NASK

Privacy by design

jakie aspekty uwzględnić w fazie projektowania

Privacy by design

Podstawa prawna

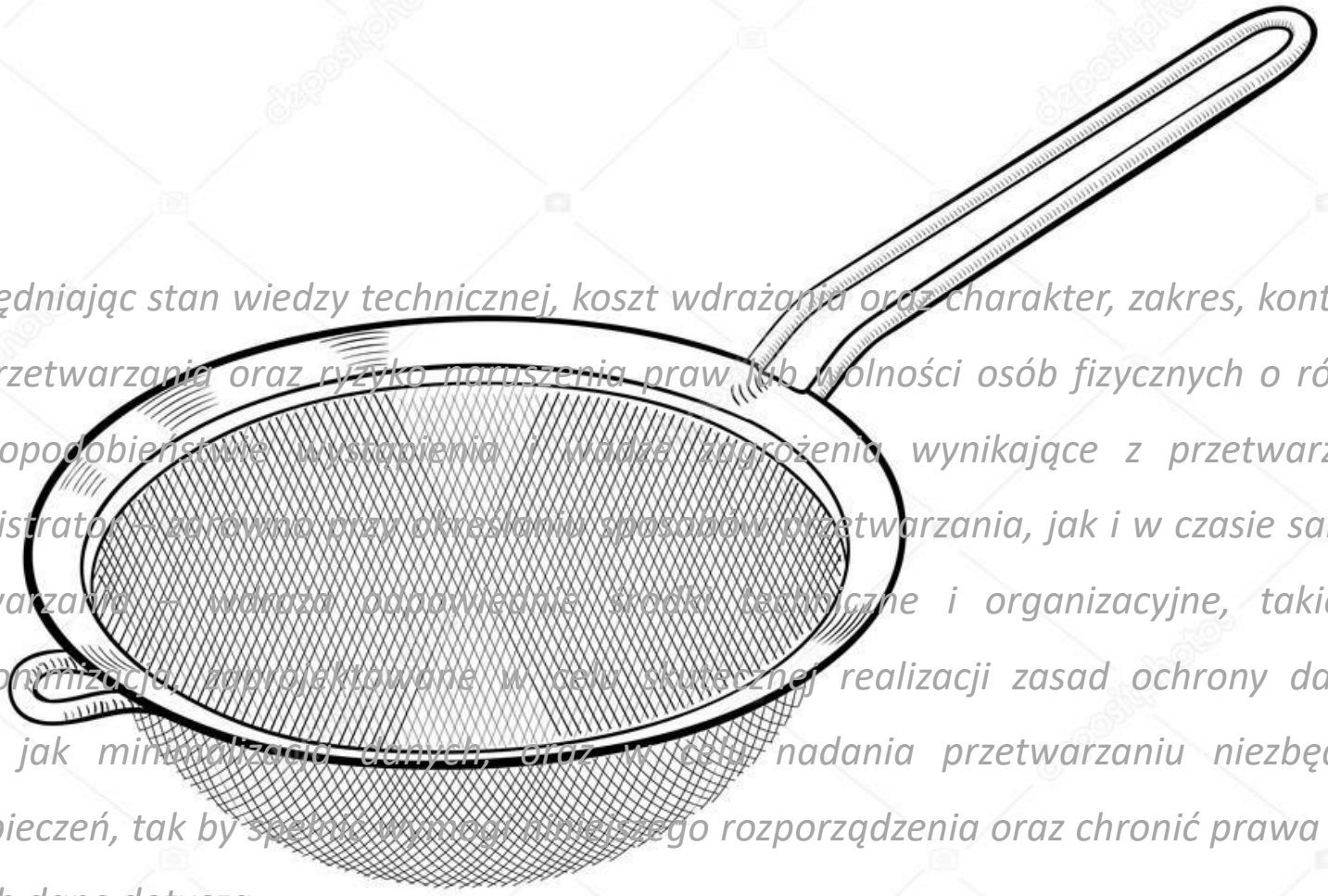
Artykuł 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Privacy by design

Podstawa prawna



Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą.

Privacy by design

Podstawa prawna

Artykuł 25

Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych

1. Uwzględniając **stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, **administrator** – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – **wdraża odpowiednie środki techniczne i organizacyjne,** takie jak pseudonimizacja, zaprojektowane **w celu skutecznej realizacji zasad ochrony danych**, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz **chronić prawa osób, których dane dotyczą**.

Privacy by design

Jak to rozumieć

Cel

- ✓ **skuteczna realizacji zasad ochrony danych;**
- ✓ **ochrona prawa osób, których dane dotyczą.**

Kto

- ✓ **Administrator**

Kiedy

przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania, wdraża odpowiednie środki techniczne i organizacyjne zaprojektowane w celu skutecznej realizacji zasad ochrony danych oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń.

