadzenie wykazu wszystkich zbiorów danych osobowych
- ❖ Prowadzenie wykazu obszaru przetwarzania danych osobowych
- ❖ Przygotowywanie wniosków zgłoszeniowych zbiorów danych osobowych do rejestracji/aktualizacji GIODO
- ❖ Nadzór nad udostępnianiem i powierzaniem danych osobowych innym podmiotom
 - Wykaz odbiorców i procesorów

Potrzeba określenia zadań ABI

- ❖ Nadzór i audyt zabezpieczeń systemu informatycznego, w którym przetwarzane są dane osobowe (lub współpraca z ABSI)
- ❖ Nadzór nad wykonywaniem obowiązków informacyjnych – klauzule informacyjne i oświadczenia dotyczące zgody
- ❖ Nadzór wykonywania zadań przez inne wyznaczone do zadań nadzorczych osoby np. Lokalnych czy terenowych ABI
- ❖ Podejmowanie działań w sytuacji naruszenia ochrony danych

Potrzeba określenia zadań ABl

- ❖ Przygotowywanie materiałów informacyjnych dla pracowników upoważnionych do przetwarzania danych osobowych
- ❖ Organizowanie/prowadzenie szkoleń dla pracowników z zakresu ochrony danych w organizacji
- ❖ Kontakt z GIODO
 - Przygotowywanie odpowiedzi
 - Udział w czasie kontroli
- ❖ Rozpatrywanie skarg i zapytań od osób w zakresie ochrony danych

Wykonywanie zadań ABI

- ❖ Łączenie problematyki ochrony danych osobowych z ochroną innych rodzajów informacji:
 - Informacje niejawne
 - Tajemnice przedsiębiorstwa
 - Informacje publiczne



Konieczne zmiany dotyczące zabezpieczenia danych osobowych

Zmiany rozdziału 5 ustawy odo - zabezpieczenia

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

Zmiany dotyczące powierzania przetwarzania danych

- ❖ **Ustalenie kwestii zabezpieczenia w zależności od obszaru przetwarzania**
- ❖ **Kontrola procesora przez ADO**
 - Tryb kontroli i uprawnienia ADO
- ❖ **Kwestia podprocesorów**
 - Zgoda ADO
 - Powiadomienie ADO
- ❖ **Kwestia obowiązku wyznaczenia ABI przez procesora**
- ❖ **Wprowadzenie definicji procesora**

Zmiana rozporządzenia

❖ Zmienić:

- Zakres dokumentacji
- Wymogi zabezpieczenie obszaru przetwarzania
- Wymogi zabezpieczenia systemu IT
- Kwestia odnotowywania informacji w systemie informatycznym

❖ Dodać:

- Kwestie wykonywania roli ABI
- Kwestie kontroli (art. 38)
- Kwestia nadawania upoważnień
- Kwestia szkoleń
- Kwestia szacowania ryzyka



Pytania?

www.sabi.org.pl

www.ensi.net