ENSI
KANCELARIA EKSPERTÓW

Stowarzyszenie Administratorów Bezpieczeństwa Informacji

# Znaczenie norm ISO we wdrażaniu bezpieczeństwa technicznego i organizacyjnego wymaganego w RODO

*Maciej Byczkowski*

© ENSI 2017

## Nowe podejście do ochrony danych osobowych w RODO

- ***Risk based approach*** – podejście oparte na ryzyku:
  - Założenie: im ryzyko związane z przetwarzaniem danych osobowych jest większe, tym większy powinien być zakres obowiązków ciążących na ADO
  - Skuteczne zastosowanie się do tej zasady wymaga szacowania przez ADO ryzyka związanego z przetwarzaniem danych osobowych, zarówno w zakresie identyfikacji zagrożeń związanych z przetwarzaniem, jak i naruszenia praw i wolności osób, których dane dotyczą
  - Szacowanie ryzyka w celu doboru zabezpieczeń jest podstawą dla standardów związanych z zarządzaniem bezpieczeństwem informacji (w tym: **ISO/IEC 27005**, oraz **ISO/IEC 29134**)

© ENSI 2017



Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Nowe podejście do ochrony danych osobowych w RODO

- **Zasada rozliczalności**:
  - ADO powinien być w stanie wykazać, że stosowane przez niego metody są zgodne z RODO oraz skuteczne
  - zastosowanie się do tej zasady wymaga wdrożenia odpowiednich procedur i prowadzenia odpowiedniej dokumentacji, dzięki którym łatwiej będzie wykazać fakt spełniania wymogów przewidzianych przez RODO
  - rozliczalność jest odpowiednikiem kategorii zabezpieczenia zdefiniowanej w normach jako zgodność, a jego realizacja jest związana zapewnianiem zgodności podejmowanych działań przy przetwarzaniu informacji zarówno z wymogami prawnymi, jak i przyjętymi w organizacji zasadami jej ochrony (w tym: ISO/IEC **27001**, ISO/IEC **27002**, ISO/IEC **29151**)
  - Jest też jedną z podstawowych zasad prywatności określoną w normie ISO/IEC **29100**

© ENSI 2017

## Zapewnienie przetwarzania danych zgodnie z RODO

- Wdrożenie przez ADO odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać (art. 24)
- Uwzględnianie przez ADO ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*) (art. 25)
- Wdrożenie przez ADO oraz procesora środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa danych odpowiedni do ryzyka związanego naruszeniem praw osób, których dane dotyczą (art. 32)
- Ocena skutków planowanych operacji przetwarzania dla ochrony danych (art. 35)

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Szacowanie ryzyka (PIA)

- Wymogi szacowania ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia w celu zapewnienia przetwarzania danych zgodnie z RODO (art. 24, 25, 32, 35)
  - Minimalizacja zagrożeń poprzez dobór odpowiednich zabezpieczeń
- Privacy impact assessment (PIA)

© ENSI 2017

## Wymóg stosowania zabezpieczeń

Art. 32 ust. 2 – Bezpieczeństwo przetwarzania:

- Przy doborze zabezpieczeń należy ocenić, czy stopień bezpieczeństwa danych jest odpowiedni, uwzględnia się w szczególności **ryzyko wiążące się z ich przetwarzaniem**, wynikające z:
  - przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji;
  - nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Wymóg stosowania zabezpieczeń

- W art. 32 RODO zostały wskazane przykładowe środki techniczne i organizacyjne zabezpieczenia danych:
  - pseudonimizacja i szyfrowanie danych osobowych
  - zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania
  - zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego
  - regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania
- Nie jest to zamknięty katalog zabezpieczeń, a wymienione kategorie zabezpieczeń powinny być dobierane adekwatnie do potrzeb, które wynikają z procesu szacowania ryzyka.

