Urząd
Ochrony
Danych
Osobowych

Stosowanie technicznych środków bezpieczeństwa w aspekcie zgłoszeń naruszeń do UODO oraz ocena wagi naruszenie w oparciu o zalecenia Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA).

Mariola Więckowska
Dyrektor ds. Innowacyjnych Technologii Ochrony Danych

UODO: Szkolenie dla Inspektorów Ochrony Danych
Warszawa, 14.01.2019

LexDigital

AGENDA

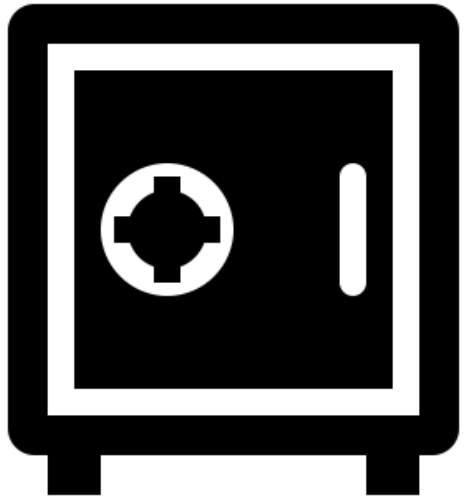
Techniczne środki zabezpieczeń danych: pseudonimizacja, szyfrowanie, anonimizacja

Naruszenie ochrony danych oraz proces jego obsługi w organizacji

Metoda oceny wagi naruszenia wg. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)

Przewidywania cyber-zagrożeń na 2019

- Atakujący wykorzystają system sztucznej inteligencji (AI) i użyją sztucznej inteligencji do wspomaganie ataków
- Obrońcy będą coraz bardziej polegać na sztucznej inteligencji, aby przeciwdziałać atakom i identyfikować podatności
- Rozwijające się wdrożenie i adaptacja 5G zacznie rozszerzać obszar powierzchni ataku
- Wydarzenia oparte na IoT przenoszą się poza masowe ataki DDoS na nowe, bardziej niebezpieczne formy ataku
- Atakujący będą coraz częściej przechwytywać dane w tranzycie
- Ataki wykorzystujące łańcuch dostaw będą rosły pod względem częstotliwości i skutków



Cyberbezpieczeństwo: statystyki

291 rekordów danych co sekundę ulega na świecie wyciekowi[1]

191 dni – tyle średnio organizacje potrzebują na wykrycie naruszenia danych

92% szkodliwego oprogramowania jest dostarczane pocztą e-mail

77% zaatakowanych ataków w 2017 roku było bez użycia plików

61% organizacji doświadczyło incydentu związanego z bezpieczeństwem IoT

56% organizacji najbardziej obawia się ukierunkowanego phishingu

CSO by DG Communications, Inc

[1]Breach Level Index by Gemalto

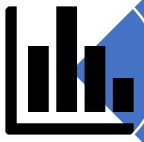
Art. 32 Bezpieczeństwo przetwarzania

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, administrator i podmiot przetwarzający wdrażają **odpowiednie środki techniczne i organizacyjne**, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

pseudonimizacja i szyfrowanie danych osobowych;

zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;

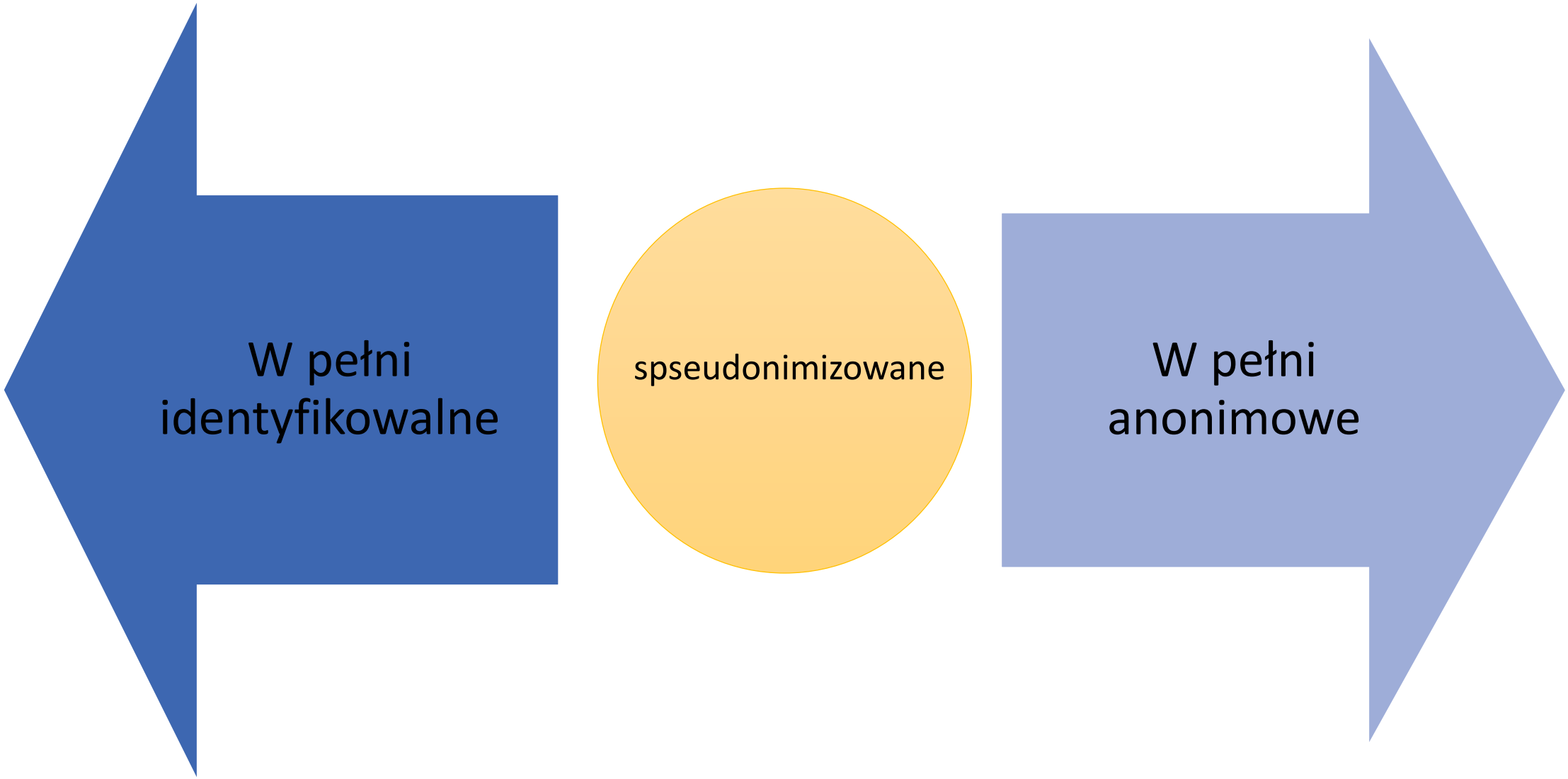
zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;



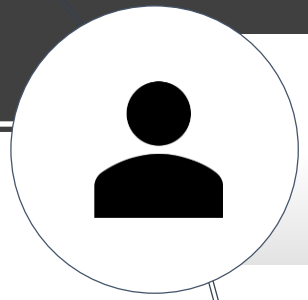
regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Techniki anonimizacji oraz pseudonimizacji

Odcienie (nie) identyfikowalności



Dane

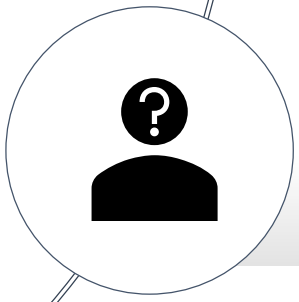


Osobowe

- informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej

Pseudonimowe

- dane nie mogą być już powiązane z osobą
- dodatkowa informacja pozwalająca na identyfikację jest trzymana oddzielnie



Anonimowe

- informacje nieodwracalnie zmienione w taki sposób, aby nie było możliwe zidentyfikowanie osoby

Pseudonimizacja – środek ochrony danych

- Polega na zastąpieniu jednego atrybutu inną wartością. W związku z tym nadal istnieje prawdopodobieństwo pośredniego zidentyfikowania osoby fizycznej.

