Zastosowanie norm w ochronie danych osobowych

Andrzej Kaczmarek

Biuro
Generalnego Inspektora
Ochrony Danych Osobowych

11. 05. 2009 r. Wars

Generalny Inspektor
Ochrony Danych Osobowych
ul. Stawki 2, 00-193 Warszawa
www.giodo.gov.pl
kancelaria@giodo.gov.pl

PLAN

- Główne elementy ochrony danych osobowych
- Ustawy i rozporządzenia jako główne źródło przepisów prawa
- Bezpieczeństwo informacji, ochrona danych – jako zagadnienia ogólne i specjalistyczne.
- Co dają standardy.,
- Standardy jako uzupełnienie przepisów prawa

GŁÓWNE OBSZARY REGULACJI W ZAKRESI OCHRONY DANYCH OSOBOWYCH

DEFINICJE I ZASADY – DOMENĄ PRZEPISÓW PRAWA (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Definicje: Dane osobowe

1. **Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej.**
2. **Osobą możliwą do zidentyfikowania jest osoba, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.**
3. **Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań.**

DEFINICJE I ZASADY – DOMENĄ PRZEPISÓW PRAWA (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Definicje: zbiór danych, przetwarzanie

1. **Zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie,**
2. **Przetwarzaniu danych - rozumie się przez to 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.**

DEFINICJE I ZASADY – DOMENĄ PRZEPISÓW PRAWA (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Zasady przetwarzania – Przetwarzanie danych jest dopuszczalne tylko wtedy gdy:

1. **osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie dotyczących jej danych,**
2. **jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa,**
3. **jest to konieczne do realizacji umowy, gdy osoba, której dane dotyczą, jest jej stroną lub gdy jest to niezbędne do podjęcia działań przed zawarciem umowy na żądanie tej osoby,**
4. **jest niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego,**
5. **jest to niezbędne dla wypełnienia prawnie usprawiedliwionych celów realizowanych przez administratorów danych albo odbiorców danych, a przetwarzanie nie narusza praw i wolności osoby, której dane dotyczą.**

DEFINICJE I ZASADY – DOMENĄ PRZEPISÓW PRAWA (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Obowiązki ADO – obowiązek informacyjny

W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

1. **adresie swojej siedziby i pełnej nazwie, a w przypadku gdy administratorem danych jest osoba fizyczna - o miejscu swojego zamieszkania oraz imieniu i nazwisku,**
2. **celu zbierania danych, a w szczególności o znanych mu w czasie udzielania informacji lub przewidywanych odbiorcach lub kategoriach odbiorców danych,**
3. **prawie dostępu do treści swoich danych oraz ich poprawiania,**
4. **dobrowolności albo obowiązku podania danych, a jeżeli taki obowiązek istnieje, o jego podstawie prawnej.**

BEZPIECZEŃSTWO INFORMACJI W PRZEPISACH PRAWA (1)

- **Ustawa z dnia 29 września 1994 r. o rachunkowości Rozdział 8 Art. 71 ust.2** - Przy prowadzeniu ksiąg rachunkowych przy użyciu komputera ochrona danych powinna polegać na stosowaniu odpornych na zagrożenia nośników danych, na doborze stosownych środków ochrony zewnętrznej, na systematycznym tworzeniu rezerwowych kopii zbiorów danych zapisanych na informatycznych nośnikach danych, pod warunkiem zapewnienia trwałości zapisu informacji systemu rachunkowości, przez czas nie krótszy od wymaganego do przechowywania ksiąg rachunkowych, oraz na zapewnieniu ochrony programów komputerowych i danych systemu informatycznego rachunkowości, poprzez stosowanie odpowiednich rozwiązań programowych i organizacyjnych, chroniących przed nieupoważnionym dostępem lub zniszczeniem.

BEZPIECZEŃSTWO INFORMACJI W PRZEPISACH PRAWA (2)

- **Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Art. 36)** - Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r.** w sprawie dokumentacja przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych. Dz. U. Nr 100, poz. 1024 z 2004 r.)
- **Ustawa z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych.** (Dz. U. 1999 r. Nr 11 poz. 95, ze zm.) .

BEZPIECZEŃSTWO INFORMACJI W PRZEPISACH PRAWA (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo – Obowiązek zabezpieczenia danych

Art. 36 u.o.d.o.)

1. **Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.**
2. **Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.**

BEZPIECZEŃSTWO INFORMACJI W PRZEPISACH PRAWA (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo – Obowiązek zabezpieczenia danych

Art. 39a.