© ENSI 2017

## Ocena skutków dla ochrony danych

**Data protection impact assessment** (DPIA)

- Ocena skutków **planowanych operacji przetwarzania** dla ochrony danych osobowych wykonywana jest przez ADO zgodnie z Art. 35 ust. 1 i 2, <u>jedynie w szczególnych sytuacjach:</u>
  - jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**,
  - przed rozpoczęciem przetwarzania
- Głównym elementem oceny skutków jest **ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą (PIA)** – art. 35 ust. 7 lit. c

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Ocena skutków dla ochrony danych

Art. 35 ust. 3:

- Ocena skutków dla ochrony danych jest wymagana w szczególności w przypadku:
  - systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną
  - przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10
  - systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie

© ENSI 2017

## Wykorzystanie norm ISO w ochronie danych osobowych

- Normy dotyczące ochrony danych identyfikujących osobę (**Personally Identifiable Information - PII**):
  - serii ISO/IEC 29100
- Normy dotyczące zarządzania bezpieczeństwem informacji:
  - serii ISO/IEC 27000
- Normy dotyczące zarządzania ryzykiem:
  - serii ISO 31000

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Wykorzystanie norm ISO w ochronie danych osobowych

- Normy ISO/IEC dotyczące ochrony danych identyfikujących osobę (PII)
  - **PN-ISO/IEC 29100**:2017-07 – „Ramy prywatności" – wersja angielska
    - **ISO/IEC 29100:2011** – „Privacy framework"
  - **ISO/IEC 29134**:2017 – „Guidelines for privacy impact assessment"
  - **ISO/IEC 29151**:2017 – „Code of practice for personally identifiable information protection"

© ENSI 2017

## Wykorzystanie norm ISO w ochronie danych osobowych

- Normy dotyczące zarządzania bezpieczeństwem informacji:
  - **PN-ISO/IEC 27001**:2017-06 – „Systemy zarządzania bezpieczeństwem informacji – wymagania" – wersja angielska
    - Zastąpiła PN-ISO/IEC 27001:2014-12
  - **PN-ISO/IEC 27002**:2017-06 – „Praktyczne zasady zabezpieczania informacji" – wersja angielska
    - Zastąpiła PN-ISO/IEC 27002:2014 -12

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Wykorzystanie norm ISO w ochronie danych osobowych

- Normy dotyczące zarządzania bezpieczeństwem informacji:
  - **PN-ISO/IEC 27005**:2014-01 – "Zarządzanie ryzykiem w bezpieczeństwie informacji"
  - **PN-ISO/IEC 27017**:2017-07 – „Praktyczne zasady zabezpieczania informacji na podstawie ISO/IEC 27002 dla usług w chmurze" – wersja angielska
  - **PN-ISO/IEC 27018**:2017-07 – "Praktyczne zasady ochrony danych identyfikujących osobę (PII) w chmurach publicznych działających jako przetwarzający PII" – wersja angielska

© ENSI 2017

## Wykorzystanie norm ISO w ochronie danych osobowych

- Normy dotyczące zarządzania ryzykiem:
  - **PN-ISO 31000**:2012 – "Zarządzanie ryzykiem - zasady i wytyczne"
  - **PN-EN 31010**:2010 – „ Zarządzanie ryzykiem -- Techniki oceny ryzyka" – wersja angielska

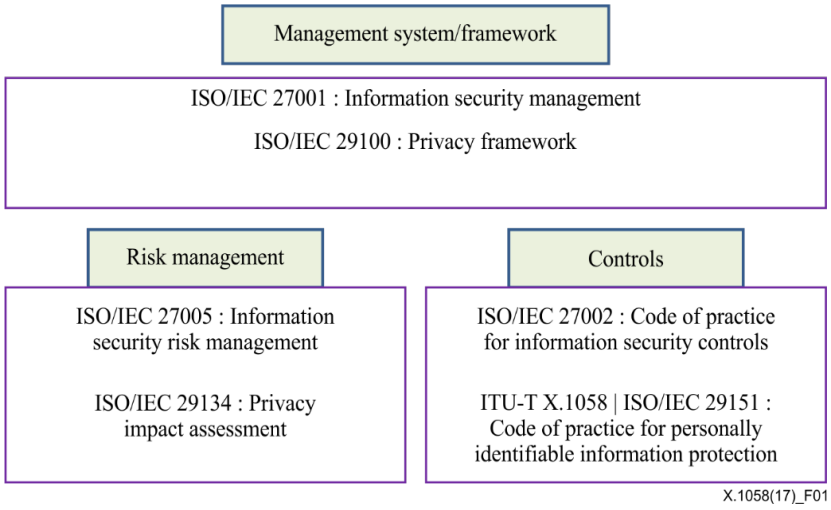
© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Powiązanie norm serii 29100 z normami serii 27000