- **Pseudonimizacja** jest skutecznym środkiem bezpieczeństwa, ale nie metodą anonimizacji, gdyż ogranicza możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą.

RODO zachęca do pseudonimizacji danych

- Umożliwia przetwarzanie danych w celu innym niż cel, którym dane zostały zebrane, pod warunkiem istnienia odpowiednich zabezpieczeń, w tym ew. szyfrowania lub pseudonimizacji (Art. 6 (4)(e))
- Pseudonimizacja jest istotnym zabezpieczeniem do przetwarzania DO dla celów naukowych, historycznych lub statystycznych (Art. 89 (1))
- Pseudonimizacja jako techniczny środek ochrony danych w fazie projektowania oraz domyślnej ochrony danych (Art. 25 (1))

RODO zachęca do pseudonimizacji danych c.d.

Administrator może użyć pseudonimizacji, by spełnić wymogi RODO dla zwiększenia bezpieczeństwa przetwarzania (Art. 32 (1)(a)).

Uniknięcie, w przypadku naruszenia ochrony danych osobowych, powiadomienia:

- Organu nadzorczego (Art. 33(1)).
- Podmiotu danych (Art. 34(1)).

RODO zachęca do przygotowania kodeksów postępowania promujących pseudonimizację (Art. 40)

Najczęstsze techniki pseudonimizacji

Szyfrowanie z kluczem tajnym – dobry klucz daje dużą gwarancję bezpieczeństwa, jednak administrator może je odszyfrować.

Funkcja skrótu – dla każdej wartości daje stałej wielkości wynik, którego nie można odwrócić (często stosowana do przechowywania haseł). Podatna na złamanie atakiem siłowym przy znajomości wkładu.

Funkcja skrótu z dodaniem losowego ciągu znaków (ang. „salt”) ogranicza prawdopodobieństwo uzyskania wartości wkładu.

Funkcja skrótu z dodanym kluczem, który jest przechowywany – łatwiejsze odzyskanie wkładu dla administratora, jednak trudne dla atakującego.

Szyfrowanie deterministyczne lub funkcja skrótu z kluczem, bez przechowywania klucza – pozwala ograniczyć ryzyko tworzenia powiązań między zbiorami przy zastosowaniu innych kluczy.

Tokenizacja, często stosowana w sektorze finansowym, polega na przypisaniu wartości, które nie zostały w sposób matematyczny uzyskane z danych pierwotnych, np. dla nr kart.

W latach 1979 do 2002 standardem był szyfr **DES** (Data Encryption Standard)

Blok wiadomości 64 bity	Klucz 56 bitów	Działa w 16 rundach

Do dziś używa się potrójnego szyfrowania DES tzw. **Triple DES**

Blok wiadomości 64 bity	Klucz 3 × 56 = 168 bitów

Od roku 2001 obowiązuje standard szyfrowania **AES** (Advanced Encryption Standard)

Długość bloku: 128	Klucz do wyboru: 128, 192, 256	Rundy: 10, 12, 14

Do dziś nie opublikowano ataku na szyfr AES.

Standardy szyfrowania

Szyfry symetryczne – używają tego samego tajnego klucza do szyfrowania i do odszyfrowania: dawniej DES (*ang. Data Encryption Standard*), a obecnie AES (*ang. Advanced Encryption Standard*):

- Jednostronne uwierzytelnianie z wykorzystaniem znacznika czasu lub liczników, lub liczb losowych
- Obustronne uwierzytelnianie

Szyfry asymetryczne – używają pary kluczy, nadawca szyfruje wiadomość kluczem publicznym odbiorcy, odbiorca deszyfruje szyfrogram swoim kluczem prywatnym. RSA, ElGamala

- Odszyfrowanie zaszyfrowanej wiadomości kluczem publicznym
- Złożenie podpisu elektronicznego oraz certyfikaty do uwierzytelniania

Uwaga: Para kluczy do uwierzytelniania nie może służyć dodatkowo do szyfrowania czy podpisywania dokumentów.

Szyfry: Uwierzytelnianie wiadomości

Szyfrowanie: bezpieczne przechowywanie i transmisja danych

Szyfrowanie dysków, katalogów, plików i nośników z danymi – system operacyjny, firmowe dyski zewnętrzne i pendrives, dodatkowe oprogramowanie szyfrujące np. TrueCrypt

1

Transmisja danych musi odbywać się za pomocą szyfrowanej transmisji (SSL, TLS, VPN)

2

Wszelkie pliki zawierające dane osobowe przesyłamy zawsze w sposób zaszyfrowany

3

Integralność i uwierzytelnianie:

- Informacje powinny trafiać tylko do uprawnionych odbiorców
- Szyfrowanie poufnych wiadomości za pomocą systemu PGP czy GnuPG (ang. GNU Privacy Guard)

Funkcje haszujące: Standardy

MD-5 - Funkcja MD5 (Message Digest 5) opracowana w 1991, daje 128 bitowe skróty. Następca funkcji MD4, MD2 autorstwa Rona Rivesta. Do dziś używana jako szybka funkcja do testowania integralności danych. Na jej konstrukcji opiera się SHA-1.

SHA-1 - wytwarza skrót 160 bitowy na podstawie 512 bitowego bloku danych

SHA-2 – w latach 2001-2005 rozszerzono standard SHA-1, by dawał dłuższe skróty i nazwano standard SHA-2: najczęściej stosowane SHA-256 dające skrót o długości 256 bitów, stosowano również rozszerzenia o SHA-224, SHA-384 i SHA-512

SHA-3 – Zupełnie inna funkcja haszująca oparta na algorytmie Keccak wykorzystującym strukturę gąbki, czyli sponge function, do osiągnięcia wymaganego poziomu bezpieczeństwa

Whirlpool - opiera się o konstrukcję szyfru Square oraz zmodyfikowaną wersję szyfru AES. Nie znaleziono do dzisiaj ataku na Whirlpool. Stosowana w TrueCrypt

Funkcje haszujące: Integralność danych

Testowanie integralności danych *(ang. Message Digestion Code, MDC)*

- Detekcja modyfikacji tekstu podczas przesyłania danych pocztą elektroniczną
- Testowanie integralności przechowywanych danych (razem z plikiem przechowywany jest skrót).

