

# Rola informatyka w procesie ochrony danych osobowych



Zakopane, 20 maja 2010

# Podstawy prawne ochrony danych osobowych

- **Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych. (tekst jednolity: Dz. U. 2002 r. Nr 101 poz. 926, ze zm.)**
- **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 (Dz. U. z 2004 r. Nr 100, poz. 1024)**

# Funkcje w ochronie danych osobowych

- Administrator Danych
- Administrator Bezpieczeństwa Informacji
- Administrator Systemów Informatycznych
- Operatorzy systemów przetwarzania danych osobowych

# Dokumentacja Bezpieczeństwa

- Raport z audytu zasobów informatycznych
- **Polityka bezpieczeństwa**
- Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
- **Instrukcja określająca sposób zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych**

# Wdrożenie Polityki Bezpieczeństwa

- Analiza stanu bezpieczeństwa danych osobowych – analiza ryzyka
- Opracowanie Polityki Bezpieczeństwa, Instrukcji i dokumentów związanych
- Wdrożenie zabezpieczeń organizacyjnych
- Wdrożenie zabezpieczeń technicznych
- Zarządzenie Administratora Danych w sprawie ochrony danych osobowych
- Szkolenie pracowników

# Obowiązki Administratora Danych

- Określenie celów, strategii i polityki zabezpieczenia danych osobowych przetwarzanych w systemie informatycznym,
- Identyfikacja i analiza zagrożeń,
- Określenie potrzeb w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych,

# Obowiązki administratora danych <sup>(2)</sup>

- Uwzględnienie potrzeby kryptograficznej ochrony danych osobowych, przy ich przesyłaniu drogą teletransmisji w sieci publicznej
- Określenie zabezpieczeń adekwatnych do zagrożeń i ryzyka
- Monitorowanie działania wdrożonych zabezpieczeń

# Obowiązki administratora danych <sup>(3)</sup>

- Opracowanie i wdrożenie programu szkoleń w zakresie zabezpieczeń danych,
- Wykrywanie i właściwa reakcja na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych je przetwarzających,
- **Opracowanie Polityki Bezpieczeństwa,**

# Obowiązki administratora danych <sup>(4)</sup>

- **Opracowanie instrukcji określającej sposób zarządzania systemem informatycznym, służącym do przetwarzania danych osobowych.**
- **Opracowanie instrukcji postępowania w sytuacji naruszenia danych osobowych, przeznaczonej dla osób zatrudnionych przy przetwarzaniu tych danych,**

# Analiza zagrożeń

- Pracownik odpowiedzialny za bezpieczeństwo danych i systemów informatycznych (ABI) wykonuje analizę potencjalnych zagrożeń, na które mogą być narażone zasoby informatyczne,
- W razie konieczności zleca się firmie specjalistycznej wykonanie audytu systemu komputerowego, sprawdzającego jego podatność na atak oraz obecność programów szpiegujących (spyware),

# Analiza zagrożeń <sup>(2)</sup>

- Bardzo często największym zagrożeniem jest niedbałość pracowników i nieprzestrzeganie przez nich podstawowych zasad bezpieczeństwa pracy z systemem informatycznym.

# Zabezpieczenia organizacyjne

Ochrona budynku przedsiębiorstwa:

- zapewnienie dozoru pomieszczeń w godzinach pracy i poza pracą,
- zabezpieczenie dostępu do pomieszczeń poprzez zastosowanie drzwi i okien antywłamaniowych, ew. rolet lub krat,
- instalacja alarmowa i ppoż.,

# Zabezpieczenia organizacyjne <sup>(2)</sup>

- Nie dopuszczanie osób postronnych do systemu informatycznego firmy,
- Wprowadzenie zakazu pozostawiania włączonych komputerów z zalogowanym do systemu użytkownikiem po opuszczeniu stanowiska pracy,

# Zabezpieczenia organizacyjne <sup>(3)</sup>

- Zaplanowanie i przeprowadzanie cyklu szkoleń dla pracowników, dotyczących bezpiecznego użytkowania systemów informatycznych oraz potencjalnych zagrożeń.

