GIODO
Generalny Inspektor
Ochrony Danych Osobowych

ZAPEWNIENIE OCHRONY DANYCH OSOBOWYCH
PORADNIK DLA ADMINISTRATORÓW DANYCH OSOBOWYCH

przygotowała: Generalny Inspektor Ochrony Danych Osobowych **dr Edyta Bielak-Jomaa**

• • •

PODSTAWA PRAWNA OCHRONY DANYCH OSOBOWYCH

Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych zobowiązuje każdego administratora danych osobowych do zapewnienia ochrony przetwarzanych danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utrata, uszkodzeniem lub zniszczeniem.

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych zawiera ogólne zapisy dotyczące tego, jak należy zabezpieczyć dane osobowe.

Przetwarzanie danych osobowych jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych.

• • •

RODZAJE DANYCH

Dane zwykłe	Dane szczególnie chronione
Dane takie jak np. imię i nazwisko, adres zamieszkania czy numer PESEL (bez tzw. danych szczególnie chronionych, o których mowa w art. 27 ust. 1 ustawy).	Dane określone w art. 27 ust. 1 ustawy, np. dane o stanie zdrowia lub o orzeczeniach sądowych bądź administracyjnych.

• • •

STOSOWANIE POZIOMÓW ZABEZPIECZEŃ DANYCH W SYSTEMACH INFORMATYCZNYCH

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym zależy od kategorii przetwarzanych danych oraz zagrożeń.

Poziom co najmniej podstawowy	Poziom co najmniej podwyższony	Poziom wysoki
administrator w prowadzonym w systemie informatycznym zbiorze przetwarza tylko dane zwykłe i żadne z urządzeń tego systemu informatycznego nie jest połączone z siecią publiczną.	administrator danych w prowadzonym w systemie informatycznym zbiorze przetwarza dane szczególnie chronione, ale żadne z urządzeń tego systemu informatycznego nie jest połączone z siecią publiczną.	przynajmniej jedno urządzenie systemu informatycznego, służącego do przetwarzania danych osobowych, połączone jest z siecią publiczną.

ADMINISTRATOR DANYCH OSOBOWYCH

organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych

• • •

Wybór środków gwarantujących przetwarzanym danym optymalny stopień zabezpieczenia
Konkretne środki wybiera administrator danych osobowych, bo najlepiej zna środowisko, w jakim przetwarza dane. Wybór zależy od:
- sposobu gromadzenia danych,
- dostępu do danych,
- infrastruktury technicznej,
- ryzyka i zagrożeń, na jakie narażone są przetwarzane dane.

Kiedy stosować zabezpieczenia teleinformatyczne? Kiedy z przeprowadzonej analizy ryzyka, dotyczącej procesu przetwarzania danych osobowych, wynika, że stwierdzone zagrożenie można zminimalizować bądź całkowicie wyeliminować poprzez dodatkowe zastosowanie takiego zabezpieczenia!

Administrator danych (obowiązki):
- upoważnia na piśmie każdą osobę przetwarzającą dane osobowe i odnotowuje ten fakt w prowadzonej ewidencji osób upoważnionych do przetwarzania danych;
- prowadzi dokumentację opisującą sposób przetwarzania danych oraz zastosowane przez niego środki techniczne i organizacyjne zapewniające ochronę danych osobowych;
- może powołać administratora bezpieczeństwa informacji (ABI), który ma obowiązek nadzorowania opracowania i aktualizowania tej dokumentacji..

• • •

Poziom bezpieczeństwa przetwarzania danych osobowych w systemie informatycznym zależy od kategorii przetwarzanych danych oraz zagrożeń.

BEZPIECZEŃSTWO FIZYCZNE
OPISANE W DOKUMENCIE POLITYKA BEZPIECZEŃSTWA

Bezpieczeństwo fizyczne: zabezpieczenia obszaru, w którym przetwarzane są dane osobowe.

- miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje),
- miejsca, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe, serwery i inne urządzenia komputerowe, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco),
- pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (taśmy, dyski, płyty CD, niesprawne komputery i inne urządzenia z nośnikami zawierającymi dane osobowe).
- miejsce w sejfie bankowym, archiwum itp., jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym czy też do składowania innych nośników danych, np. dokumentów źródłowych.
- Jeżeli do danych osobowych przetwarzanych w systemie informatycznym dostęp poprzez sieć telekomunikacyjną posiada wiele podmiotów, to w dokumentacji stanowiącej politykę bezpieczeństwa administrator danych powinien wskazać informacje o tych podmiotach, jako obszar przetwarzania danych osobowych (czyli ich nazwę, siedzibę, pomieszczenia, w których przetwarzane są dane osobowe).

• • •

Inspektor GIODO

kontroluje skuteczność zastosowanych rozwiązań, m.in.:
- system organizacji służby ochrony,
- budowlane urządzenia zabezpieczające,
- urządzenia fizycznej kontroli dostępu do pomieszczeń,
- elektroniczne urządzenia zabezpieczające przed włamaniem i pożarem,
- elektroniczny system kontroli dostępu, z rejestracją operacji otwierania i zamykania pomieszczeń przez osoby uprawnione.