Podpis elektroniczny

- Złożenie podpisu pod konkretnym dokumentem – podpisanie skrótu dokumentu i przesłanie do razem z tekstem jawnym

Znakowanie czasem – posiadając skrót daty nie można zmienić wartości daty bez zmiany jego skrótu

Zobowiązania bitowe

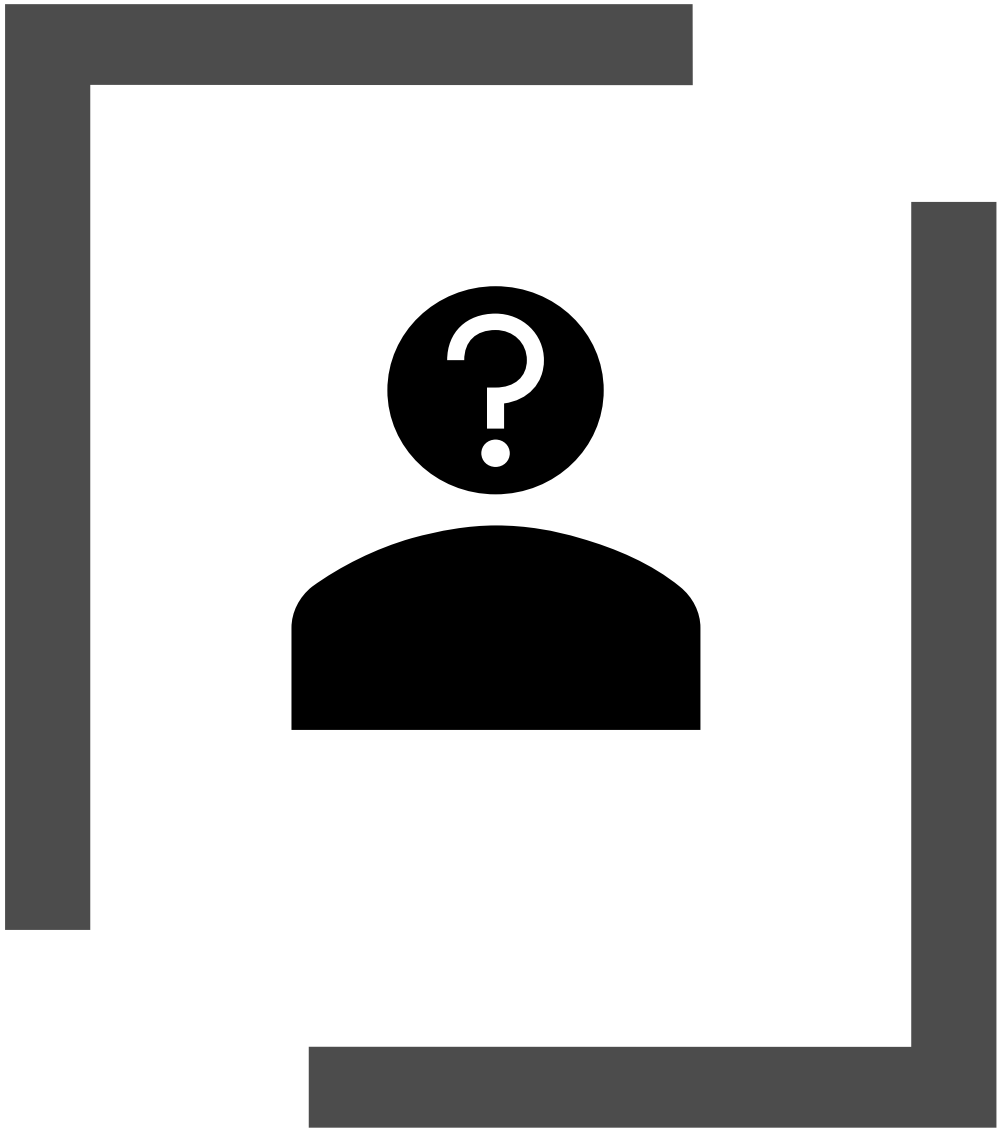
Przechowywanie haseł w systemach

Zagrożenia użycia pseudonimizacji

- **Sieci społecznościowe** – wykazano, że informacje chronione można wydobyć z grafów powiązań społecznościowych mimo pseudonimizacji. Powiązania między osobami fizycznymi są niepowtarzalne i mogą zostać wykorzystane jako identyfikatory.
- **Lokalizacje** – dane dotyczące czasowej mobilności przestrzennej w powiązaniu z innymi punktami danych mogą pozwolić na identyfikację:
  - 4 punkty – pozwalają wyodrębnić 95% populacji
  - 2 punkty – 50% populacji (przy czym najprawdopodobniej 1 punkt to dom lub biuro)
- **Opieka zdrowotna** – dla znanych funkcji skrótu i danych osobowych potencjalnych osób łatwo uzyskać informację, których z nich te dane dotyczą
- Znając kod pocztowy, płeć i datę urodzenia można zidentyfikować **87% Amerykanów**

Definicja anonimizacji

- „Zasady ochrony danych **nie powinny więc mieć zastosowania do informacji anonimowych**, czyli informacji, które nie wiążą się ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną, ani do danych osobowych zanonimizowanych w taki sposób, że osób, których dane dotyczą, w ogóle nie można zidentyfikować lub już nie można zidentyfikować. Niniejsze rozporządzenie nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych.”(motyw 26 RODO)
- „**anonimizacja jest procesem**, w którym informacje umożliwiające identyfikację osoby są **nieodwracalnie** zmienione w taki sposób, aby nie istniała już możliwość bezpośredniego lub pośredniego zidentyfikowania podmiotu informacji umożliwiających identyfikację osoby przez administratora informacji umożliwiających identyfikację osoby działającego samodzielnie lub we współpracy z jakąkolwiek inną stroną” (ISO 29100:2011).



Po co jest potrzebna anonimizacja?

- Możliwość wtórnego wykorzystania danych w sytuacjach, w których przepisy o ochronie danych osobowych na to nie pozwalają (otwarte dane, Big Data etc.)
- Zatrzymanie lub przetwarzanie danych przez administratora po osiągnięciu celów pierwotnych.

