Stowarzyszenie Administratorów Bezpieczeństwa Informacji

System ochrony danych osobowych a System Zarządzania Bezpieczeństwem Informacji

- w kontekście normy PN-ISO 27001:2014 oraz Rozporządzenia o Krajowych Ramach Interoperacyjności

Marcin Soczko

Stowarzyszenie Administratorów Bezpieczeństwa Informacji, CODGiK

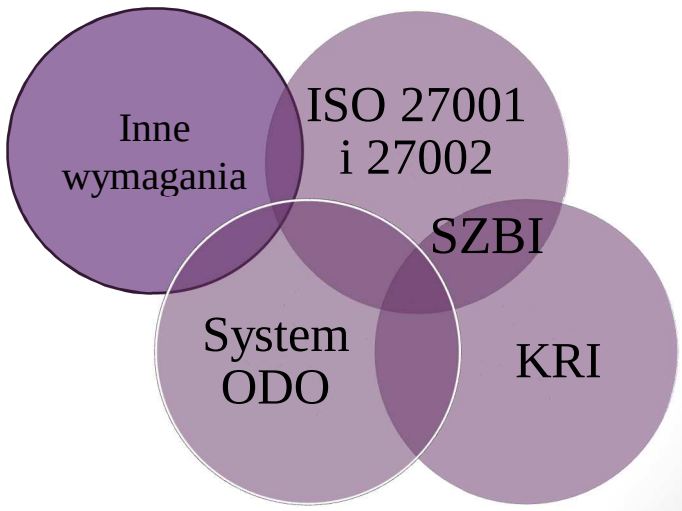
Agenda

- Źródła wymagań dotyczących bezpieczeństwa informacji
- System Ochrony Danych Osobowych (ODO) a System Zarządzania Bezpieczeństwem Informacji
  - Analiza ryzyka
  - Dokumentacja
  - Sprawdzanie zgodności, audyt wewnętrzny
  - Zapoznawanie, uświadamianie, szkolenia
  - Bezpieczeństwo zasobów ludzkich
  - Rozliczalność
  - Kontrola dostępu
  - Bezpieczeństwo fizyczne i środowiskowe
  - Ochrona przed szkodliwym oprogramowaniem
  - Ciągłość działania
  - Kopie zapasowe
  - Urządzenia mobilne
  - Postępowanie z nośnikami
  - Bezpieczeństwo sprzętu i aktywów poza siedzibą
  - Dostęp do sieci i usług sieciowych
  - Kryptografia
  - Zgodność
- Podsumowanie

Źródła wymagań dotyczących bezpieczeństwa informacji

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2014 r. poz. 1182 z późn. zm.; UODO)
  - Rozporządzenie 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; RT/O),
- Rozporządzenie w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526; KRI)
  - na podstawie art. 18 ustawy 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)
- normy ISO
  - cała grupa norm z serii 27000 – SZBI (ISO 27001, ISO 27002)
  - PN-ISO/IEC 20000-1 i PN-ISO/IEC 20000-2 – zarządzanie usługami
  - PN-ISO/IEC 24762 – odtwarzanie w ramach ciągłości działania
  - PN-ISO 31000:2012 – ogólne wytyczne dotyczące zarządzania ryzykiem

System ODO a SZBI



Analiza ryzyka

- UODO Art. 36. 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.
- KRI § 20. 2. 3) Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez (…) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- PN-EN ISO IEC 27001:2014-12 pkt. 6 Planowanie i pkt. 8 Działania operacyjne

Dokumentacja

- UODO Art. 36 2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki [techniczne i organizacyjne zapewniające ochronę oraz]
- UODO Art. 36a 2. 1) b) [do jego zadań należy] nadzorowanie (…) aktualizowania dokumentacji, o której mowa (…);
- KRI § 20. 2. 1) (…) zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie (…) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- ISO 27001 pkt. 7.5 Udokumentowane informacje

Realizacja: RTO § 4 i § 5 + kontrola wersji, integralność PBDO i IZSI (uprawnienia do edycji), a wgląd wewnątrz organizacji

Sprawdzanie zgodności, audyt wewnętrzny

- Art. 36a 2. 1) a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych (…); b) nadzorowanie (…) zasad określonych [w PBDO];
- RT/O zał. część A. VII Administrator danych monitoruje wdrożone zabezpieczenia systemu informatycznego.
- KRI § 20. 2. 14) zapewnienie okresowego audytu wewnętrznego w zakresie bezpieczeństwa informacji, nie rzadziej niż raz na rok.
- ISO 27001 pkt. 9.2 Audyt wewnętrzny

