Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną

Andrzej Kaczmarek
Biuro GIODO

Plan prezentacji:

- **Przepisy określające wymagania w zakresie bezpieczeństwa przetwarzania danych**
- **Standardy i normy międzynarodowe dotyczące bezpieczeństwa przetwarzania danych przy użyciu systemów teleinformatycznych**
- **Standardy dotyczące protokołów wymiany danych**
- **Elementy bezpieczeństwa systemów teleinformatycznych wg ISO/IEC 27002 (PN-ISO/IEC 17799)**
- **Realizacja wymogów ustawy o ochronie danych osobowych poprzez wdrożenie standardów bezpieczeństwa**
- **Zarządzanie bezpieczeństwem w cyklu przetwarzania danych osobowych**

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Dwa główne podejścia:

I Model centralny

- **Odwołanie w sprawach dotyczących bezpieczeństwa teleinformatycznego do standardów np. PN, EN, ISO**
- **Odwołanie się w aktach prawnych do wytycznych opracowywanych przez wyspecjalizowane instytucje (np. BSI w Niemczech)**

II Model rozproszony

- **Odwołanie się do przepisów prawa (różnych ustaw i rozporządzeń)**
  - **Ustawa o rachunkowości**
  - **Ustawa o ochronie danych osobowych**
  - **Ustawa o ochronie informacji niejawnych**
  - **Inne ustawy, rozporządzenia**

Regulacje prawne wprowadzające elementy centralnego modelu zarządzania bezpieczeństwem informacji

- **Przepisy rangi ustawowej**
- **Rozporządzenia (odwołujące się do standardów krajowych i/lub międzynarodowych**
- **Dobre praktyki, rekomendacje, zalecenia.**

Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565 z późn. zm.)

Rozdział 3 ustawy wprowadza delegacje ustawowe do określenia mechanizmów, które mają zapewnić interoperacyjność na trzech płaszczyznach, jakimi są:

- **stosowanie systemu teleinformatycznego,**
- **prowadzenie rejestrów publicznych oraz**
- **prowadzenie wymiany dokumentów w formie elektronicznej**

W odniesieniu do systemów teleinformatycznych ustawa wprowadza zasadę wykorzystywania systemów spełniających tzw. **minimalne wymagania dla systemów teleinformatycznych**. Jednocześnie ustawodawca określił minimalne wymagania jako zespół wymagań organizacyjnych i technicznych, których spełnienie przez system teleinformatyczny używany do realizacji zadań publicznych umożliwia **wymianę danych z innymi systemami teleinformatycznymi**.

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766 z 2005 r,).

§ 2 Systemy teleinformatyczne używane przez podmioty publiczne do realizacji zadań publicznych

1) **powinny spełniać właściwości i cechy w zakresie funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, określone w normach ISO zatwierdzonych przez krajową jednostkę normalizacyjną, na etapie projektowania, wdrażania i modyfikowania tych systemów.**

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766 z 2005 r,).

2) **powinny zostać wyposażone w składniki sprzętowe i oprogramowanie:**

   a) **umożliwiające wymianę danych z innymi systemami teleinformatycznymi używanymi do realizacji zadań publicznych za pomocą protokołów komunikacyjnych i szyfrujących określonych w załączniku nr 1 do rozporządzenia, stosownie do zakresu działania tych systemów,**

   b) **zapewniające dostęp do zasobów informacji udostępnianych przez systemy teleinformatyczne używane do realizacji zadań publicznych przy wykorzystaniu formatów danych określonych w załączniku nr 2 do rozporządzenia**

Rozporządzenie Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych (Dz. U. Nr 212, poz. 1766 z 2005 r,).

W § 3 ww. rozporządzenia zapisano, że:

1. **Podmiot publiczny opracowuje, modyfikuje w zależności od potrzeb oraz wdraża politykę bezpieczeństwa dla systemów teleinformatycznych używanych przez ten podmiot do realizacji zadań publicznych.**

2. **Przy opracowywaniu polityki bezpieczeństwa, o której mowa w ust. 1, podmiot publiczny powinien uwzględniać zalecenia Polskich Norm z zakresu bezpieczeństwa informacji.**

ROZPORZĄDZENIE MINISTRA ZDROWIA z dnia 21 grudnia 2006 r.

w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz. U. z dnia 28 grudnia 2006 r.)