Proces anonimizacji musi być**:**

- **trwały**
- **nieodwracalny**

Techniki anonimizacji opisane w opinii GR art.29

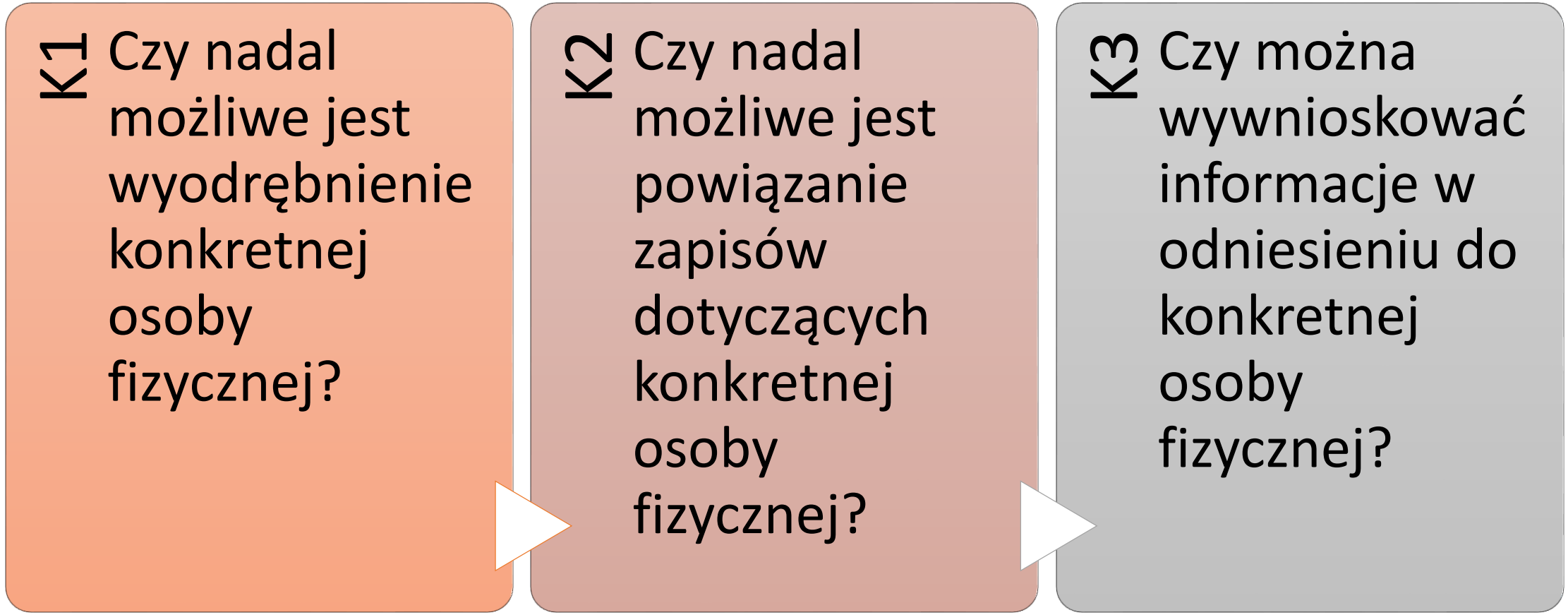
Randomizacja - usuwanie informacji identyfikacyjnych

- Dodanie zakłóceń – modyfikacja atrybutów w zbiorze danych
- Permutacja – zmiana wartości w zbiorze danych poprzez podstawienie wartości z jednego zapisu do innego zapisu
- Prywatność różnicowa – generowanie zanonimizowanego widoku online

Uogólnianie - zapewnienie niejednoznaczności danych

- Agregacja i K-anonimizacja - zestaw danych jest k-anonimowy, gdy każdy rekord w obrębie tych danych jest nierozróżnialny od co najmniej k-1 innych rekordów
- L-dywersyfikacja/T-bliskość - każdy atrybut ma co najmniej L różnych wartości

Kryteria oceny skuteczności anonimizacji danych



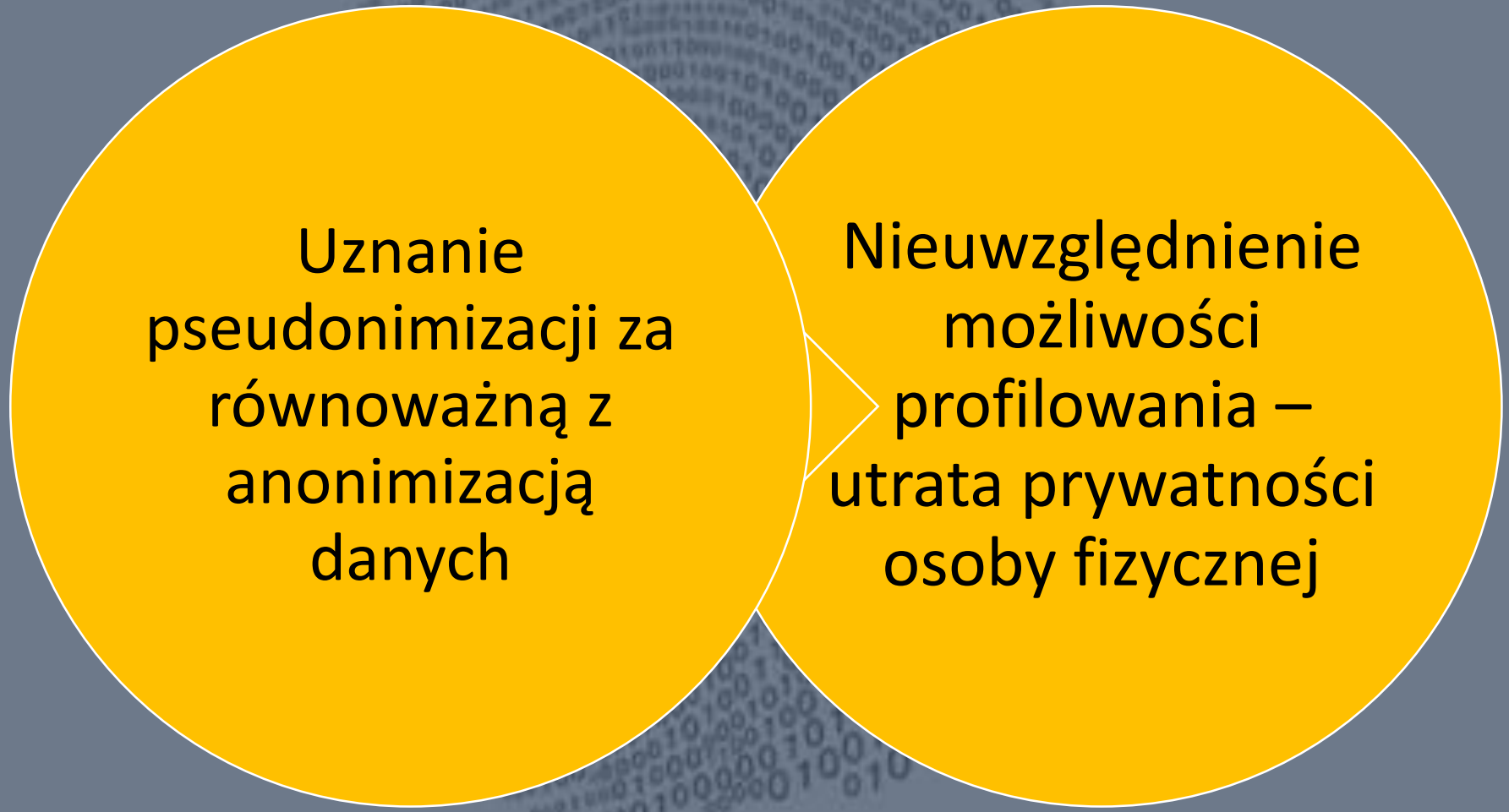
Jaką technikę wybrać?