*Źródło: ISO/IEC 29151*

## Ramy prywatności – ISO/IEC 29100

- Norma wydana w 2011 r. w trakcie prac nad pierwszym projektem RODO (25.01.2012 r.)
- Miała kluczowy wpływ na wymogi dotyczące szacowania ryzyka (PIA) oraz sposobu doboru środków technicznych i organizacyjnych zabezpieczenia danych określonych w RODO.
- Definiuje takie pojęcia jak pseudonimizacja czy uwzględnianie ochrony danych w fazie projektowania – ***privacy by design***

© ENSI 2017



© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Ramy prywatności – ISO/IEC 29100

- Norma określa proces zarządzania ryzykiem prywatności oraz wskazuje, że jednym z jej wyników może być **ocena wpływu na prywatność**, będąca składnikiem zarządzania ryzykiem, które skupia się na zapewnianiu zgodności z wymogami prawnymi dotyczącymi ochrony prywatności i danych oraz ocenie wpływu nowych lub znacząco zmienionych technologii IT lub operacji przetwarzania na prywatność.

© ENSI 2017

## Ramy prywatności – ISO/IEC 29100

- **Norma wyznacza ramy prywatności**, które:
  - definiują wspólne nazewnictwo dotyczące prywatności
  - definiują uczestników przetwarzania danych identyfikujących osoby (PII) oraz ich role w tym procesie
  - opisują wymogi w zakresie ochrony prywatności
  - wskazują podstawowe zasady prywatności (11 pryncypiów).

© ENSI 2017



© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Ramy prywatności – ISO/IEC 29100

- W szczególności ramy prywatności odnoszą się do technologii informatycznych służących do przetwarzania danych określając:
  - uczestników przetwarzania i ich role
  - interakcje pomiędzy uczestnikami przetwarzania
  - metody rozpoznawania PII (identyfikacja danych w systemie)
  - metody ograniczania możliwości identyfikacji osób – pseudonimizacja danych oraz zasady przechowywania danych
  - uwzględnianie ochrony danych w fazie projektowania
  - wymogi w zakresie ochrony prywatności – wskazanie czynników, które mogą oddziaływać na wymogi ochrony danych w różnych organizacjach
  - identyfikacja wymogów, szacowanie ryzyka, ocena skutków dla podmiotów danych, monitoring mechanizmów kontroli
  - wymogi dla tworzenia polityki prywatności oraz szczegółowych zasad i obowiązków dla ochrony danych
  - mechanizmy kontroli prywatności – zarówno w fazie projektowania, jak i podczas przetwarzania danych.

© ENSI 2017

## Pryncypia prywatności

1. Zgoda i wybór – w tym zapewnienie możliwości swobodnego wyrażania zgody na przetwarzanie danych osobowych
2. Legalność i określenie celów – przetwarzanie danych w prawnie uzasadnionych celach
3. Ograniczenie zbierania danych – jedynie do dozwolonych w granicach prawa i niezbędnych do określonego celu ich przetwarzania
4. Minimalizacja danych

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Pryncypia prywatności

5. Ograniczenia dotyczące używania, przechowywania i ujawniania danych
6. Prawidłowość i jakość danych
7. Otwartość, przejrzystość i zawiadamianie – realizacja praw osób, których dane dotyczą
8. Indywidualne uczestnictwo i dostęp – umożliwienie dostępu do danych
9. Rozliczalność (odpowiedzialność)
10. Bezpieczeństwo informacji
11. Zapewnienie zgodności z zasadami prywatności

© ENSI 2017

## ISO/IEC 29100 - zastosowanie

- Norma będzie przydatna w szczególności przy:
  - tworzeniu i wdrożeniu polityk ochrony danych, o których mowa w art. 24 ust. 2 RODO (określonych w normie jako polityki prywatności),
  - określaniu polityk lub procedur związanych z uwzględnianiem ochrony danych w fazie projektowania (*privacy by design*) oraz domyślnej ochrony danych (*privacy by default*) zgodnie z art. 25 RODO.
  - wyborze mechanizmów kontroli prywatności, w tym procedur związanych z monitorowaniem ochrony danych zarówno przez administratora danych (art. 24 ust. 1 zd. 2 , 32 ust. 1 lit. d), jak i inspektora ochrony danych (art. 39 ust. 1 lit. b).