W § 59 ww. rozporządzenia zapisano, że:

1. **Zbiory informacji objętych dokumentacją prowadzoną w postaci elektronicznej powinny być sporządzane z uwzględnieniem postanowień Polskich Norm, których przedmiotem są zasady gromadzenia i wymiany informacji w ochronie zdrowia przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy**
2. **W przypadku braku Polskich Norm przenoszących normy europejskie lub normy innych państw członkowskich Europejskiego Obszaru Gospodarczego przenoszących te normy uwzględnia się**
   1) **normy międzynarodowe;**
   2) **Polskie Normy;**
   3) **europejskie normy tymczasowe.**

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

ROZPORZĄDZENIE MINISTRA ZDROWIA z dnia 21 grudnia 2006 r.

w sprawie rodzajów i zakresu dokumentacji medycznej w zakładach opieki zdrowotnej oraz sposobu jej przetwarzania (Dz. U. z dnia 28 grudnia 2006 r.)

W § 60 ww. rozporządzenia zapisano, że:

1. **Dokumentację prowadzoną w postaci elektronicznej uważa się za zabezpieczoną, jeżeli w sposób ciągły są spełnione łącznie następujące warunki:**
   1) **zapewniona jest jej dostępność wyłącznie dla osób uprawnionych;**
   2) **jest chroniona przed przypadkowym lub nieuprawnionym zniszczeniem;**
   3) **są zastosowane metody i środki ochrony dokumentacji, których skuteczność w czasie ich zastosowania jest powszechnie uznawana.**

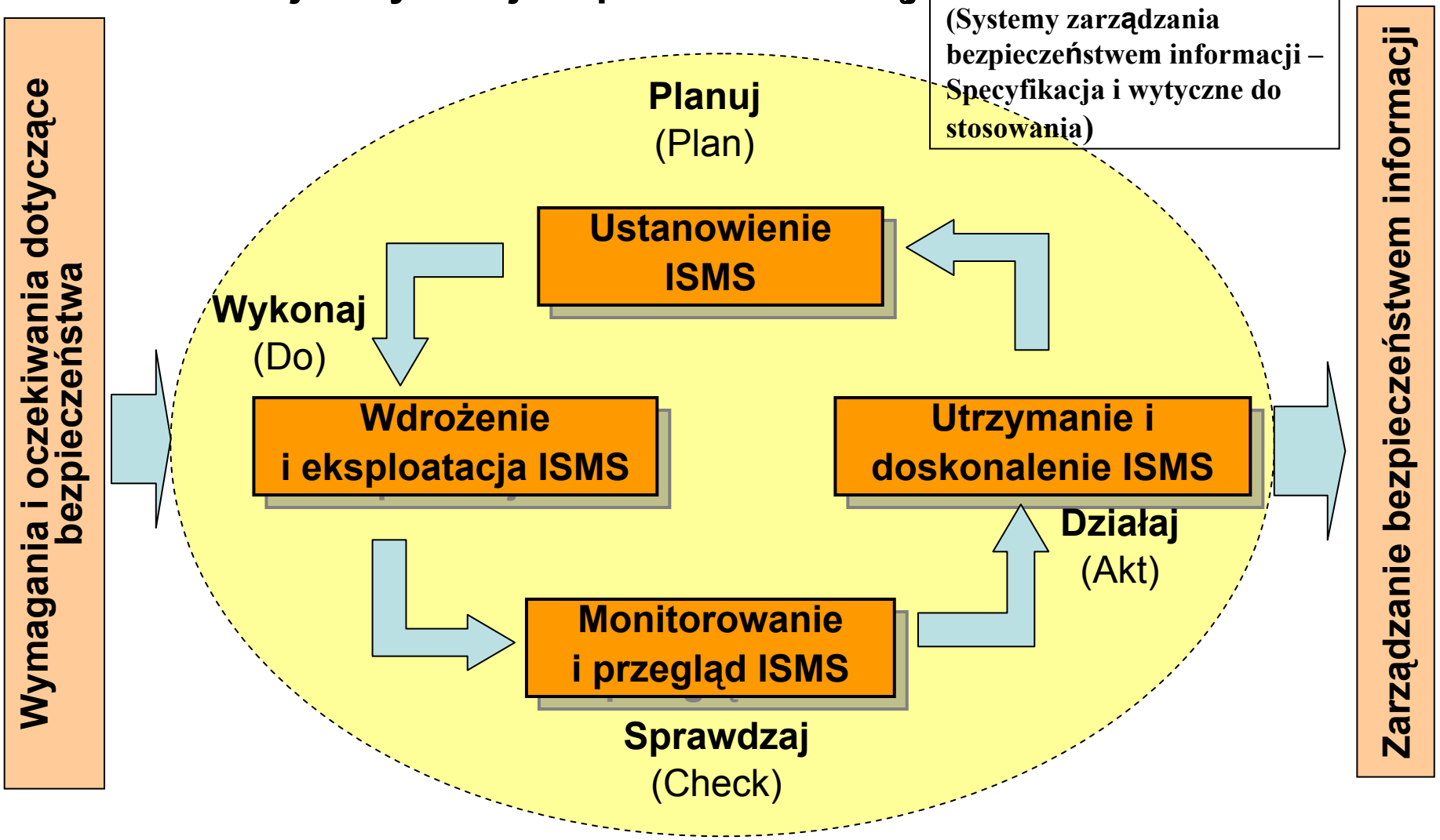
2. **Zabezpieczenie dokumentacji prowadzonej w postaci elektronicznej wymaga w szczególności:**
   1) **systematycznego dokonywania analizy zagrożeń;**
   2) **opracowania i stosowania procedur zabezpieczania dokumentacji i systemów ich przetwarzania, w tym procedur dostępu oraz przechowywania;**
   3) **stosowania środków bezpieczeństwa adekwatnych do zagrożeń;**