	Czy nadal istnieje ryzyko wyodrębnienia?	Czy nadal istnieje ryzyko możliwości tworzenia powiązań?	Czy nadal istnieje ryzyko wnioskowania?
Pseudonimizacja	Tak	Tak	Tak
Dodawanie zakłóceń	Tak	Być może nie	Być może nie
Zastąpienie	Tak	Tak	Być może nie
Agregacja lub k-anonimizacja	Nie	Tak	Tak
L-dywersyfikacja	Nie	Tak	Być może nie
Prywatność różnicowa	Być może nie	Być może nie	Być może nie
Skracanie/Tokenizacja	Tak	Tak	Być może nie

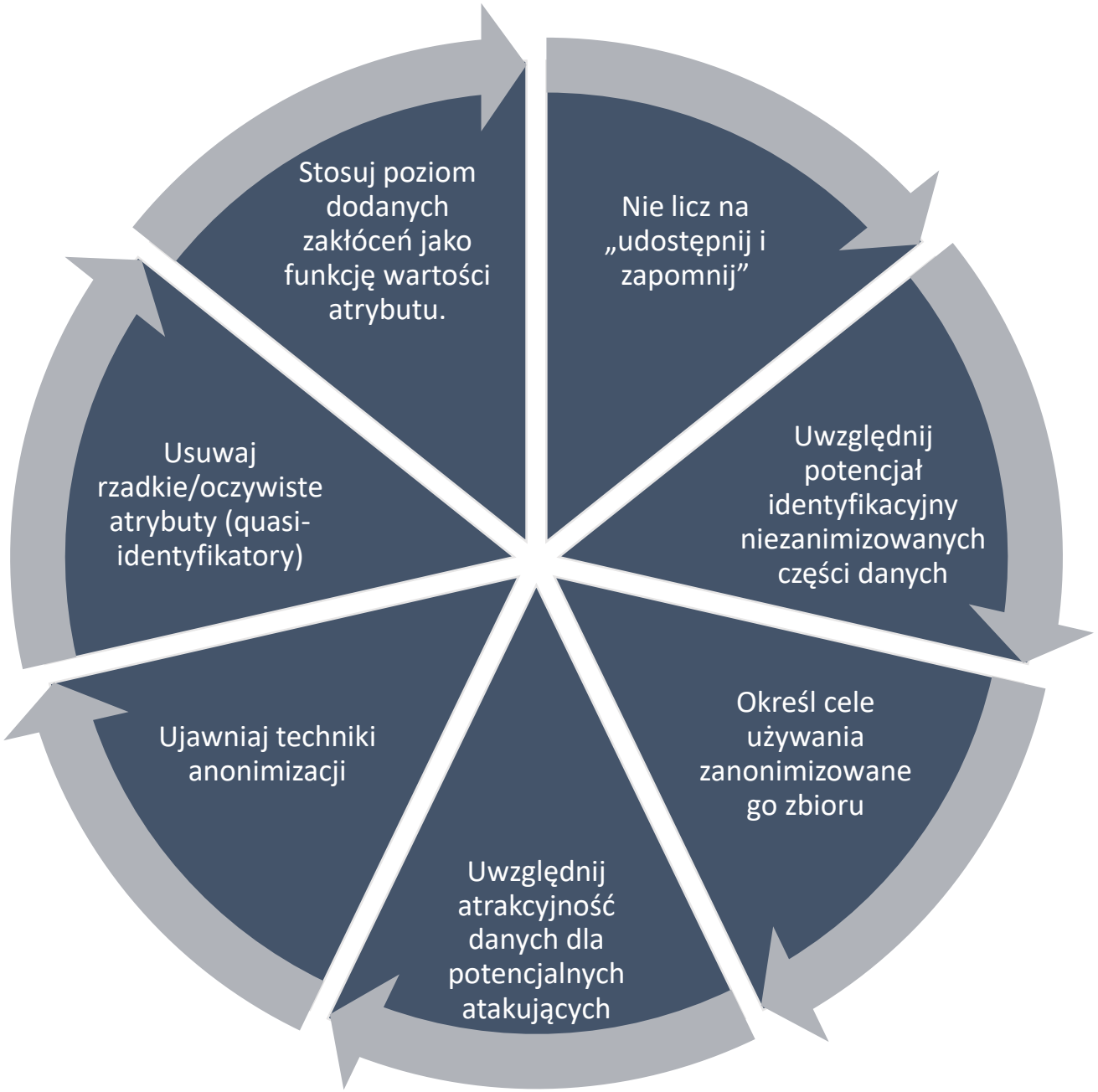
Przykład wykorzystania technik anonimizacji i pseudonimizacji - zwanych zaciemnieniem danych

Pole	Typ zmiany	Technika
ID_Pracownika	Hashowanie	SHA-2 z solą
DataUrodzin	Wstawić losowa data z przedziału (1-2000)	Randomizacja
NazwikoPanieńkieMatki	Usunąć	Usunięcie rzadkich atrybutów
Pesel/Nip	Zastąpić numerem rozliczeniowym pracownika	Zastąpienie
EmailAddress	Zamienić na mail@sabi.pl dla wszystkich	Uogólnienie
Telefon	Zamienić na losowy numer	Randomizacja
Ulica	Zamienić na jeden adres dla wszystkich pracowników	Uogólnienie
NumerBudynkuMieszkania	Zamienić na numer z zakresu 1-1000	Uogólnienie
KodPocztowy	Zamienić na kod miasta wojewódzkiego	Uogólnienie
Miasto	Zamienić na miasto wojewódzkie	Uogólnienie