Minister właściwy do spraw administracji publicznej w porozumieniu z ministrem właściwym do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych i bezpieczeństwa przetwarzanych danych.

BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

1. Zarządzanie bezpieczeństwem informacji (ZBI) jest dziedziną interdyscyplinarna z pogranicza techniki, organizacji i prawa.
2. ZBI ma własna ciągle rozwijająca się terminologię i metodykę.
3. Kluczowymi pojęciami z obszaru ZBI są pojęcia: zasoby (aktywa), zagrożenia, podatności, następstwa, ryzyka.
4. ZBI wykorzystuje szereg modeli. Kluczowym modelem jest model związków pomiędzy elementami bezpieczeństwa oraz model związków w zarządzaniu ryzykiem.
5. ZBI w instytucji. Trójpoziomowy model hierarchii celów, strategii i polityk bezpieczeństwa.

I. Bezpieczeństwo instytucji
II. Bezpieczeństwo systemów informatycznych w instytucji
III. Bezpieczeństwo konkretnego systemu (serwera, klientów, łączności)

BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (2)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Bezpieczeństwo informacji: zachowanie poufności, integralności i dostępności informacji: PN-ISO/IEC 27000

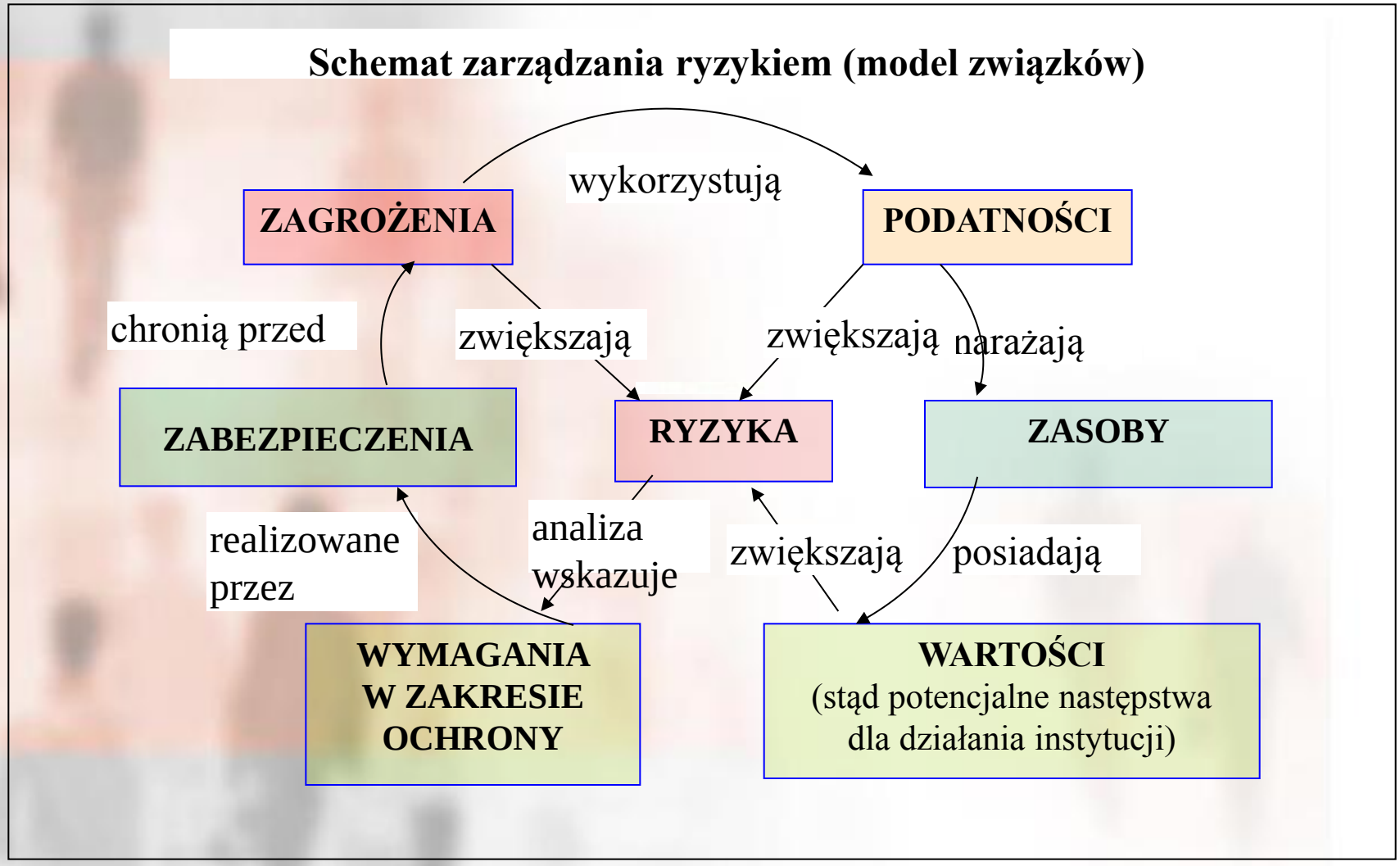
Poufność–zapewnienie, że informacja jest dostępna jedynie osobom upoważnionym