   …..

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Zasada: Planuj – Wykonaj – Sprawdź – Działaj

PN-ISO/IEC 27001
(Systemy zarządzania bezpieczeństwem informacji – Specyfikacja i wytyczne do stosowania)



Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

ISO/IEC 27002
PN-ISO/IEC 17799
(Praktyczne zasady zarządzania bezpieczeństwem informacji)

Norma PN ISO/IEC 17799

Rozdział 10

Zarządzanie systemami i sieciami

- Procedury eksploatacyjne i zakresy odpowiedzialności
- Zarządzanie usługami strony trzeciej
- Planowanie i odbiór systemów
- Ochrona przed szkodliwym i mobilnym k
- Kopie zapasowe
- **Zarządzanie bezpieczeństwem sieci**
- Obsługa nośników
- **Wymiana informacji**
- **Usługi handlu elektronicznego**

Zabezpieczenia sieciowe
Bezpieczeństwo usług sieciowych

Polityki i procedury wymiany informacji
Umowy wymiany informacji
Transportowanie nośników fizycznych
Wiadomości elektroniczne
Biznesowe systemy informacyjne

Handel elektroniczny
Transakcje on-line
Informacja publicznie dostępna

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Norma PN ISO/IEC 17799

Rozdział 11

Kontrola dostępu

- Wymagania biznesowe dla kontroli dostę
- Zarządzanie dostępem użytkowników
- Odpowiedzialność użytkowników
- **Kontrola dostępu do sieci**
- **Kontrola dostępu do systemów operacyjnych**
- Kontrola dostępu do aplikacji i informacji
- **Przetwarzanie mobilne i praca na odległość**

Polityka dotycząca korzystania z usług sieciowych
Uwierzytelnianie użytkowników przy połączeniach zewnętrznych
Identyfikacja urządzeń w sieciach
Ochrona zdalnych portów diagnostycznych i konfiguracyjnych
Rozdzielanie sieci
Kontrola połączeń sieciowych
Zabezpieczenie routingu w sieciach

Procedury bezpiecznego rejestrowania
Identyfikacja i uwierzytelnianie użytkowników
System zarządzania hasłami
Korzystanie z narzędzi systemowych
Zamykanie sesji po określonym czasie
Ograniczanie czasu trwania połączenia