Privacy by design

Jak to rozumieć

Co należy uwzględnić

- ✓ **cele przetwarzania;**
- ✓ **charakter, zakres, kontekst;**
- ✓ **ryzyko naruszenia praw lub wolności osób fizycznych;**
- ✓ **stan wiedzy technicznej;**
- ✓ **koszt wdrażania.**

Privacy by design

Jak to rozumieć

Ochrona danych ze względu na konstrukcję ma szczególne znaczenie dla całego cyklu życia danych osobowych od momentu ich zebrania poprzez przetwarzanie aż do ich usunięcia. Powinna koncentrować się na zapewnieniu dokładności, poufności, integralności, fizycznego bezpieczeństwa i usuwania danych osobowych.

Privacy by design

Jak to zrobić?

Powołać zespół projektowy

- ✓ Właściciel systemu;
- ✓ Osoby odpowiedzialne za zaprojektowanie systemu;
- ✓ Osoby odpowiedzialne za późniejsze utrzymanie systemu;
- ✓ Osoby odpowiedzialne za bezpieczeństwo;
- ✓ Inspektor Ochrony Danych Osobowych – rola konsultacyjna?;

Privacy by design

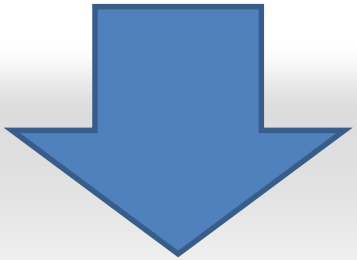
Jak to zrobić?

Określić kontekst przetwarzania danych

- ✓ cel przetwarzania;
- ✓ zakres przetwarzania;
- ✓ zdefiniować odbiorców przetwarzających dane osobowe (interesariuszy);

oraz określić:

- ✓ okres przechowywania danych osobowych;
- ✓ operacje przetwarzania.



Rejestr czynności przetwarzania

Privacy by design

Jak to zrobić?

Określić zainteresowane strony

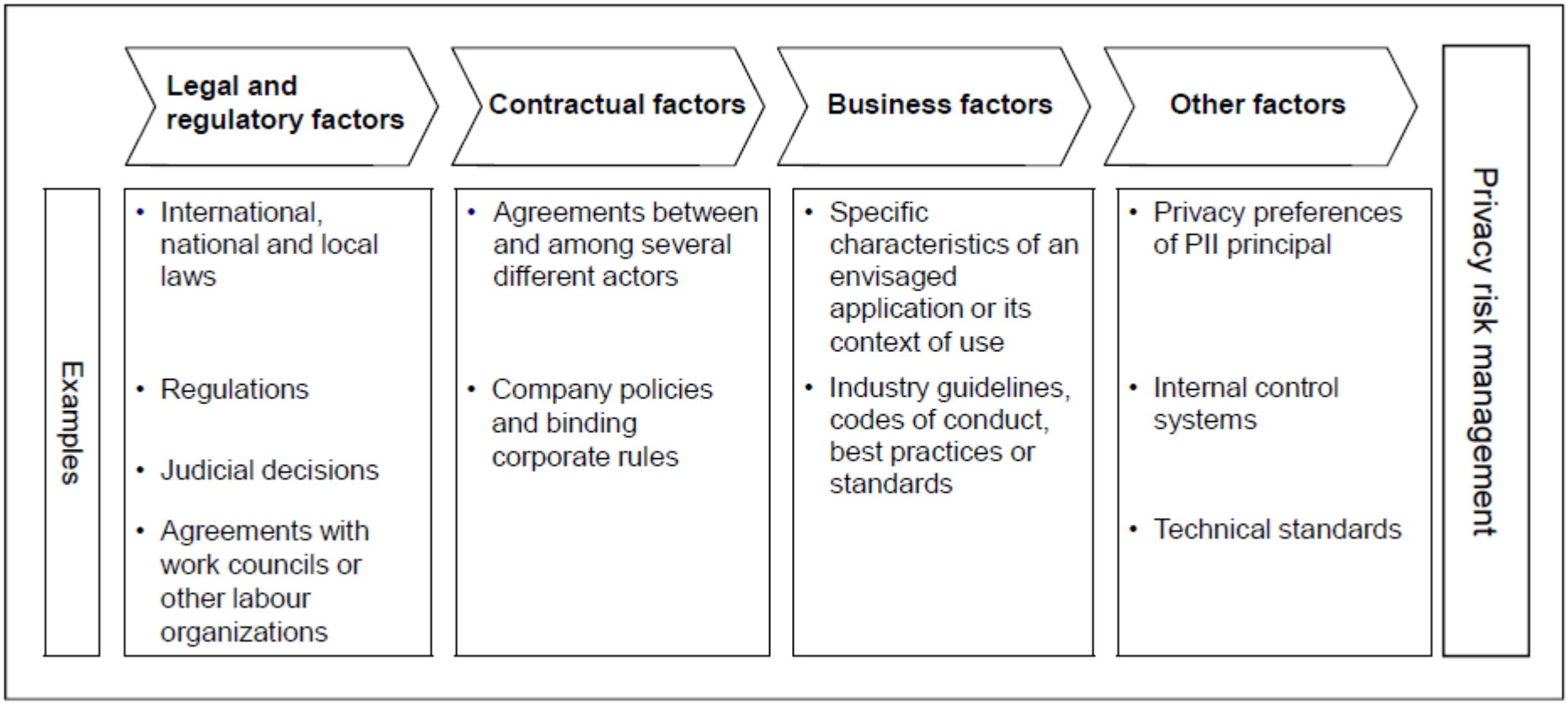
- ✓ użytkownicy;
- ✓ odbiorcy;
- ✓ role w systemie;