Integralność–zapewnienie dokładności i kompletności informacji oraz metod przetwarzania

Dostępność-zapewnienie ze osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy gdy jest to potrzebne

www.giodo.gov.pl

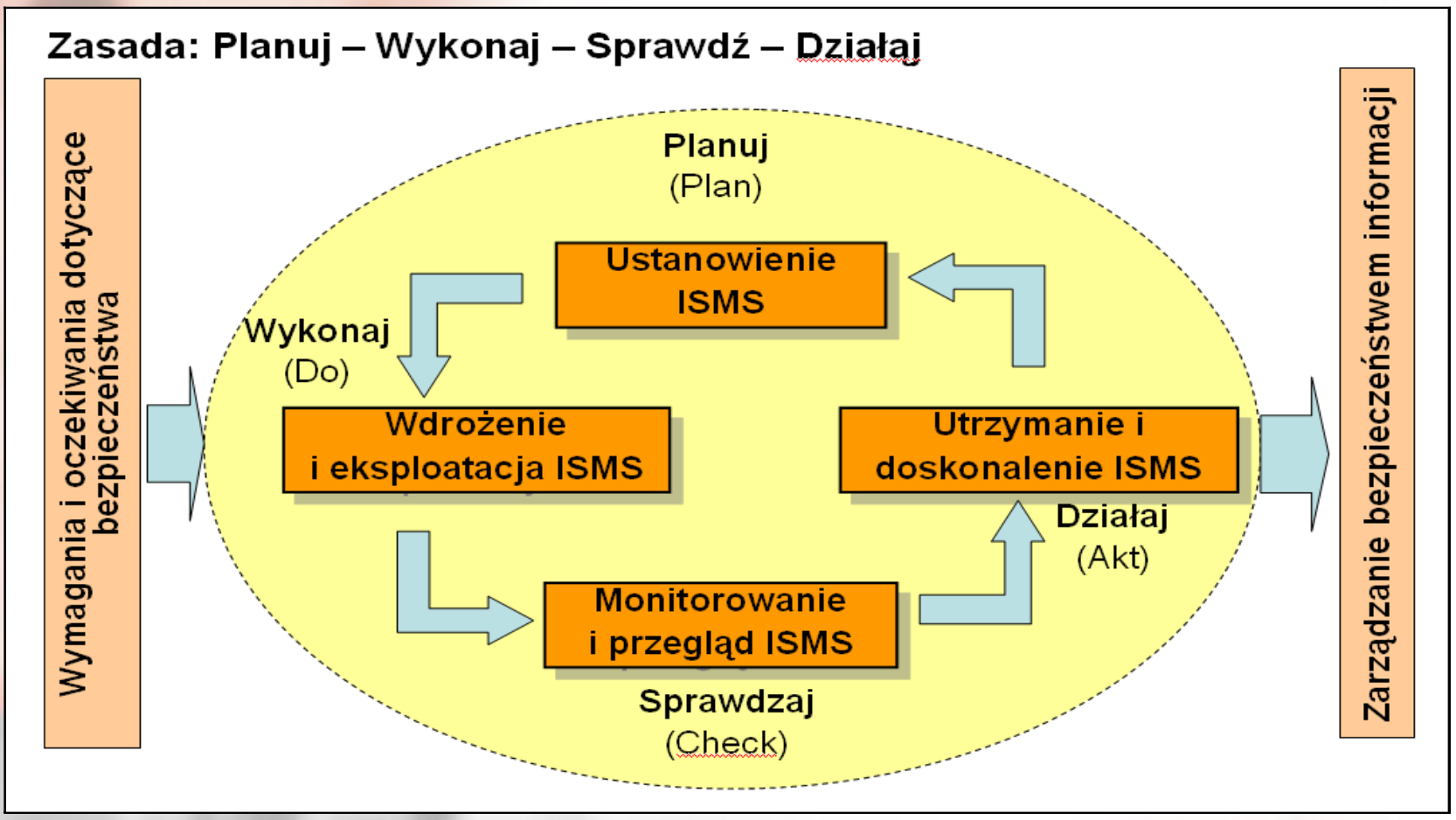
BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (3)



BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

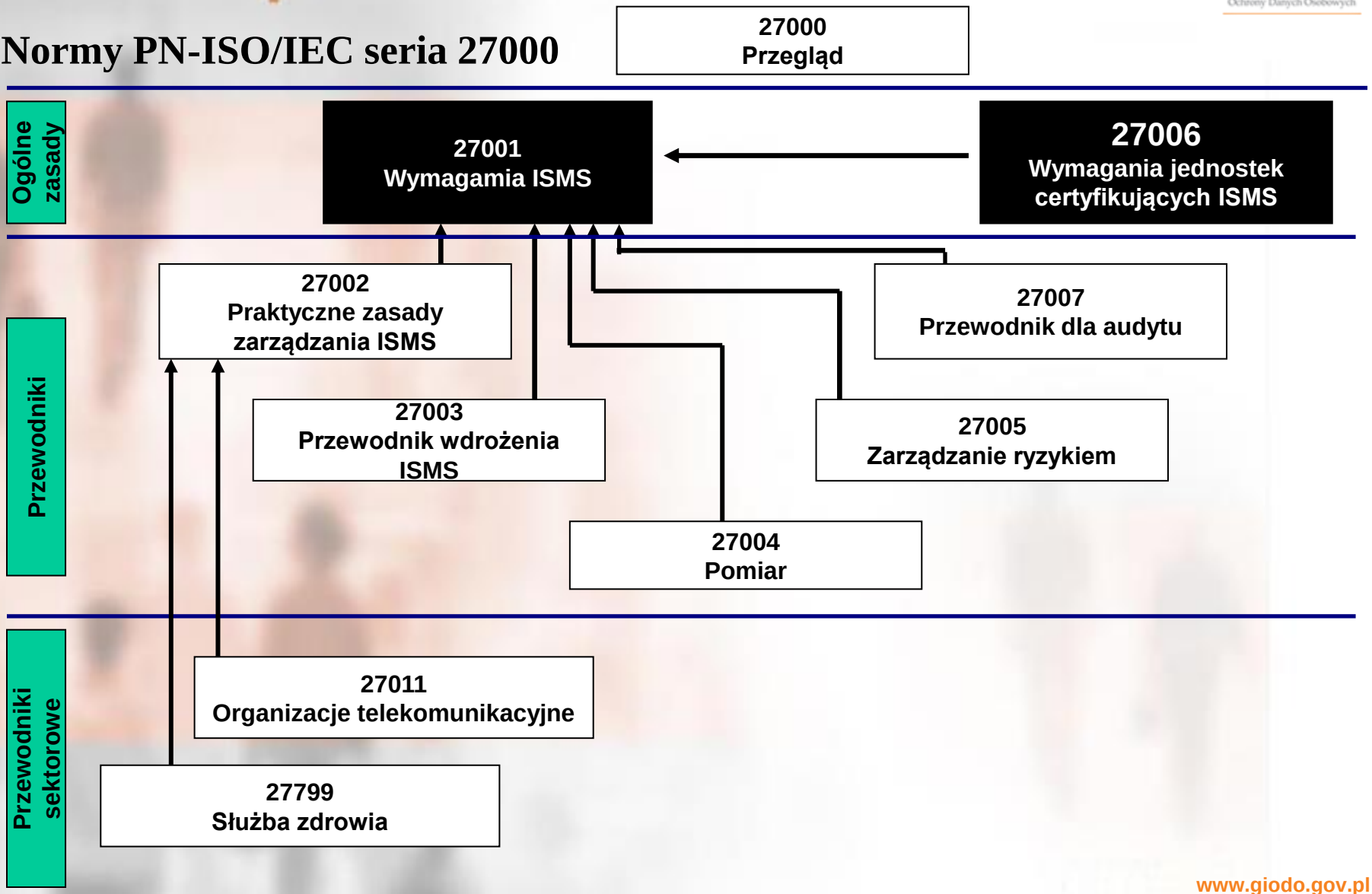
Zarządzanie bezpieczeństwem



BEZPIECZEŃSTWO JAKO PROBLEM OGÓLNY (5)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Normy PN-ISO/IEC seria 27000



www.giodo.gov.pl

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (6)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