Przetwarzanie i komunikacja mobilna
Praca na odległość

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Norma PN ISO/IEC 17799
Rozdział 12
Pozyskiwanie, rozwój i utrzymanie systemów informacyjnych

- Wymagania bezpieczeństwa systemów informacyjnych
- Poprawne przetwarzanie w aplikacjach
- **Zabezpieczenia kryptograficzne**
- Bezpieczeństwo plików systemowych
- **Bezpieczeństwo w procesach rozwojowych i obsługi informatycznej**
- **Zarządzanie podatnościami technicznymi**

Polityka korzystania z zabezpieczeń kryptograficznych
Zarządzanie kluczami

Procedury kontroli zmian
Techniczny przegląd aplikacji po zmianach w systemie operacyjnym
Ograniczenia dotyczące zmian w pakietach oprogramowania
Wyciek informacji
Prace rozwojowe nad oprogramowaniem powierzone firmie zewnętrznej

Nadzór nad podatnościami technicznymi

Dostawcy są często pod znacznym naciskiem, aby wydawać poprawki tak szybko, jak to możliwe. Z tego powodu poprawka może nie rozwiązywać problemu w wystarczający sposób oraz może mieć negatywne skutki uboczne. Ponadto, w niektórych przypadkach, po zainstalowaniu poprawki jej odinstalowanie może być utrudnione

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Załącznik nr 1 do Rozporządzenia Rady Ministrów z dnia 11 października 2005 r. w sprawie minimalnych wymagań dla systemów teleinformatycznych

1. **Protokoły do wymiany danych z systemami teleinformatycznymi :**

IP w. 4	Internet Protocol
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
ICMP	Internet Control Message Protocol
HTTP w.1.1	Hypertext Transfer Protocol

2. **Protokoły do wymiany danych pomiędzy klientem i serwerem poczty elektronicznej**:

SMTP/MIME	Simple Mail Transfer Protocol/ Multi-Purpose Internet Mail Extensions
POP3	Post Office Protocol
IMAP	Internet Message Access Protocol

3. **Protokoły do szyfrowania danych przesyłanych w sieci telekomunikacyjnej (Internecie)**

SSL w. 3/TLS	Secure Sockets Layer / Transport Layer Security
S/MIME w. 3	Secure Multi-Purpose Internet Mail Extensions

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Kiedy stosować szyfrowanie ?

Przesyłanie danych w sieci telekomunikacyjnej

1. **Logowanie do zdalnego systemu (przesyłanie danych uwierzytelniających)**
2. **Zdalne przeglądanie danych objętych tajemnicą (dane osobowe, inne dane prawnie chronione)**
3. **Zdalne wprowadzanie lub edycja danych objętych tajemnicą prawnie chronioną**

Jakie stosować środki ostrożności ?

1	Sprawdzać adres systemu
2	Sprawdzać czy sesja jest szyfrowana
3	Sprawdzać certyfikat serwera

1	Stosować złożone hasło (co najmniej 8 znaków)
2	Zmieniać hasło po określonym okresie czasu (30 dni)
3	Zachować ostrożność przy wprowadzaniu hasła aby nie zostało podglądnięte
4	Chronić hasło przed ujawnieniem (starać się zapamiętać, nie zapisywać w postaci łatwej do odczytania)
5	Zastosować dodatkowe elementy (blokada dostępu po 3 nieudanych logowaniach, sprawdzać datę ostatniego logowania)

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Kiedy stosować szyfrowanie ?

Przy braku teletransmisji

1. **Przekazywanie danych na nośnikach informatycznych poza strefę przetwarzania**
2. **Przetwarzanie danych na komputerach przenośnych**

Jakie stosować środki ostrożności ?