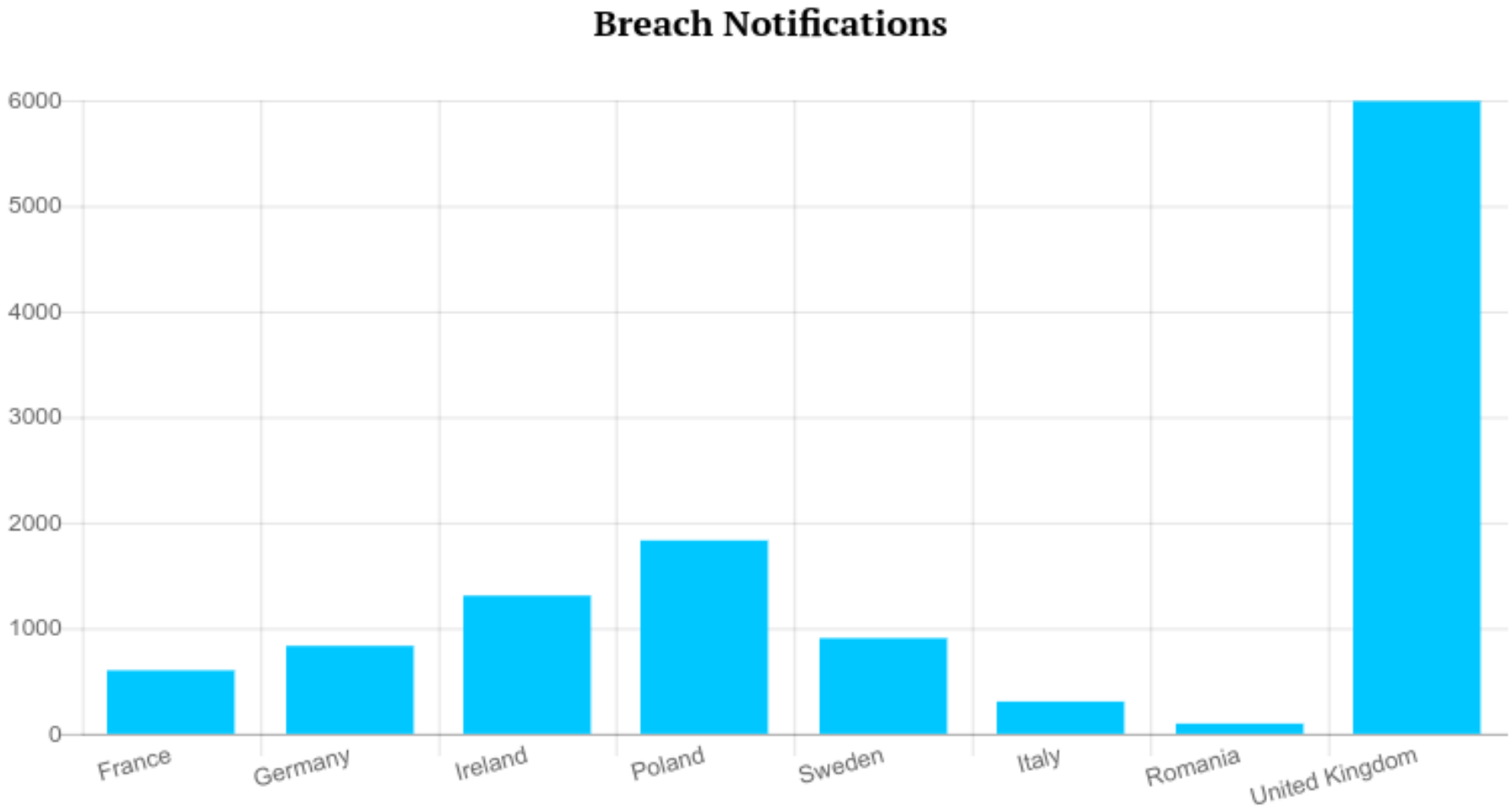
Ryzyka anonimizacji danych



Kilka dobrych praktyk



Statystyki naruszeń



Liczba zgłoszonych naruszeń po wejściu RODO w różnych krajach (źródło: GDPR Today)

Definicja naruszenia

RODO

- „**naruszenie ochrony danych osobowych**” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;

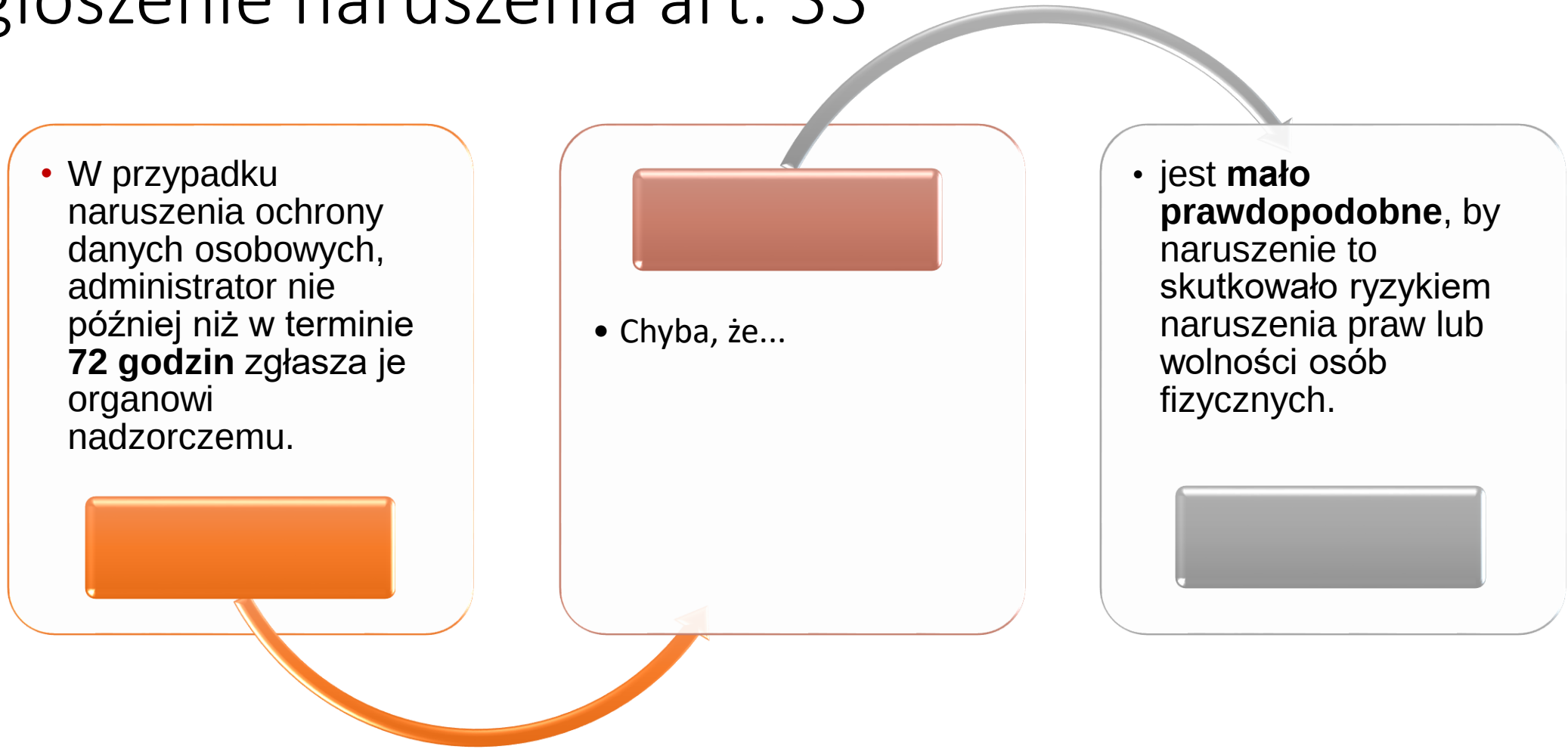
ISO

- **incydent związany z bezpieczeństwem informacji** - pojedyncze niepożądane lub niespodziewane zdarzenie związane z bezpieczeństwem informacji lub seria takich zdarzeń, które stwarzają znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrażają bezpieczeństwu informacji;

Zarządzanie incydentami związanymi z bezpieczeństwem informacji

- procesy wykrywania, raportowania, szacowania, reagowania, podejmowania akcji i wyciągania wniosków z incydentów związanych z bezpieczeństwem informacji;

