

Poradnik adresowany jest do osób przygotowujących dokumentację ochrony danych osobowych w organizacji w celu jej późniejszego wdrożenia. W książce przedstawiono od strony praktycznej, krok po kroku tworzenie niezbędnych zapisów, które muszą być umieszczone w treści dokumentacji ochrony danych osobowych na przykładzie trzech organizacji, tj. spółki kapitałowej, podmiotu sektora publicznego oraz jednoosobowej działalności gospodarczej.

Poradnik pozwala uzyskać odpowiedzi na następujące pytania:

- jakie elementy musi zawierać polityka bezpieczeństwa?
- jakie elementy musi zawierać instrukcja zarządzania systemem informatycznym?
- jak powinno wyglądać upoważnienie do przetwarzania danych osobowych?
- jak tworzyć umowy powierzenia przetwarzania danych osobowych?
- jak przygotować wniosek o zgłoszenie zbioru danych osobowych do rejestru GODO?
- jakim dokumentem powołać ABI i jak wypełnić wniosek o jego zgłoszenie?
- jak przygotować plan sprawdzeń oraz sprawozdanie ze sprawdzenia planowego?
- jak przygotować sprawozdanie ze sprawdzenia doraźnego?

Konrad Gałaj-Emiliańczyk

prawnik, administrator bezpieczeństwa informacji, audytor wiodący systemu zarządzania ciągłością działania wg normy PN-EN ISO 22301. Wykładowca licznych konferencji i seminariów, samodzielnie przeprowadził ponad 100 otwartych szkoleń i warsztatów dla administratorów bezpieczeństwa informacji. Zawodowo zajmuje się m.in. kontrolą i audytem w zakresie bezpieczeństwa informacji, tworzeniem wewnętrznych procedur i dokumentacji, oraz sporządzaniem opinii prawnych. Odpowiedzialny za bezpieczeństwo informacji w kilkunastu podmiotach.

Z recenzji Leszka Kępy, eksperta ds. ochrony danych osobowych i bezpieczeństwa informacji:

Jest to kolejna książka z serii, stanowiąca doskonałe uzupełnienie poprzedniej publikacji, poświęconej tworzeniu systemu ochrony danych osobowych. Do tej pory bardzo brakowało jednej publikacji, w której całościowo przedstawia się jakie dokumenty powinny zostać wytworzone w podmiocie przetwarzającym dane osobowe, przez kogo, dla kogo i w jakich przypadkach. Przykłady i wzory zapisów odzwierciedlających najbardziej typowe przypadki przetwarzania danych przez spółkę, gminę i osobę fizyczną prowadzącą działalność gospodarczą, stanowią nieocenioną pomoc przy tworzeniu własnej dokumentacji. Inspiruje nowatorskie podejście do niektórych kwestii takich jak np. dekalogi ochrony danych osobowych. Bez wątplenia jedna z obowiązkowych pozycji.

Spis treści:

Wstęp

Rozdział 1. Dokumentacja ochrony danych osobowych – gromadzenie informacji

Od struktury organizacyjnej
Przez przepisy branżowe
Do gotowej dokumentacji do wdrożenia

Rozdział 2. Zakres wymaganych dokumentów

Polityka bezpieczeństwa przetwarzania danych osobowych
Instrukcja zarządzania systemem informatycznym przetwarzającym dane osobowe
Umowa powierzenia przetwarzania danych osobowych
Zgłoszenie zbioru danych osobowych do rejestru GODO
Zgłoszenie ABI do rejestru GODO
Narzędzia pracy ABI
Praktyczne dokumenty dodatkowe

Rozdział 3. Polityka bezpieczeństwa

Wykaz budynków, pomieszczeń lub części pomieszczeń
Wykaz zbiorów danych osobowych
Opis struktury zbiorów danych osobowych
Sposób przepływu danych pomiędzy poszczególnymi systemami
Niezbędne środki techniczne i organizacyjne

Rozdział 4. Instrukcja zarządzania systemem informatycznym

Procedura nadawania i rejestrowania uprawnień w systemie informatycznym
Metody i środki uwierzytelniania użytkowników
Procedury rozpoczęcia, zawieszenia i zakończenia pracy w systemie informatycznym
Procedury tworzenia kopii zapasowych
Sposób, miejsce i okres przechowywania nośników danych i kopii zapasowych
Sposoby zabezpieczania systemu przed szkodliwym oprogramowaniem
Sposoby rejestracji dostępu odbiorców danych w systemie informatycznym
Procedura wykonywania przeglądów i konserwacji systemu informatycznego

Rozdział 5. Umowy powierzenia przetwarzania danych osobowych oraz umowy o zachowaniu poufności danych

Szablon umowy powierzenia przetwarzania danych osobowych
Dodatkowe zapisy umowne w umowach głównych
Listy kontrolne kierowane do „procesorów” danych osobowych

Rozdział 6. Przygotowanie wniosku o rejestrację zbioru danych w GODO

System e-GIODO a wersja papierowa
Sekcja od A do D
Sekcja od E do F

Rozdział 7. Przygotowanie wniosku o rejestrację ABI w GODO

Warunki pełnienia funkcji ABI
Wypełnianie wniosku i zgłoszenie

Rozdział 8. Narzędzia pracy ABI

Plan sprawdzeń ochrony danych osobowych
Sprawozdanie ze sprawdzenia planowego
Sprawozdanie ze sprawdzenia doraźnego
Rejestr zbiorów prowadzony przez ABI

Rozdział 9. Praktyczne dokumenty dodatkowe

Regulamin ochrony danych osobowych
Dekalogi ochrony danych osobowych W jakich sytuacjach informować ABI?

Rozdział 10. Podsumowanie

Hierarchia dokumentów w organizacji
Weryfikacja zgodności dokumentacji ze stanem faktycznym

Zakończenie