# Zabezpieczenia techniczne

- Instalacja sprzętowych i programowych zabezpieczeń systemu: firewall, IDS, IPS,
- Instalacja poprawek i aktualizacji systemów operacyjnych,
- Instalacja skutecznego oprogramowania antywirusowego i uaktualnianie na bieżąco baz danych o wirusach,

## Zabezpieczenia techniczne <sup>(2)</sup>

- Odseparowanie galwaniczne sieci wewnętrznej, zawierającej najcenniejsze zasoby danych, od Internetu,
- Wprowadzenie systemu identyfikatorów i haseł użytkowników sieci LAN, baz danych i aplikacji,
- Ustawianie odpowiednich uprawnień użytkownikom systemu

# Zabezpieczenia techniczne <sup>(3)</sup>

- Założenie haseł na BIOS,
- Wymuszenie zmiany haseł przez użytkowników z określoną częstotliwością,
- Zainstalowanie wygaszaczy ekranów,

# Obszar przetwarzania danych osobowych

- Za obszar, w którym są przetwarzane dane osobowe uznaje się pomieszczenia w których znajdują się urządzenia komputerowe przeznaczone do przetwarzania danych osobowych, serwery komputerowych sieci lokalnych, urządzenia aktywne tych sieci oraz wszystkie pomieszczenia w których zlokalizowany jest sprzęt komputerowy w pamięci którego są przetwarzane dane osobowe.

# Zasady dostępu do obszaru przetwarzania danych osobowych

- Przebywanie w obszarze przetwarzania danych osobowych osób nieuprawnionych do dostępu do danych osobowych jest dopuszczalne jedynie w obecności osoby zatrudnionej przy przetwarzaniu tych danych, a w przypadku nieobecności tej osoby tylko i wyłącznie za zgodą administratora bezpieczeństwa informacji lub administratora danych osobowych.

# Zasady dostępu do obszaru przetwarzania danych osobowych <sup>(2)</sup>

- Pomieszczenia obszaru przetwarzania danych osobowych w czasie nieobecności w nich osób uprawnionych powinny być zamykane w sposób uniemożliwiający dostęp do nich osób trzecich.

# Procedury rozpoczęcia i zakończenia pracy

- Osoba rozpoczynająca pracę ma obowiązek każdorazowego sprawdzenia, czy nie naruszono bezpieczeństwa, szczególnie przez sprawdzenie zamknięcia drzwi i okien,
- Podczas pracy w systemie niedozwolone jest pozostawienie bez dozoru komputera z uruchomionym programem i aktywnym użytkownikiem,

# Procedury rozpoczęcia i zakończenia pracy <sup>(2)</sup>

- Po zakończeniu pracy ostatni opuszczający pomieszczenie pracownik ma obowiązek sprawdzenia wyłączenia urządzeń elektrycznych i łączności, oraz sprawdzenia zamknięcia drzwi i okien,
- Administrator Bezpieczeństwa Informacji jest odpowiedzialny za zabezpieczenie pomieszczeń w czasie wolnym od pracy w sposób uniemożliwiający dostęp do nich osób nieuprawnionych,

# Procedury rozpoczęcia i zakończenia pracy <sup>(3)</sup>

- Każda osoba dopuszczona do pracy przy przetwarzaniu danych osobowych musi:
  - ✓ być zaznajomiona z przepisami o ochronie danych osobowych oraz instrukcją określającą sposób postępowania w przypadku naruszenia bezpieczeństwa, co potwierdza własnoręcznym podpisem,
  - ✓ posiadać własny identyfikator i własne hasło dostępu,
  - ✓ w swoim zakresie czynności mieć określone odpowiednie uprawnienia i odpowiedzialność w zakresie przetwarzania danych osobowych.

# Serwisowanie systemów informatycznych

- Urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, zasilane energią elektryczną, winny być zabezpieczone przed utratą tych danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej,
- Przeglądy i konserwację systemów służących do przetwarzania danych osobowych dokonują Administratorzy systemów,

# Serwisowanie systemów informatycznych <sup>(2)</sup>

- Prace związane z zarządzaniem systemami informatycznymi, ich instalowaniem, konfiguracją, modernizacją itp. mogą wykonywać jedynie wyznaczeni administratorzy tych systemów lub inne osoby za każdorazową zgodą administratora bezpieczeństwa informacji lub administratora danych osobowych. W szczególnych przypadkach tego wymagających dopuszcza się wykonywanie tych prac przez pracowników specjalistycznych podmiotów zewnętrznych, przy czym może to następować tylko i wyłącznie pod bezpośrednim nadzorem wyznaczonych pracowników.

# Serwisowanie systemów informatycznych <sup>(3)</sup>

- Przeglądy i aktualizacje zbiorów danych osobowych dokonują uprawnieni użytkownicy systemów,
- Firmy lub osoby nie będące pracownikami, pełniące funkcję administratorów lub serwisantów systemów, składają na piśmie zobowiązanie o:
  - ✓ przestrzeganiu zapisów ustawy o ochronie danych osobowych i nie wykorzystywaniu danych, do których mają dostęp do celów innych niż wynikających z potrzeby administrowania systemem
  - ✓ zachowaniu w tajemnicy swoich identyfikatorów i haseł dostępu do systemów informatycznych.