Zgłoszenie naruszenia art. 33



…powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

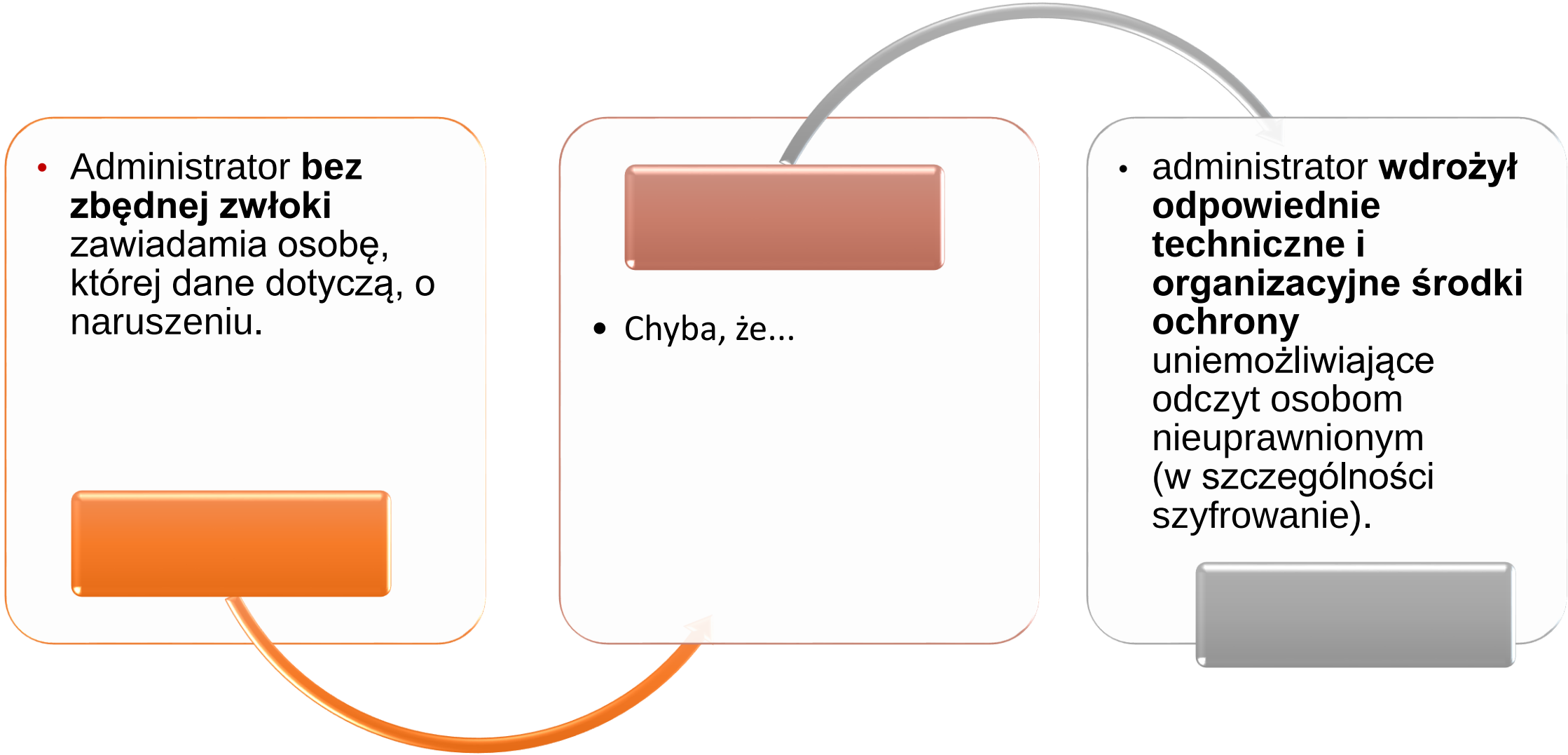
Co zgłoszenie powinno zawierać?

W szczególności

- charakter naruszenia, w tym w miarę możliwości wskazywać
- kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz
- kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
- imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub innego punktu kontaktu;
- możliwe konsekwencje naruszenia;
- środki zaradcze zastosowane lub proponowane do naruszeniu ochrony danych osobowych, w tym minimalizujące jego ewentualne negatywne skutki.

Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia, jego skutki oraz podjęte działania zaradcze.

Naruszenie – zawiadomienie podmiotu art. 34



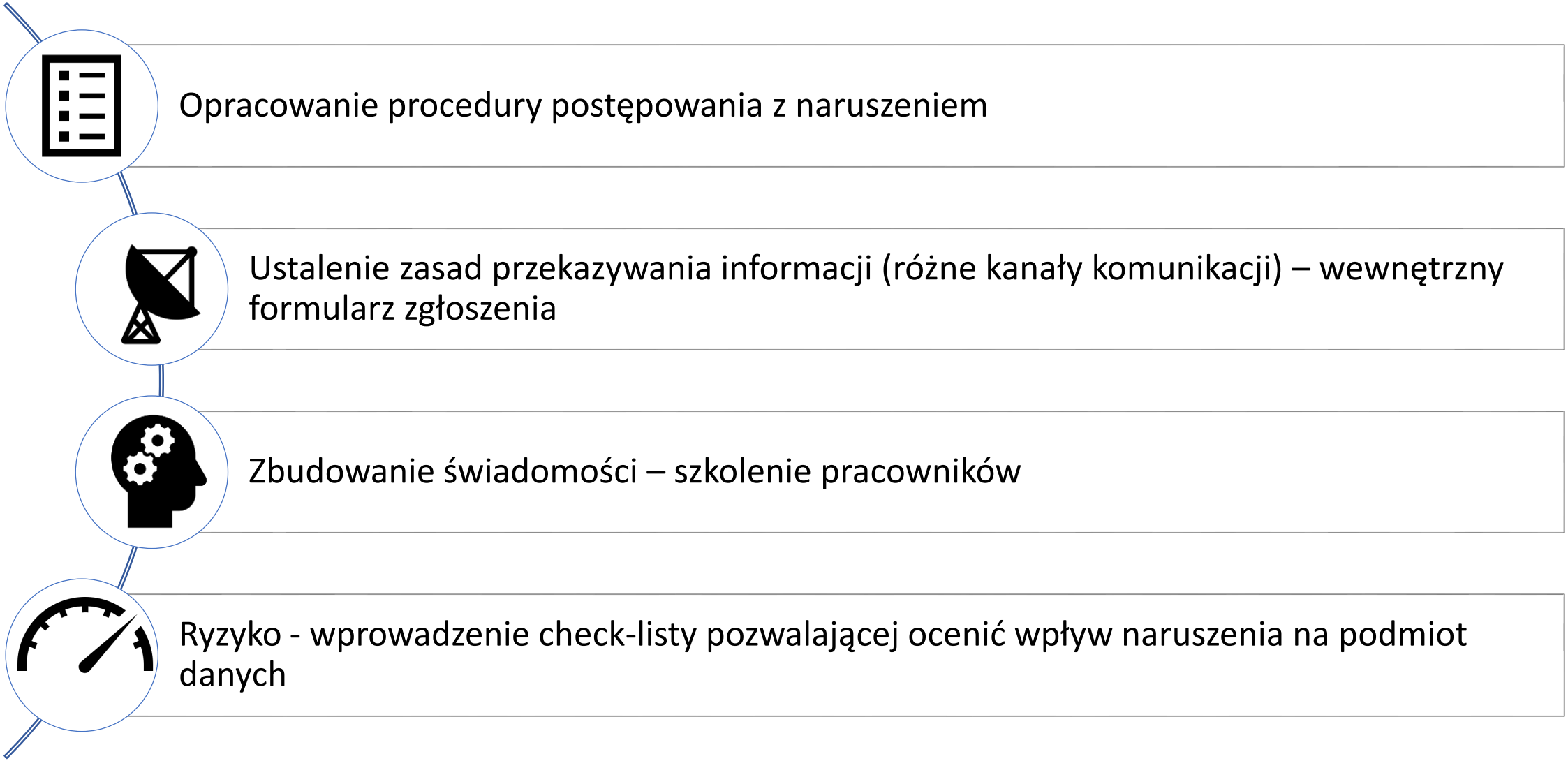
Kiedy zawiadomienie osoby nie jest wymagane

administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak **szyfrowanie**, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;

administrator zastosował następnie **środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby**, której dane dotyczą, o którym mowa w ust. 1;