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

# Proces zarządzania ryzykiem

- Standardy dotyczące procesu zarządzania ryzykiem zostały określone w normie **ISO 31000** - ogólny schemat procesu zarządzania ryzykiem uwzględnia:
  - Ustanowienie kontekstu
  - Szacowanie ryzyka:
    - Identyfikowanie ryzyka
    - Analiza ryzyka
    - Ocena ryzyka
  - Postępowanie z ryzykiem
  - Monitorowanie i przegląd ryzyka
  - Informowanie i konsultowanie ryzyka

© ENSI 2017

# Szacowanie ryzyka - etapy

W normie **ISO/IEC 27005** zostały określone szczegółowe etapy procesu szacowania ryzyka w bezpieczeństwie informacji w tym:

1. Określenie kontekstu
2. Wykonanie szacowania ryzyka
   - Identyfikowanie ryzyka
     - Zidentyfikowanie aktywów
     - Zidentyfikowanie zagrożeń dla aktywów
     - Zidentyfikowanie istniejących zabezpieczeń
     - Zidentyfikowanie podatności
     - Zidentyfikowanie następstw (scenariusze incydentów)
   - Dokonanie analizy ryzyka
     - Oszacowanie następstw
     - Oszacowanie prawdopodobieństwa incydentu
     - Określenie poziomu ryzyka
   - Ocena ryzyka

© ENSI 2017



Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Szacowanie ryzyka - etapy

3. Postępowanie z ryzykiem:
   - Ustalenie planu postępowania z ryzykiem
   - Warianty postępowania z ryzykiem
     - modyfikowanie ryzyka
     - zachowanie ryzyka
     - unikanie ryzyka
     - dzielenie ryzyka
4. Oszacowanie ryzyka szczątkowego (rezydualnego)
5. Akceptowanie ryzyka:
   - Formalne udokumentowanie decyzji o zaakceptowaniu ryzyka
6. Monitorowanie i przegląd ryzyka

© ENSI 2017

## ISO/IEC 27005 - zastosowanie

- Zasady opisane w normie mogą być stosowane przy realizacji wymogów dotyczących szacowania ryzyka naruszenia praw i wolności osób, których dane dotyczą (PIA), które są określone w art. 24, 25, 32 lub 35 RODO.
- W stosowanych obecnie metodykach szacowania ryzyka opartych o normę, należy uwzględnić ocenę skutków dla osoby, której dane dotyczą.

© ENSI 2017



Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Wytyczne dla PIA – ISO/IEC 29134

- Norma zawiera wskazówki do:
  - Przeprowadzenia procesu szacowania skutków dla prywatności osoby, której dane dotyczą (PIA)
  - Struktury i zawartości raportu z przeprowadzenia PIA
- Może być stosowana w różnych sytuacjach dotyczących przetwarzania PII, np:
  - Identyfikacji skutków, ryzyk i odpowiedzialności dotyczących prywatności
  - Dostarczania wskazówek do zapewniania ochrony PII w fazie projektowania (privacy by design)
  - Ograniczania ryzyka związanego z przetwarzaniem PII w odniesieniu do pryncypiów prywatności (ISO 29100)

© ENSI 2017

## Wytyczne dla PIA – ISO/IEC 29134

- Określenie kiedy PIA jest wymagane
- Przygotowanie PIA
- Przeprowadzanie PIA
- Działania po zakończeniu PIA
- Przygotowanie raportu z PIA
- Skale i kryteria dotyczące szacowania poziomu oddziaływania i prawdopodobieństwa jego wystąpienia
- Lista typowych zagrożeń dla PII
- Przykłady ilustrujące proces PIA

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## ISO/IEC 29134 - zastosowanie

- Wytyczne mogą być stosowane w powiązaniu z wytycznymi normy **ISO/IEC 27005** przy realizacji wymogów dotyczących szacowania ryzyka naruszenia praw i wolności osób, których dane dotyczą (PIA), które są określone w art. 24, 25, 32 lub 35 RODO.
- Norma wskazuje również, że dobór zabezpieczeń PII w celu minimalizacji oszacowanego ryzyka powinien być realizowany przy pomocy normy **ISO/IEC 29151** – Praktyczne zasady zabezpieczania PII

© ENSI 2017

## Dobór zabezpieczeń PII – ISO 29151

- Norma **ISO/IEC 29151** określa wytyczne dotyczące doboru zabezpieczeń dla ochrony PII w odniesieniu do pryncypiów prywatności określonych w normie ISO/IEC **29100** (12 kategorii).
- Jako **główne źródła wymagań** norma wskazuje:
  - wymagania prawne, statutowe lub kontraktowe związane z ochroną PII;
  - szacowanie ryzyk dla organizacji oraz dla PII (ryzyka bezpieczeństwa i prywatności – BIA i PIA);
  - polityki korporacyjne.