1	Klucza szyfrującego, hasła nie przekazywać razem z nośnikiem danych zaszyfrowanych
2	Korzystać z bezpiecznych środków przekazywania (kurier, poczta specjalna)
3	Zabezpieczyć nośnik przed fizycznym uszkodzeniem

Procedury zarządzanie kluczami kryptograficznymi

1. Stosuj bezpieczne procedury zarządzania kluczami
2. Stosuj zmienne i odpowiednio długie klucze kryptograficzne
3. Nie umieszczaj kluczy kryptograficznych w kodach programów
4. Stosuj zaufane i sprawdzone systemy ochrony kryptograficznej

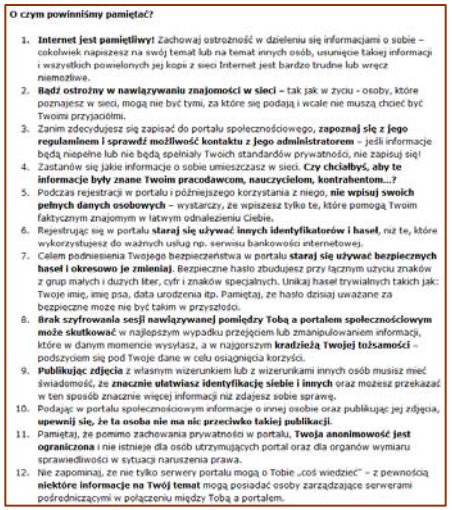
Przy określaniu odpowiedniego poziomu ochrony oraz odpowiedniej specyfikacji, która ma zapewnić wymagany poziom ochrony i wspierać wdrożenie bezpiecznego systemu zarządzania kluczami, zaleca się korzystanie ze specjalistycznego wsparcia.
ISO/IEC JTC1 SC27 opracował kilka norm związanych z zabezpieczeniami kryptograficznymi. Więcej informacji na ten temat można znaleźć też w IEEE P1363 i „Zaleceniach kryptograficznych" OECD.

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Informowanie użytkowników o wymaganiach jakie powinny spełniać użytkowane przez nich systemy informatyczne w celu zapewnienia bezpiecznej komunikacji

Jak zabezpieczyć komputer

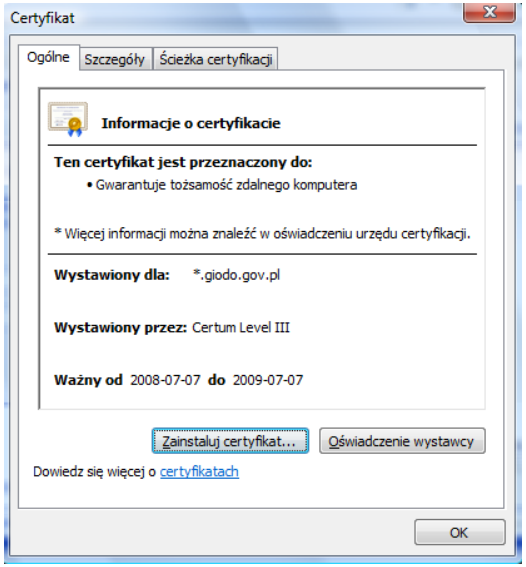
Procedury i środki bezpieczeństwa stacji komputerowej

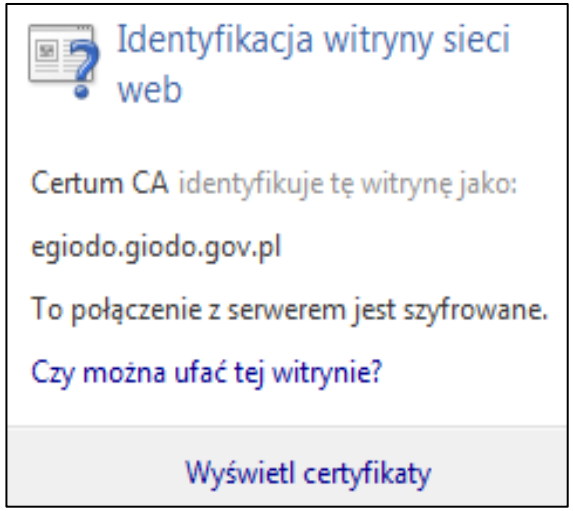


O czym powinniśmy pamiętać?