# Archiwizacja danych osobowych

- Kopie awaryjne danych są wykonywane przez administratora systemu lub wyznaczonego pracownika z odpowiednią częstotliwością i przekazywane do przechowywania w wyznaczonym do tego miejscu (najlepiej poza podstawową lokalizacją przetwarzania danych).

# Archiwizacja danych osobowych <sup>(2)</sup>

- Administrator Bezpieczeństwa Informacji oraz Administrator Systemu okresowo sprawdzają kopie awaryjne pod kątem ich dalszej przydatności do odtworzenia danych systemu.
- Po ustaniu użyteczności kopie i ich nośniki są bezzwłocznie kasowane w sposób bezpowrotny.

# Zasady postępowania z nośnikami danych

- Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia przechowuje się w pomieszczeniach i pojemnikach (sejfy, szafy metalowe, gabloty) właściwie zabezpieczonych i wskazanych przez Administratora Bezpieczeństwa Informacji.

# Zasady postępowania z nośnikami danych <sup>(2)</sup>

- Dostęp do nośników informacji i wydruków zawierających dane osobowe mają tylko pracownicy uprzednio przeszkoleni i upoważnieni przez Administratora Bezpieczeństwa Informacji.

# Zasady postępowania z nośnikami danych <sup>(3)</sup>

- w czasie korzystania z materiałów zawierających dane osobowe pracownik:
  - ✓ nie może udostępnić materiałów lub ich treści celowo lub nieumyślnie osobom postronnym,
  - ✓ nie może opuścić pomieszczenia, w którym pracuje bez właściwego zabezpieczenia materiałów.

# Zasady postępowania z nośnikami danych <sup>(4)</sup>

- Nośniki informacji oraz wydruki zawierające dane osobowe nie mogą być zabierane poza miejsce pracy.
- Po zakończeniu pracy materiały te powinny być zabezpieczone w sposób ustalony z Administratorem Bezpieczeństwa Informacji.

# Zasady postępowania z nośnikami danych <sup>(5)</sup>

- Przeznaczone do likwidacji urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe pozbawia się wcześniej zapisu tych danych, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie.

# Zasady postępowania z nośnikami danych <sup>(6)</sup>

- Przeznaczone do przekazania innemu podmiotowi nie uprawnionemu do otrzymania danych osobowych urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe pozbawia się wcześniej zapisu tych danych.

# Zasady postępowania z nośnikami danych <sup>(7)</sup>

- Przeznaczone do naprawy urządzenia, dyski lub inne informatyczne nośniki zawierające dane osobowe pozbawia się przed naprawą zapisu tych danych albo naprawia się je pod nadzorem osoby upoważnionej przez administratora systemu.

# Zasady postępowania z nośnikami danych <sup>(8)</sup>

- Wydruki, które zawierają dane osobowe i są przeznaczone do usunięcia należy zniszczyć w stopniu uniemożliwiającym ich odczytanie.

# Identyfikatory i hasła użytkowników systemów

- Do pracy z systemami informatycznymi, szczególnie systemami zawierającymi dane osobowe, mogą być dopuszczeni jedynie uprawnieni pracownicy posiadający indywidualny identyfikator użytkownika i hasło.

# Identyfikatory i hasła użytkowników systemów <sup>(2)</sup>

- Administrator danego systemu informatycznego lub lokalnej sieci komputerowej ustala indywidualny identyfikator każdemu użytkownikowi tego systemu lub sieci, a także sposób przydziału haseł dla użytkowników i częstotliwość ich zmian oraz prowadzi ewidencję nadanych indywidualnych identyfikatorów użytkowników zawierającą nazwę użytkownika, jego identyfikator, datę nadania oraz datę wycofania.

# Identyfikatory i hasła użytkowników systemów <sup>(3)</sup>

- Hasła powinny być proste, łatwe do zapamiętania, aby uniknąć zapisywania ich przez pracowników, ale nie mogą być to hasła oczywiste do odgadnięcia (np. imiona lub nazwiska, nazwy własne, data urodzenia itp.).
- Hasła powinny być zmieniane najrzadziej raz w miesiącu.

# Identyfikatory i hasła użytkowników systemów <sup>(4)</sup>

- Za wymuszanie zmian haseł z odpowiednią częstotliwością odpowiedzialny jest Administrator danego systemu lub sieci lokalnej.