BEZPIECZEŃSTWO SYSTEMÓW INFORMATYCZNYCH
OPISANE W DOKUMENCIE: INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

organ, jednostka organizacyjna, podmiot lub osoba decydująca o celach i środkach przetwarzania danych

• • •

Jest to dokument zatwierdzony przez administratora danych i u niego obowiązujący, w którym zawarte procedury i wytyczne powinny być przekazane osobom odpowiedzialnym za ich realizację. Instrukcja zarządzania systemem informatycznym musi zawierać:

- zastosowany poziom bezpieczeństwa przetwarzania danych osobowych;
- opis procedur związanych z bezpieczeństwem przetwarzanych danych osobowych (§ 5 rozporządzenia):
  - nadawanie uprawnień do przetwarzania danych i rejestrowanie tych uprawnień w systemie informatycznym,wraz ze wskazaniem osoby odpowiedzialnej za te czynności.
  - procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu;
  - stosowane metody i środki uwierzytelnienia związane z zarządzaniem i użytkowaniem (np. procedury tworzenia i przyznawania haseł użytkownikom).
  - tworzenie kopii zapasowych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania, a także ich miejsce i okres przechowywania;
- informację, w jaki sposób zabezpieczono system informatyczny przed działalnością oprogramowania szkodliwego;
- procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych;
- jeśli dane przetwarzane w zbiorze udostępnia się innym podmiotom za pomocą systemu informatycznego (teletransmisja danych) - sposób takiego przepływu danych.

• • •

W przypadku teletransmisji danych, podstawowym wymogiem jest zabezpieczenie informacji przesyłanych drogą teletransmisji przed udostępnieniem ich osobom nieuprawnionym oraz przed utratą, uszkodzeniem lub zniszczeniem danych. Jeśli administrator danych wykorzystuje przenośne urządzenia zawierające dane osobowe (np. laptop, pendrive), jest zobowiązany do szyfrowania tych danych.

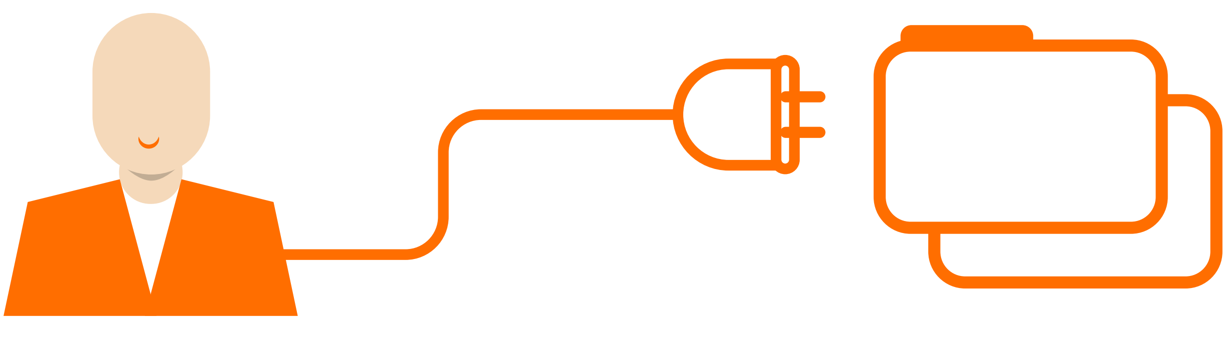
• • •

Przykładowe wymogi wobec systemu informatycznego

Dla bezpieczeństwa danych przetwarzanych w systemie informatycznym każdy administrator ma obowiązek zapewnić, aby system ten odnotowywał kilka podstawowych informacji:
- datę pierwszego wprowadzenia danych do systemu,
- identyfikator użytkownika, który wprowadza dane osobowe do sytemu (jeśli zajmuje się tym kilka osób),
- źródło danych, czyli informację skąd pochodzą gromadzone dane,
- odbiorców, czyli komu dane osobowe zostały udostępnione oraz kiedy i w jakim zakresie,
- sprzeciw, czyli informację kto wniósł sprzeciw wobec wykorzystywania jego danych, a co związane jest z tym, że dane takiej osoby nie mogą być już dalej przetwarzane.

Ponadto system informatyczny, w którym przetwarza się dane osobowe: powinien zapewnić sporządzenie i wydrukowanie dla każdej osoby,

HASŁO UŻYTKOWNIKA SYSTEMU INFORMATYCZNEGO



Przetwarzane są tylko dane zwykłe i system nie jest podłączony do sieci publicznej
- hasło musi składać się z co najmniej z 6 znaków.
- zmiana nie rzadziej niż co 30 dni.

Przetwarzane są, oprócz danych zwykłych, również dane szczególnie chronione oraz (lub) system ten jest połączony z siecią publiczną
- hasło musi składać się z co najmniej 8 znaków – z małych i wielkich liter oraz z cyfr lub znaków specjalnych.
- zmiana nie rzadziej niż raz na 30 dni.

STRONA INTERNETOWA GIODO ŹRÓDŁEM CENNYCH INFORMACJI

Na stronie internetowej GIODO znajduje się wiele materiałów dotyczących ochrony danych osobowych przetwarzanych w systemach informatycznych. Są one dostępne m.in. pod linkiem:
http://www.giodo.gov.pl/1520074/j/pl/

GIODO
Generalny Inspektor
Ochrony Danych Osobowych