1. **Internet jest pamiętliwy!** Zachowaj ostrożność w dzieleniu się informacjami o sobie – cokolwiek napiszesz na swój temat lub na temat innych osób, usunięcie takiej informacji i wszystkich powielonych jej kopii z sieci Internet jest bardzo trudne lub wręcz niemożliwe.
2. **Bądź ostrożny w nawiązywaniu znajomości w sieci** – tak jak w życiu - osoby, które poznajesz w sieci, mogą nie być tymi, za które się podają i wcale nie muszą chcieć być Twoimi przyjaciółmi.
3. Zanim zdecydujesz się zapisać do portalu społecznościowego, **zapoznaj się z jego regulaminem i sprawdź możliwość kontaktu z jego administratorem** – jeśli informacje będą niepełne lub nie będą spełniały Twoich standardów prywatności, nie zapisuj się!
4. Zastanów się jakie informacje o sobie umieszczasz w sieci. **Czy chciałbyś, aby te informacje były znane Twoim pracodawcom, nauczycielom, kontrahentom...?**
5. Podczas rejestracji w portalu i późniejszego korzystania z niego, **nie wpisuj swoich pełnych danych osobowych** – wystarczy, że wpiszesz tylko te, które pomogą Twoim faktycznym znajomym w łatwym odnalezieniu Ciebie.
6. Rejestrując się w portalu **staraj się używać innych identyfikatorów i haseł**, niż te, które wykorzystujesz do ważnych usług np. serwisu bankowości internetowej.
7. Celem podniesienia Twojego bezpieczeństwa w portalu **staraj się używać bezpiecznych haseł i okresowo je zmieniaj**. Bezpieczne hasło zbudujesz przy łącznym użyciu znaków z grup małych i dużych liter, cyfr i znaków specjalnych. Unikaj haseł trywialnych takich jak: Twoje imię, imię psa, data urodzenia itp. Pamiętaj, że hasło dzisiaj uważane za bezpieczne może nie być takim w przyszłości.
8. **Brak szyfrowania sesji nawiązywanej pomiędzy Tobą a portalem społecznościowym może skutkować** w najlepszym wypadku przejęciem lub zmanipulowaniem informacji, które w danym momencie wysyłasz, a w najgorszym **kradzieżą Twojej tożsamości** – podszyciem się pod Twoje dane w celu osiągnięcia korzyści.
9. **Publikując zdjęcia** z własnym wizerunkiem lub z wizerunkami innych osób musisz mieć świadomość, że **znacznie ułatwiasz identyfikację siebie i innych** oraz możesz przekazać w ten sposób znacznie więcej informacji niż zdajesz sobie sprawę.
10. Podając w portalu społecznościowym informacje o innej osobie oraz publikując jej zdjęcia, **upewnij się, że ta osoba nie ma nic przeciwko takiej publikacji**.
11. Pamiętaj, że pomimo zachowania prywatności w portalu, **Twoja anonimowość jest ograniczona** i nie istnieje dla osób utrzymujących portal oraz dla organów wymiaru sprawiedliwości w sytuacji naruszenia prawa.
12. Nie zapominaj, że nie tylko serwery portalu mogą o Tobie „coś wiedzieć" – z pewnością **niektóre informacje na Twój temat** mogą posiadać osoby zarządzające serwerami pośredniczącymi w połączeniu między Tobą a portalem.