# Identyfikatory i hasła użytkowników systemów <sup>(5)</sup>

- Każdy użytkownik systemu posiada własny identyfikator, który nie podlega zmianom. Jeżeli użytkownik utracił uprawnienia dostępu do systemu administrator ma obowiązek bezzwłocznie wyrejestrować identyfikator z systemu. Po wyrejestrowaniu nie może on przechodzić na inną osobę.

# Identyfikatory i hasła użytkowników systemów <sup>(6)</sup>

- Administrator systemu jest zobowiązany do prowadzenia dziennika systemu, w którym winien odnotowywać ważniejsze informacje o pracy systemu i wykonywanych czynnościach.

# Identyfikatory i hasła użytkowników systemów <sup>(7)</sup>

- Komunikacja w komputerowej sieci lokalnej poprzez istniejący system przyznanym uprawnień użytkowników, powinna uniemożliwiać dostęp do danych osobowych osób nie zatrudnionych przy ich przetwarzaniu.

# Identyfikatory i hasła użytkowników systemów <sup>(8)</sup>

- Hasła użytkownika umożliwiające dostęp do systemu informatycznego utrzymuje się w tajemnicy również po upływie terminu ich ważności.

# Profilaktyka i kontrola antywirusowa

- Administratorzy sieci i systemów z określoną częstotliwością sprawdzają systemy służące do przetwarzania danych osobowych, pod kątem obecności wirusów komputerowych, za pomocą posiadanego oprogramowania antywirusowego.

# Profilaktyka i kontrola antywirusowa <sup>(2)</sup>

- Użytkownicy systemów służących do przetwarzania danych osobowych mają obowiązek każdorazowego sprawdzania dyskietek programem antywirusowym przed kopiowaniem danych na nich zawartych na dysk twardy komputera lub dysk sieciowy.

# Zabezpieczenia systemu informatycznego

- Hasła dostępu na BIOS
- Identyfikatory i hasła dostępu do systemu operacyjnego i sieci
- Hasła dostępu systemów baz danych
- Hasła dostępu do aplikacji
- Wygaszacze ekranowe
- Ustawienie monitorów w sposób uniemożliwiający wgląd do danych osobom postronnym

# Internet a ochrona danych osobowych

- System informatyczny służący przetwarzaniu danych osobowych nie może mieć bezpośredniego dostępu do sieci Internet, bez zastosowania skutecznych środków ochrony przed nieuprawnionym dostępem do danych z zewnątrz.

# Internet a ochrona danych osobowych <sup>(2)</sup>

- Dane osobowe mogą być przesyłane Internetem wyłącznie przy zastosowaniu kryptograficznej ochrony danych wykorzystywanych do uwierzytelnienia.

# Reguły postępowania w praktyce

- Nie instalowanie oprogramowania niepewnego pochodzenia,
- Sprawdzanie zewnętrznych nośników na obecność wirusów przed skopiowaniem z nich danych,
- Unikanie stron internetowych z podejrzaną zawartością,

# Reguły postępowania w praktyce (2)

- Dokładne czytanie wszystkich komunikatów przeglądarki internetowej przed ich akceptacją,
- Powstrzymanie się od rozsyłania dalej anonimowych maili,
- Informowanie administratora systemu o wszelkich zakłóceniach w pracy lub nietypowym zachowaniu systemu.

# Naruszenie bezpieczeństwa danych osobowych

- wystąpienie zagrożeń dla substancji materialnej (np. pożar, powódź, włamanie),
- przebywanie osób nieuprawnionych w obszarach przetwarzania danych i obszarach węzła sieci,

# Naruszenie bezpieczeństwa danych osobowych <sup>(2)</sup>

- wykorzystywanie zasobów materialnych, programów i danych do celów pozasłużbowych
- udostępnianie danych osobom nieupoważnionym,
- ujawnienie metod zabezpieczenia danych,

# Naruszenie bezpieczeństwa danych osobowych <sup>(3)</sup>

- ujawnienie metod przetwarzania i sposobu przechowywania danych,
- umożliwienie dostępu do systemu przetwarzającego dane osobowe osobom nieupoważnionym,

# Naruszenie bezpieczeństwa danych osobowych <sup>(4)</sup>

- ujawnienie informacji mogących przyczynić się do ułatwienia dostępu osobom nieupoważnionym lub w sposób nieuprawniony,
- wystąpienie awarii sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych osobowych.

**Dziękuję za uwagę.**