Realizacja: program audytów realizowany przez odpowiednich audytorów i odpowiednio dokumentowany, a wyniki sprawozdawane kierownictwu

Zapoznawanie, uświadamianie, szkolenia

- UODO Art. 36a 2. 1) c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
- KRI § 20. 2. 6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
- ISO 27001 7.2.2 Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

Bezpieczeństwo zasobów ludzkich

- UODO Art. 37. Do przetwarzania danych mogą być dopuszczone wyłącznie osoby posiadające upoważnienie nadane przez ADO.
- Art. 39. 2. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia.
- KRI – brak
- ISO 27001 pkt. 7.1.2 Warunki zatrudnienia

- Realizacja – np. powiązanie zakresu upoważnienia z zakresem obowiązków pracownika lub opisem stanowiska, na którym został zatrudniony

Rozliczalność

- UODO Art. 38. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
- RT/O § 7 Obowiązek zapewnienia odnotowania w systemie informatycznym szeregu informacji dla każdej osoby, której dane osobowe są w nim przetwarzane
- KRI § 21. ust. 1. – 5.
- ISO 27002 pkt. 12.4 Rejestrowanie zdarzeń i monitorowanie

- Realizacja zgodnie z RT/O

Kontrola dostępu

- Art. 39. 1. Administrator danych prowadzi ewidencję osób upoważnionych do ich przetwarzania, która powinna zawierać: 1) imię i nazwisko osoby upoważnionej; 2) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych; 3) identyfikator (...) w systemie informatycznym.
- RT/O zał. część A. II oraz IV ust. 1. i 2. oraz część B. VIII – wymagania dotyczące identyfikatorów i haseł
- KRI § 20. 2. 4) podejmowanie działań zapewniających, że osoby zaangażowane w proces przetwarzania informacji posiadają stosowne uprawnienia i uczestniczą w tym procesie w stopniu adekwatnym do realizowanych przez nie zadań oraz obowiązków mających na celu zapewnienie bezpieczeństwa informacji;
- ISO 27002 pkt. 9.4 Kontrola dostępu do systemów i aplikacji

Bezpieczeństwo fizyczne i środowiskowe

- RT/O A. I 1. Obszar [przetwarzania danych] zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych do przetwarzania danych osobowych. 2. Przebywanie osób nieuprawnionych w obszarze [przetwarzania danych] jest dopuszczalne za zgodą administratora danych lub w obecności osoby upoważnionej do przetwarzania danych osobowych.
- KRI § 20. 2. 9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- ISO 27002 pkt. 11.1.2 Fizyczne zabezpieczenie wejścia
- Realizacja – np. nadzorowanie pobytu gości (tzw. księga gości), identyfikatory, karty dostępu

Ochrona przed szkodliwym oprogramowaniem

- RT/O A. III System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed (…) działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego;
- KRI – brak
- ISO 27002 pkt. 12.2 Ochrona przed szkodliwym oprogramowaniem

- Realizacja – np. stosowanie odpowiednio skonfigurowanego oprogramowania antywirusowego (a najlepiej równolegle dwóch różnych narzędzi); podnoszenie na szkoleniach świadomości pracowników nt. zagrożeń; izolowanie środowisk szczególnie wrażliwych

Ciągłość działania

- RT/O A. III System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed (…) utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
- KRI § 20. 2. 12) b) minimalizowanie ryzyka utraty informacji w wyniku awarii,
- ISO 27002 pkt. 17.2.1 Dostępność środków przetwarzania informacji

- Realizacja – np. zastosowanie nadmiarowych komponentów, tzw. redundancja (podwojenie) elementów architektury, dostawców prądu; stosowanie systemów UPS, generatorów prądu

Kopie zapasowe

- RT/O A. IV 3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. 4. Kopie zapasowe: a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem; b) usuwa się niezwłocznie po ustaniu ich użyteczności
- KRI § 20. 2. 9) zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikacje, usunięcie lub zniszczenie;
- ISO 27002 pkt. 12.3 Kopie zapasowe

- Realizacja – testowanie odtwarzania kopii zapasowych i przechowywanie w innej lokalizacji niż system produkcyjny; szyfrowanie nośników; rejestr kopii zapasowych