Przeprowadzić analizę ryzyka

zabezpieczenia dla ochrony danych osobowych (w tym kontrole bezpieczeństwa) powinny być wybierane na podstawie oceny ryzyka.

Privacy by design

Jak to zrobić?



Czynniki wpływające na zarządzanie ryzykiem związanym z prywatnością

PN-ISO/IEC 29100:2017

Privacy by design

A może?

Definiowanie ryzyk poprzez pryzmat scenariuszy ataku?

Privacy by design

Jak to zrobić?

Minimalizacja danych:
systemy przetwarzania danych należy zaprojektować i wybrać zgodnie z celem zbierania, przetwarzania lub wykorzystywania żadnych danych osobowych lub jak najmniejszej liczby danych osobowych.

Kontrola:
System informatyczny powinien zapewniać podmiotom danych skuteczne środki kontroli dotyczące ich danych osobowych. Możliwości dotyczące zgłoszenia i sprzeciwu powinny być poparte środkami technologicznymi.

Privacy by design

Jak to zrobić?

Przejrzystość:
zarówno deweloperzy, jak i operatorzy systemów informatycznych muszą zadbać o to, aby osoby, których dane dotyczą, były wystarczająco poinformowane o środkach działania systemów. Dostęp elektroniczny / informacja powinna być włączona.

Systemy przyjazne dla użytkownika:
funkcje i funkcje związane z prywatnością powinny być przyjazne dla użytkownika, tzn. Powinny zapewniać wystarczającą pomoc i proste interfejsy do wykorzystania także przez mniej doświadczonych użytkowników.

Poufność danych:
konieczne jest zaprojektowanie i zabezpieczenie systemów IT w taki sposób, aby tylko upoważnione podmioty miały dostęp do danych osobowych.

Privacy by design

Jak to zrobić?

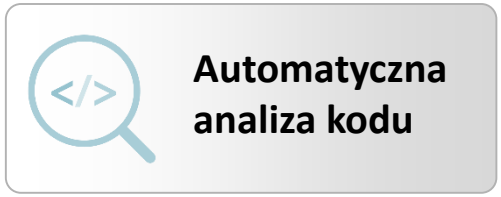
Zdefiniować zasady bezpiecznego projektowania

- ✓ Bezpieczne środowisko developerskiego;
- ✓ Bezpieczeństwo repozytoriów;
- ✓ Bezpieczeństwo kontroli wersji;
- ✓ Dokumentowanie kodu ale również zmian;
- ✓ Analiza kodu;

Privacy by design

Jak to zrobić?