Jak sprawdzić wiarygodność systemu

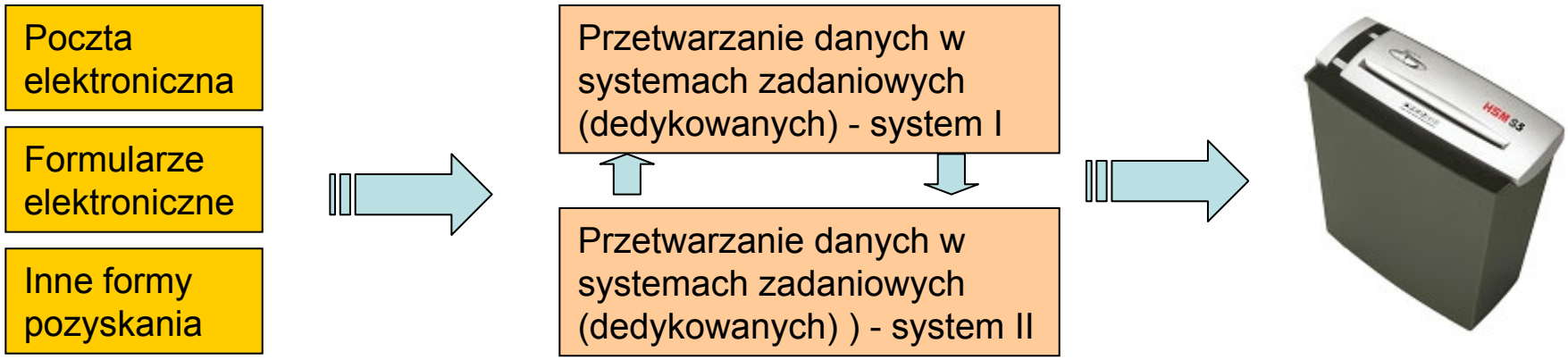




Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Procedury i środków bezpieczeństwa należy stosować w całym cyklu przetwarzania (od chwili pozyskania do usunięcia danych)

Szerokie spektrum zasad legalności i bezpieczeństwa przetwarzania danych osobowych sprawia, że zarządzania ochroną danych osobowych to nie pojedynczy mechanizm ochrony ale całokształt działań obejmujących cały cykl przetwarzania od chwili pozyskania danych do ich usunięcia.



Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Przykład elementów kontroli w cyklu przetwarzania danych osobowych

Wymagania	Kontrola	Dokumentacja stosowania	Zabezpieczenie wykonania
Poinformowanie podmiotu o celach przetwarzania danych osobowych i uzyskanie zgody	Wymagane jest posiadanie podpisanej przez podmiot deklaracji zgody. W przypadku pozyskiwania zgody droga elektroniczna należy stosować zasadę opt-in (np. checkbox)	Archiwizacja podpisanych dokumentów	Regularny audyt
Określenie celów przetwarzania i wykonanie obowiązku informacyjnego	Porównanie zakresu wprowadzanych danych z potrzebami osiągnięcia celu przetwarzania	Dokumentowanie celów przetwarzania i wykonania obowiązku informacyjnego	Regularna ocena, audyt
Ograniczenie zakresu do zidentyfikowanych celów	Przed rozpoczęciem pozyskiwania danych należy uzasadnić potrzebę pozyskiwania określonego zakresu danych	Dokumentacja wyboru ustalonego zakresu	Regularne raporty
Stosowanie minimalizacji zakresu danych	Ograniczenie danych do niezbędnych dla osiągnięcia celu	Dokumentacja działań, określenie wytycznych	Regularna ocena, audyt

Zalecenia standaryzacyjne dotyczące bezpieczeństwa wymiany danych osobowych drogą elektroniczną – element modelu centralnego

Przykład elementów kontroli w cyklu przetwarzania danych osobowych

Wymagania	Kontrola	Dokumentacja stosowania	Zabezpieczenie wykonania
Usuwanie danych po osiągnięciu celu	Określenie w procesie przetwarzania zadań usuwania lub anonimizacji danych osobowych po wykonaniu celu	Dokumentacja procesu usuwania, data realizacji	Regularna ocena i audyt
Zapewnienie podmiotom danych dostępu do informacji o przetwarzanych danych ich dotyczących	W procesie realizacji powinna być zapewniona identyfikacja podmiotu danych. Ponadto w procesie tym jeżeli realizowany jest drogą elektroniczna należy zapewnić bezpieczeństwo transmisji	Dokumentacja polityki informacyjnej. Dokumentacja wytycznych dotyczących transmisji	Regularna ocena i audyt
Sprawdzanie poprawności i jakości danych	Należy kontrolować dokładność i jakość wprowadzanych danych. Dane przechowywane przez dłuższy okres czasu powinny być poddawane weryfikacji	Dokumentacja przeprowadzanych kontroli	Regularna ocena i audyt. Jeśli możliwe przez stronę trzecią

Andrzej Kaczmarek
Biuro GIODO

Dziękuję za uwagę