Urządzenia mobilne

- RT/O A. V Osoba użytkująca komputer przenośny zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania poza obszarem [przetwarzania danych], w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych.
- KRI § 20. 2. 8) ustanowienia podstawowych zasad gwarantujących bezpieczną pracę przy przetwarzaniu mobilnym i pracy na odległość;
- KRI § 20. 2. 11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- ISO 27002 pkt. 6.2.1 Polityka stosowania urządzeń mobilnych

- Realizacja – wykaz urządzeń mobilnych; szyfrowanie dysków twardych; zasady zdalnego dostępu do zasobów w siedzibie

Postępowanie z nośnikami

- RT/O B. IX Urządzenia i nośniki zawierające dane osobowe [wrażliwe], przekazywane poza obszar [przetwarzania], zabezpiecza się w sposób zapewniający poufność i integralność tych danych.
- RT/O A. VI Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do (…) likwidacji — pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
- KRI – brak
- ISO 27002 pkt. 8.3 Postępowanie z nośnikami

- Realizacja – np. szyfrowanie; redundancja (również w innej postaci); rejestr nośników (w tym wycofanych); monitorowanie kopiowania; zasady transportu

Bezpieczeństwo sprzętu i aktywów poza siedzibą

- RT/O A. VI Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do (...) przekazania podmiotowi nieuprawnionemu do przetwarzania danych — pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie; [a przeznaczone do] naprawy — pozbawia się wcześniej zapisu tych danych (…) albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych.
- KRI § 20. 2. 11) ustalenia zasad postępowania z informacjami, zapewniających minimalizację wystąpienia ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
- ISO 27002 pkt. 11.2.6 Bezpieczeństwo sprzętu i aktywów poza siedzibą
- ISO 27002 pkt. 11.2.7 Bezpieczne zbywanie lub przekazywanie do ponownego użycia

- Realizacja – np. autoryzacja wyniesienia sprzętu poza siedzibę; dziennik

Dostęp do sieci i usług sieciowych

- RT/O C. XII 1. System informatyczny służący do przetwarzania danych osobowych chroni się przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem. 2. W przypadku zastosowania logicznych zabezpieczeń (…) obejmują one: a) kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną; b) kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych.
- KRI § 20. 2. 7) c) zapewnienie środków uniemożliwiających nieautoryzowany dostęp na poziomie systemów operacyjnych, usług sieciowych i aplikacji;
- ISO 27002 pkt. 9.1.2 Dostęp do sieci i usług sieciowych

- Realizacja: autoryzacja i monitorowanie dostępu do sieci (w tym bezprzewodowych) i poszczególnych usług; kanały VPN

Kryptografia

- RT/O C. XIII Administrator danych stosuje środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.
- KRI § 20. 2. 12) d) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na (…) stosowaniu mechanizmów kryptograficznych w sposób adekwatny do zagrożeń lub wymogów przepisu prawa,
- ISO 27002 pkt. 10.1.1 Polityka stosowania zabezpieczeń kryptograficznych

- Realizacja: ujednolicenie zasad stosowanych w organizacji; zbadanie wpływu szyfrowania na inne zabezpieczenia; HTTPS

Zgodność

- UODO rozdział 3, 4, 6 i 7
  - Przesłanka legalności (podstaw prawnych), na podstawie których przetwarzane są dane osobowe (art. 23 i 27),
  - Realizacja obowiązku informacyjnego, w tym poprawności klauzul informacyjnych i oświadczeń na formularzach do zbierania danych (art. 24 i 25),
  - Realizacja obowiązków dotyczących celowości, adekwatności i czasu przetwarzania danych osobowych (art. 26),
  - Poprawność wypełnienia obowiązków związanych z powierzaniem danych innym podmiotom lub przez inny podmiot (art. 31),
  - Realizacja praw osób, których dane są przetwarzane (art. 32 i 33),
  - Realizacja obowiązku rejestracji (i aktualizacji) zbiorów danych (art. 40 i 41),
  - Poprawność procedur dotyczących udostępniania danych do państw trzecich – poza UE (art. 47 i 48).
- KRI § 20. 2. 12) h) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na (…) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
- ISO 27002 pkt. 18.1.4 Prywatność i ochrona danych identyfikujących osobę

Podsumowanie

- Wybór modelu zapewniania przestrzegania przepisów o ochronie danych osobowych (ABI / bez ABI)
- Stosowanie wymagań prawnych lub normatywnych w jednym albo drugim modelu
- Podział obowiązków wynikających z SZBI i ODO albo ich połączenie