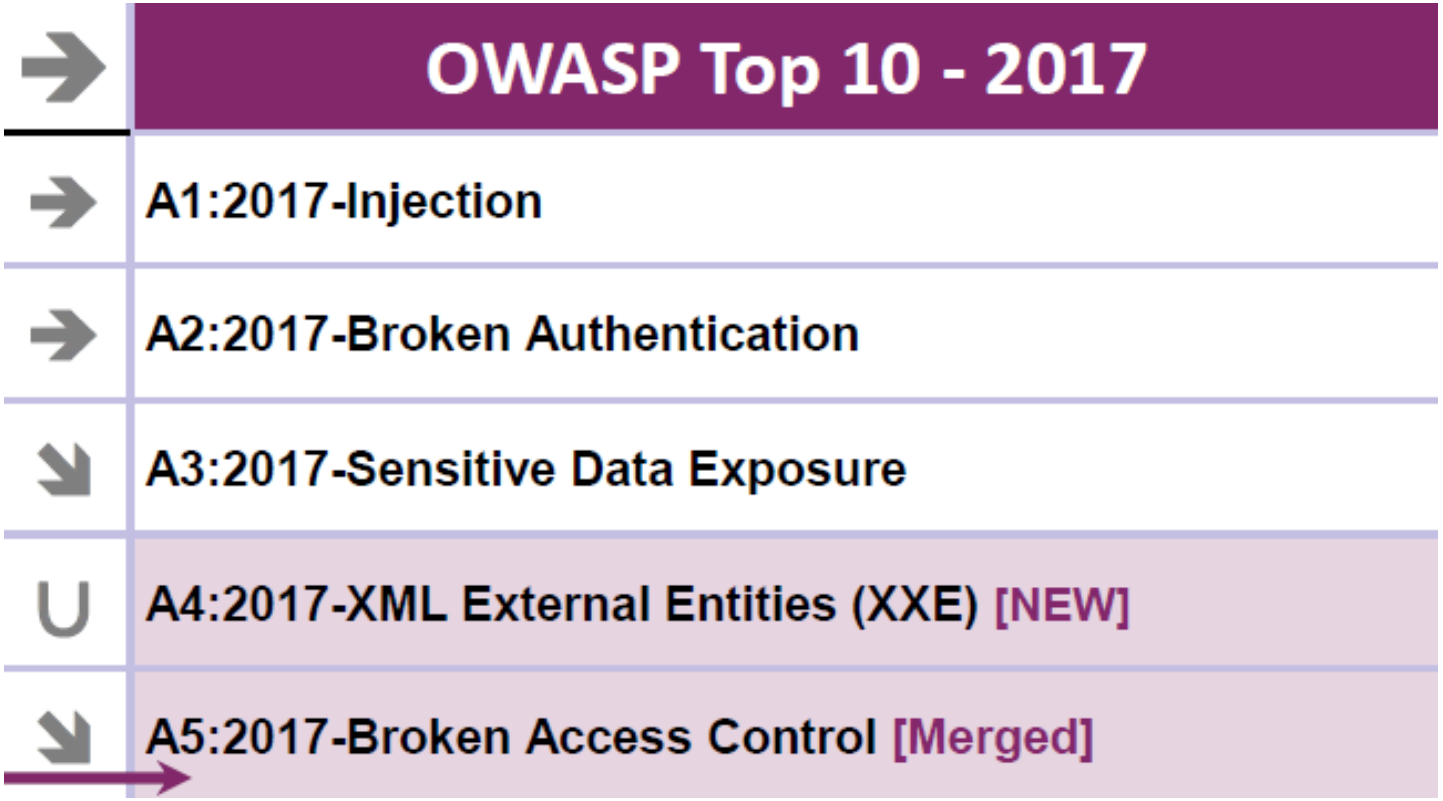
Analiza kodu w procesie wytwarzania



Privacy by design

Jak to zrobić?

Uwzględniać znane podatności



Privacy by design

Jak to zrobić?

Uwzględniać znane podatności

↗	A6:2017-Security Misconfiguration
U	A7:2017-Cross-Site Scripting (XSS)
☒	A8:2017-Insecure Deserialization [NEW, Community]
→	A9:2017-Using Components with Known Vulnerabilities
☒	A10:2017-Insufficient Logging&Monitoring [NEW,Comm.]

Privacy by design

Jak to zrobić?

Zdefiniować zabezpieczenia z wykorzystaniem norm

ISO/IEC 27001:2013

Technika informatyczna - Techniki bezpieczeństwa - Praktyczne zasady zabezpieczania informacji

ISO/IEC 29151:2017

Information technology — Security techniques — Code of practice for personally identifiable information protection

PN-ISO/IEC 29100:2017

Technika informatyczna - Techniki bezpieczeństwa - Ramy prywatności

ISO/IEC TS 27034

Information Technology - Security Techniques - Application Security

Privacy by design

Co uwzględnić w definiowaniu wymagań

- ✓ Projektuj zabezpieczenia uwzględniając CIA:
  - ✓ poufność,
  - ✓ integralności
  - ✓ dostępność;
- ✓ wymagania dotyczące niezaprzeczalności (logowanie);
- ✓ Wymagania biznesowe dotyczące kontroli dostępu
  - zarządzanie uprzywilejowanymi prawami dostępu
  - zarządzanie informacjami uwierzytelniającymi
  - zarządzanie prawami dostępu użytkowników

- ✓ wymagania dotyczące monitorowania i audytowania;
- ✓ połączenia z innymi systemami;
- ✓ wymagania dotyczące testów bezpieczeństwa;
- ✓ zastosuj zabezpieczenia na wszystkich warstwach
- ✓ zastosuj najlepsze praktyki bezpieczeństwa;
- ✓ przygotuj się na zdarzenia bezpieczeństwa;

NASK

Dziękuję za uwagę

Dariusz Stefański