Stowarzyszenie Administratorów Bezpieczeństwa Informacji

ABI nie tylko audytor i koordynator

Wykonywanie przez ABI innych obowiązków niż określone w ustawie o ochronie danych osobowych

Andrzej Rutkowski

Stowarzyszenie Administratorów Bezpieczeństwa Informacji

Agenda

1. Możliwość wykonywania przez ABI innych zadań niż określone w u.o.d.o. jako przedmiot nowelizacji u.o.d.o.
   - funkcja ABI,
   - status ABI.
2. Przesłanki pozwalające na wykonywanie przez ABI innych zadań dotyczących ochrony danych osobowych .
3. Przesłanki pozwalające na wykonywanie przez ABI innych zadań nie dotyczących ochrony danych osobowych.
4. Przykłady innych zadań ABI dotyczących ochrony danych osobowych.
5. Przykłady innych zadań ABI nie dotyczących ochrony danych osobowych.

Funkcja ABI

Administrator Bezpieczeństwa Informacji to funkcja.

Z uzasadnienia do projektu nowelizacji ustawy o ochronie danych osobowych (u.o.d.o.)

- Druk nr 2606 str. 21

„… w ramach proponowanych rozwiązań określony zostaje status ABI, na który składają się: **wymogi stawiane osobie mającej pełnić omawianą funkcję, organizacyjne usytuowanie funkcji** … ,

… Celowo projektowana zmiana unika regulowania kwestii zmierzających do tworzenia nowej grupy zawodowej.”

Status ABI

Nowelizacja u.o.d.o. określiła status ABI.

Z uzasadnienia do projektu nowelizacji u.o.d.o.

- Druk nr 2606 str. 21

„… w ramach proponowanych rozwiązań określony zostaje status ABI, na który składają się: wymogi stawiane osobie mającej pełnić omawianą funkcję, organizacyjne usytuowanie funkcji **oraz dopuszczenie nałożenia na ABI innych zadań niż określone w u.o.d.o.”**

Inne zadania ABI

Administrator danych może powierzyć ABI wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w ust. 2 – art. 36a ust. 3 u.o.d.o.

Możliwość wykonywania innych zadań przez ABI jest częścią składową:

- wykonywania funkcji ABI,
- ustawowego statusu ABI.

Inne zadania ABI

Czy powołanie ABI się opłaca?

Jakie zadania, oprócz określonych w u.o.d.o., może wykonywać ABI?

Przesłanka 1

1. Podstawowym zadaniem ABI jest zapewnienie przestrzegania przepisów o ochronie danych osobowych, ***w szczególności przez***: … – art. 36a ust. 2 pkt 1 u.o.d.o.

ABI już nie jest tylko nadzorcą zasad techniczno – organizacyjnego bezpieczeństwa przetwarzania danych osobowych.

Wypełnianie funkcji ABI to wykonywanie zadań obejmujących wszystkie obszary ochrony danych osobowych.

Przesłanka 2

2. ABI może być osoba, która posiada odpowiednią wiedzę w zakresie ochrony danych osobowych – art. 36a ust. 5 pkt 2.

ADO, w celu obniżenia kosztów funkcjonowania ABI, może/powinien powierzyć mu wykonywanie innych zadań niż określone w u.o.d.o., dotyczących ochrony danych osobowych

Inne zadania ABI - przykłady

1. Prowadzenie szkoleń w zakresie ochrony danych osobowych.
2. Zgłaszanie do rejestru GIODO zbiorów danych osobowych wrażliwych.
3. Przygotowywanie projektów lub opiniowanie projektów umów powierzenia przetwarzania danych.
4. Dokonywanie wstępnej oceny spełniania wymogów ochrony danych przez potencjalnych procesorów.
5. Przygotowywanie projektów klauzul zgody na przetwarzanie danych i klauzul informacyjnych.

Inne zadania ABI - przykłady

6. Przygotowywanie projektów polityki prywatności oraz polityki cookies.
7. Odbieranie oświadczeń o zapoznaniu się osób z przepisami prawa o ochronie danych osobowych oraz innych informacji prawnie chronionych i zobowiązaniu do zachowania tajemnicy tych danych oraz informacji a także ich zabezpieczeń.
8. Wydawanie upoważnień do przetwarzania danych osobowych.
9. Prowadzenie ewidencji osób upoważnionych.

Przesłanka 3

3. Stosowane środki techniczne i organizacyjne powinny zapewnić ochronę przetwarzanych danych odpowiednią do zagrożeń i kategorii danych objętych ochroną – art. 36 ust. 1 u.o.d.o.