© ENSI 2017



© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Praktyczne zasady zabezpieczenia PII – ISO 29151

- Zabezpieczenia PII powinny być dobierane na podstawie szacowania ryzyka (PIA) np. zgodnie z wytycznymi normy **ISO/IEC 29134**
- Specyfikacja opisanych w normie zabezpieczeń odnosi się do kategorii zabezpieczeń określonych w normie **ISO/IEC 27002**
- Norma zawiera rozszerzony zbiór zabezpieczeń dla ochrony PII – podział na 12 kategorii w odniesieniu do pryncypiów prywatności określonych w normie **ISO/IEC 29100**

© ENSI 2017

## Praktyczne zasady zabezpieczania informacji – ISO/IEC 27002

- Norma **PN-ISO/IEC 27002** określa zalecenia dotyczące standardów bezpieczeństwa informacji, w tym wyboru wdrażania i zarządzania zabezpieczeniami z uwzględnieniem środowiska, w którym w organizacji występuje ryzyko w bezpieczeństwie informacji.
- Norma zawiera 35 głównych kategorii zabezpieczeń i 114 zabezpieczeń.

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

## Praktyczne zasady zabezpieczania informacji – ISO/IEC 27002

- Każda główna kategoria zabezpieczeń zawiera:
  - cel stosowania zabezpieczenia, określający co należy osiągnąć
  - co najmniej jedno zabezpieczenie, które można zastosować aby osiągnąć cel stosowania zabezpieczenia
- Opisy zabezpieczenia:
  - Szczegółowa deklaracja zabezpieczenia
  - Wskazówki dotyczące wdrożenia zabezpieczenia
  - Informacje dodatkowe, w tym aspekty prawne i odwołania do innych norm.

© ENSI 2017

## Kategorie zabezpieczeń informacji – ISO/IEC 27002

- Polityki bezpieczeństwa informacji
- Organizacja bezpieczeństwa informacji
- Bezpieczeństwo zasobów ludzkich
- Zarządzanie aktywami
- Kontrola dostępu
- Kryptografia
- Bezpieczeństwo fizyczne i środowiskowe
- Bezpieczna eksploatacja
- Bezpieczeństwo komunikacji
- Pozyskiwanie i rozwój systemów
- Relacje z dostawcami
- Zarządzanie incydentami związanymi z bezpieczeństwem informacji
- Aspekty bezpieczeństwa informacji w zarządzaniu ciągłością działania
- Zgodność

© ENSI 2017

Autor: Maciej Byczkowski

© ENSI 2017

Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.

# Wnioski końcowe

1. Wymagania dotyczące realizacji obowiązków zapewniania przestrzegania przepisów RODO, w tym zabezpieczania danych, **powinny być realizowane z wykorzystaniem norm ISO/IEC serii 29100** odnoszących się do ochrony danych identyfikujących osobę, w powiązaniu z normami ISO/IEC serii **27000**.

2. Normy stanowią w tym przypadku najlepszą podstawę, ponieważ **koncepcja ochrony danych osobowych przyjęta w RODO oparta jest o standardy i wytyczne określone w normach** dotyczących zarządzania bezpieczeństwem informacji, w tym szacowania ryzyka dla doboru odpowiednich zabezpieczeń oraz zapewnienia zgodności z przepisami.

© ENSI 2017

ENSI
KANCELARIA EKSPERTÓW

Stowarzyszenie Administratorów Bezpieczeństwa Informacji

# Dziękuję za uwagę!

**www.ensi.net**
m.byczkowski@sabi.org.pl
www.sabi.org.pl

© ENSI 2017



Prowadzenie jakiejkolwiek działalności gospodarczej lub jednorazowej czynności o charakterze komercyjnym z wykorzystaniem niniejszych materiałów przez uczestnika konferencji oraz osoby trzecie jest zabronione pod groźbą odpowiedzialności cywilnej i karnej. Wykorzystywanie tych materiałów, w szczególności do prowadzenia szkoleń, wykładów oraz innych celów wymaga zgody ENSI Sp. z o.o. z siedzibą w Warszawie przy Al. Jana Pawła II 34.