NORMALIZACJA

LEGISLACJA

NORMY

- opracowywane przez zainteresowane strony w ramach jednostki normalizacyjnej
- mają status zaleceń

PRZEPISY TECHNICZNE

- przyjmowane przez prawodawcze organy państwa
- stanowią obowiązek prawny dla obywateli

www.giodo.gov.pl

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (7)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

POWOŁYWANIE SIĘ NA NORMY W PRZEPISACH

Powołanie w sposób wyłączny, z którego wynika, że jedynym sposobem spełnienia wymagań przepisu jest zgodność z normami na które się powołano

Powołanie wskazujące, z którego wynika, że jednym z możliwych sposobów spełnienia wymagań przepisu prawnego jest osiągnięcie zgodności z normami na które się powołano *(np. koncepcja norm zharmonizowanych z Dyrektywami Nowego Podejścia)*

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (1)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

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.**

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (2)

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.**

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (3)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV. § 15

1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne projektuje się, wdraża oraz eksploatuje z uwzględnieniem ich funkcjonalności, niezawodności, używalności, wydajności, przenoszalności i pielęgnowalności, przy zastosowaniu norm oraz uznanych w obrocie profesjonalnym standardów i metodyk.
2. Zarządzanie usługami realizowanymi przez systemy teleinformatyczne ma na celu dostarczanie tych usług na deklarowanym poziomie dostępności i odbywa się w oparciu o udokumentowane procedury.
3. Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeśli projektowanie, wdrażanie, eksploatowanie, monitorowanie, przeglądanie, utrzymanie i udoskonalanie zarządzania usługą podmiotu realizującego zadanie publiczne odbywają się z uwzględnieniem Polskich Norm: **PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2.**

www.giodo.gov.pl

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (4)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV. § 16

1. Systemy teleinformatyczne używane przez podmioty realizujące zadania publiczne wyposaża się w składniki sprzętowe lub oprogramowanie umożliwiające wymianę danych z innymi systemami teleinformatycznymi za pomocą protokołów komunikacyjnych i szyfrujących określonych w obowiązujących przepisach, normach, standardach lub rekomendacjach ustanowionych przez krajową jednostkę normalizacyjną lub jednostkę normalizacyjną Unii Europejskiej.

2. W przypadku gdy w danej sprawie brak jest przepisów, norm lub standardów, o których mowa w ust. 1, stosuje się standardy uznane na poziomie międzynarodowym, w szczególności opracowane przez:
   1) **Internet Engineering Task Force (IETF) i publikowane w postaci Request For Comments (RFC),**
   2) **World Wide Web Consortium (W3C) i publikowane w postaci W3C Recommendation (REC)**

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (5)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV. § 16

§ 19. W systemie teleinformatycznym podmiotu realizującego zadania publiczne służące prezentacji zasobów informacji należy zapewnić spełnienie przez ten system wymagań **Web Content Accessibility Guidelines (WCAG 2.0)**, z uwzględnieniem poziomu AA, określonych w załączniku nr 4 do rozporządzenia.

§ 20. 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

§ 20. 2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań:

BEZPIECZEŃSTWO W OBECNIE OBOWIĄZUJĄCYCH PRZEPISACH PRAWA (6)

GIODO
Generalny Inspektor Ochrony Danych Osobowych

Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności (..).

Rozdział IV. § 16 § 20. 2.

1) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;

2) utrzymywania aktualności inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację;

3) przeprowadzania okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowania działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;

---

§ 20. 3 Wymagania określone w ust. 1 i 2 uznaje się za spełnione, jeżeli system zarządzania bezpieczeństwem informacji został opracowany na podstawie Polskiej Normy **PN-ISO/IEC 27001**, a ustanawianie zabezpieczeń, zarządzanie ryzykiem oraz audytowanie odbywa się na podstawie Polskich Norm związanych z tą normą, w tym:. **1) PN-ISO/IEC 17799, 2) PN-ISO/IEC 27005, 3) PN-ISO/IEC 24762**

Dziękuję za uwagę

Andrzej Kaczmarek

BIURO

GENERALNEGO INSPEKTORA OCHRONY

DANYCH OSOBOWYCH