Polityka bezpieczeństwa danych

Kategoria: Aktualności
Opublikowano: sobota, 14, wrzesień 2013 00:00
Barbara Łączna
Odsłony: 1536

Administrator danych obowiązany jest do opracowania w formie pisemnej i wdrożenia polityki bezpieczeństwa. Polityka bezpieczeństwa to zestaw praw, reguł i praktycznych doświadczeń dotyczących sposobu zarządzania, ochrony i dystrybucji danych osobowych wewnątrz określonej organizacji. Polityka bezpieczeństwa powinna odnosić się całościowo do problemu zabezpieczenia danych osobowych u administratora danych tj. zarówno do zabezpieczenia danych przetwarzanych tradycyjnie, jak i danych przetwarzanych w systemach informatycznych. Jej celem jest wskazanie działań, jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować, aby właściwie zabezpieczyć dane osobowe.

Polska Norma PN-ISO/IEC 17799:2005, określająca praktyczne zasady zarządzania bezpieczeństwem informacji w obszarze technik informatycznych, jako cel polityki bezpieczeństwa wskazuje „zapewnienie kierunków działania i wsparcie kierownictwa dla bezpieczeństwa informacji ". Jako minimum w powyższej normie wskazuje się, aby dokument określający politykę bezpieczeństwa zawierał:

- mechanizm umożliwiający współużytkowanie informacji;
- oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań biznesowych;
- strukturę wyznaczania celów stosowania zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem;
- krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, zawierające:

1) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;
2) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;
3) zarządzanie ciągłością działania biznesowego;
4) konsekwencje naruszenia polityki bezpieczeństwa;

- definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;
- odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.

Dokument określający politykę bezpieczeństwa nie może mieć zbyt abstrakcyjnego charakteru. Zasady postępowania w niej wskazane powinny zawierać uzasadnienie wyjaśniające przyjęte standardy i wymagania. Jeżeli ma to miejsce, to rzadziej dochodzi do ich naruszenia.

Dokument w zakresie przedmiotowym powinien koncentrować się na bezpieczeństwie przetwarzania danych osobowych, co wynika z art. 36 ustawy. Prawidłowe zarządzanie zasobami, w tym również informacyjnymi, zwłaszcza w aspekcie bezpieczeństwa informacji, wymaga właściwej identyfikacji tych zasobów oraz określenia miejsca i sposobu ich przechowywania. Wybór zaś odpowiednich dla poszczególnych zasobów metod zarządzania ich ochroną i dystrybucją zależny jest od zastosowanych nośników informacji, rodzaju urządzeń, sprzętu komputerowego i oprogramowania. Stąd też w § 4 rozporządzenia wskazano, że polityka bezpieczeństwa powinna zawierać w szczególności następujące punkty:

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane

są dane osobowe;
2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;
3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;
4) sposób przepływu danych pomiędzy poszczególnymi systemami;
5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przy przetwarzaniu danych.

Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe należy rozumieć jako wyszczególnienie w sposób spójny i jednoznaczny miejsc, w których przetwarza się dane osobowe zarówno w zbiorach prowadzonych w postaci zwykłej (papierowej), jak i elektronicznej. Należy zauważyć, że miejscem, o którym mowa powyżej, może być zarówno obszar całego budynku lub budynków, obszar kilku wybranych pomieszczeń, jak i obszar stanowiący wydzieloną część danego pomieszczenia. Przykładowo, gdy upoważniony podmiot realizuje przetwarzanie danych osobowych we wszystkich pomieszczeniach budynku, wówczas zawartym w polityce bezpieczeństwa wykazem obszaru przetwarzania danych może być ogólna informacja, że miejscem przetwarzania danych osobowych są wszystkie pomieszczenia znajdujące się w budynku o danym adresie. Podobnie jest, gdy proces przetwarzania danych realizowany jest w pomieszczeniach zajmujących całe piętro budynku – w wykazie można wówczas opisać wszystkie pomieszczenia znajdujące się na danym piętrze budynku o wskazanym adresie. Wskazanie w sposób ogólny miejsca przetwarzania danych – rozumianego jako pomieszczenia stanowiące cały budynek, wybraną kondygnację budynku itp. – możliwe jest tylko wówczas, gdy we wszystkich pomieszczeniach tego obszaru podmiot przetwarza dane osobowe.

Wykaz zbiorów danych osobowych, wraz ze wskazaniem programów używanych do ich przetwarzania, powinien zawierać informacje o tym, jakie zbiory danych osobowych są przetwarzane przez podmiot oraz przy użyciu jakich systemów dane zawarte w tych zbiorach są przetwarzane.

Źródło: www.giodo.gov.pl, Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.