3a. Nowelizacja wymogów zabezpieczenia danych wprowadzi wymóg dokonywania udokumentowanej oceny zagrożeń przetwarzania danych osobowych.

ABI może być inicjatorem i uczestniczyć we wdrażaniu zarządzania bezpieczeństwem przetwarzania danych opartego na ocenie ryzyka występującego podczas przetwarzania danych.

Inne zadania ABI - przykłady

Uczestnictwo w:

1. tworzeniu listy procesów służących do zarządzania bezpieczeństwem,
2. identyfikowaniu podatności i zagrożeń występujących w przebiegu poszczególnych procesów,
3. przeprowadzeniu analizy ryzyka,
4. klasyfikacji procesów ze względu na wynik analizy ryzyka,
5. doborze narzędzi postępowania z ryzykiem.

Przesłanka 4

4. Nowelizacja u.o.d.o. jest przygotowaniem do wykonywania nowych wymogów ochrony danych przewidzianych w ogólnym rozporządzeniu o ochronie danych osobowych UE.

ABI może być inicjatorem i uczestniczyć we wdrażaniu:

1) ochrony danych w fazie projektowania,
2) ochrony danych jako opcji domyślnej,
3) procedur zgłaszania i powiadamiania o naruszeniu ochrony danych osobowych,
4) oceny skutków w zakresie ochrony danych osobowych.

Inne zadania ABI - przykłady

1. Opiniowanie potrzeby stosowania wymogów prawa ochrony danych osobowych na etapie projektowania produktu lub usługi.
2. Uczestnictwo w doborze środków ochrony danych na etapie projektowania systemu informatycznego wspomagającego produkt lub świadczenie usługi.
3. Uczestnictwo w opracowywaniu i wdrażaniu zasad i procedur postępowania z incydentami.
4. Uczestnictwo w opracowywaniu i wdrażaniu zasad i procedur zarządzania ciągłością działania lub planów awaryjnego działania.
5. Prowadzenie szkoleń z zakresie planowania ciągłości działania, czy też awaryjnego działania.

Przesłanka 5

5. ABI wykonując ustawowe zadania odnoszące się do dalej idącej ochrony danych osobowych, o której mowa w art. 5 u.o.d.o., ma kompetencje w zakresie ochrony innych informacji prawnie chronionych.

ABI może wykonywać zadania w zakresie np. ochrony tajemnicy przedsiębiorstwa oraz/lub ochrony tajemnicy zawodowej.

Inne zadania ABI - przykłady

1. Uczestnictwo w opracowaniu i wdrożeniu klasyfikacji informacji.
2. Uczestnictwo w opracowaniu i wdrożeniu instrukcji postępowania w dokumentami stanowiącymi tajemnicę przedsiębiorstwa.
3. Przygotowywanie projektów klauzul o poufności.
4. Prowadzenie szkoleń w zakresie ochrony tajemnicy przedsiębiorstwa.

Przesłanka 6

6. Nowelizacja u.o.d.o. poprzez uchwalenie ustawy z 7.11.2014 r. o ułatwieniu wykonywania działalności gospodarczej (Dz. U. z 2014 r. poz. 1662).

ABI poprzez uczestnictwo w budowaniu procesów, zasad oraz procedur służących zarządzaniu bezpieczeństwem może ułatwić wykonywanie działalności gospodarczej ADO.

Przesłanka 7

7. Stanowisko uznanego autora piśmiennictwa w zakresie prawa ochrony danych osobowych.

Po dokonaniu przez ADO oceny w konkretnych okolicznościach faktycznych, wykonywanie funkcji ABI można łączyć z wykonywaniem funkcji administratora systemu informatycznego, zwłaszcza gdy dotyczy to podmiotu działającego w niewielkich strukturach organizacyjnych (Paweł Fajgielski, Pozycja prawna i zadania administratora bezpieczeństwa informacji po nowelizacji ustawy o ochronie danych osobowych, Monitor Prawniczy, 2015 r., nr 6, s. 4-5.)

Inne zadania ABI - wniosek

Wykonywanie innych zadań przez ABI nie musi kolidować z jego odrębnością organizacyjną i niezależnym wykonywaniem zadań ustawowych gdy:

1) wykonywanie innych zadań będzie uczestnictwem ABI jako specjalisty, eksperta w zespołowych przedsięwzięciach, projektach,
2) inne zadania wykonywane przez ABI indywidualnie zostaną poddane audytowi wewnętrznemu.