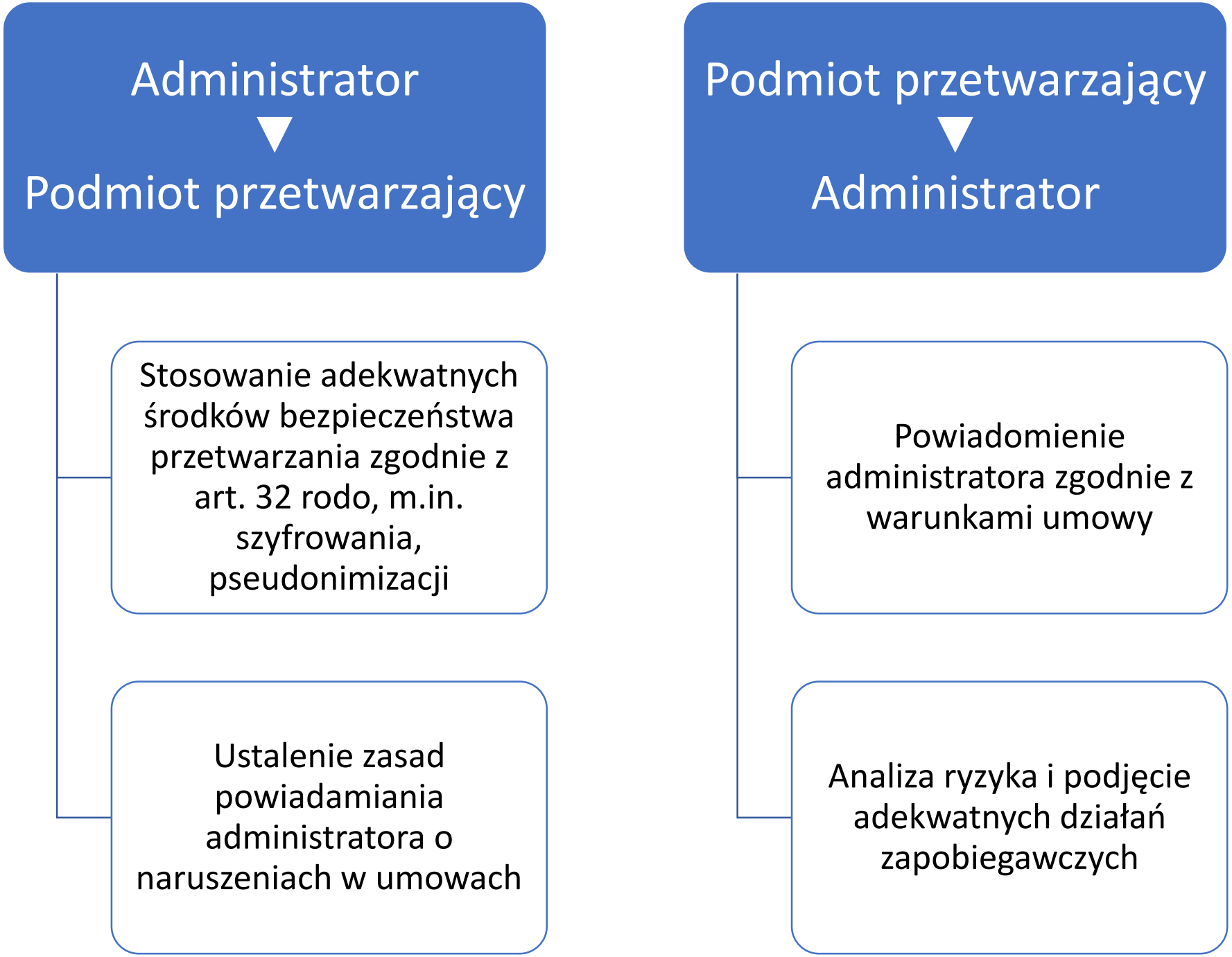
wymagałoby ono **niewspółmiernie dużego wysiłku**. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Obsługa naruszeń – jak ją wdrożyć?



Procedura postępowania z naruszeniami

Identyfikacja	• Incydent wykryty • Przekazanie informacji do właściwego zespołu • Rejestracja incydentu w wewnętrznym rejestrze
Potwierdzenie	• Ustalenie czy incydent dotyczy danych osobowych • Aktywacja zespołu odpowiedzialnego za obsługę incydentu
Działania	• Włączenie osób, które powinny uczestniczyć w analizie naruszenia • Ustalenie ryzyka prawdopodobieństwa naruszenia praw lub wolności osób
Notyfikacja	• Podjęcie decyzji o notyfikacji do UODO • Wysokie ryzyko: poinformowanie osób
Prewencja	• Wdrożenie środków ochronnych zapobiegających podobnym incydentom w przyszłości


Administrator
▼
Podmiot przetwarzający
Stosowanie adekwatnych środków bezpieczeństwa przetwarzania zgodnie z art. 32 rodo, m.in. szyfrowania, pseudonimizacji
Ustalenie zasad powiadamiania administratora o naruszeniach w umowach
Podmiot przetwarzający
▼
Administrator
Powiadomienie administratora zgodnie z warunkami umowy
Analiza ryzyka i podjęcie adekwatnych działań zapobiegawczych

Zgłoszenie naruszenia

Incydent

- Wyłącznie: „chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować **ryzyko naruszenia praw lub wolności osób fizycznych**”

Zgłoszenie

- Do: Właściwy organ nadzorczy
- Termin: bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie **72 godzin** po stwierdzeniu naruszenia

Dokumentacja

- Zakres:
  - Okoliczności
  - Skutki
  - Podjęte działania

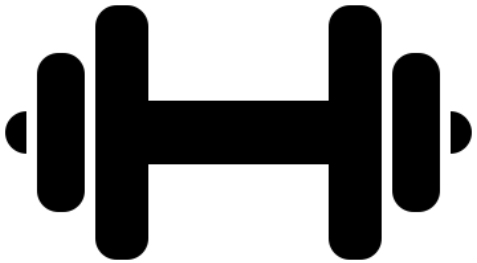
GR29: Czynniki ryzyka

- Rodzaj naruszenia (poufność, integralność, dostępność)
- Charakter, wrażliwość i ilość danych osobowych
- Łatwość identyfikacji osób fizycznych
- Waga konsekwencji dla osób fizycznych
- Cechy szczególne danej osoby fizycznej
- Cechy szczególne administratora
- Liczba osób fizycznych, na które naruszenie wywiera wpływ

Metoda oceny wagi naruszenia wg. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)[1]

WN = KPD * PI + ON

- **Waga Naruszenia - WN**
- **Kontekst Przetwarzania Danych - KPD** – główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania
- **Prawdopodobieństwo Identyfikacji - PI** – czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich.
- **Okoliczności Naruszenia - ON** – czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.



[1] https://www.enisa.europa.eu/publications/dbn-severity/

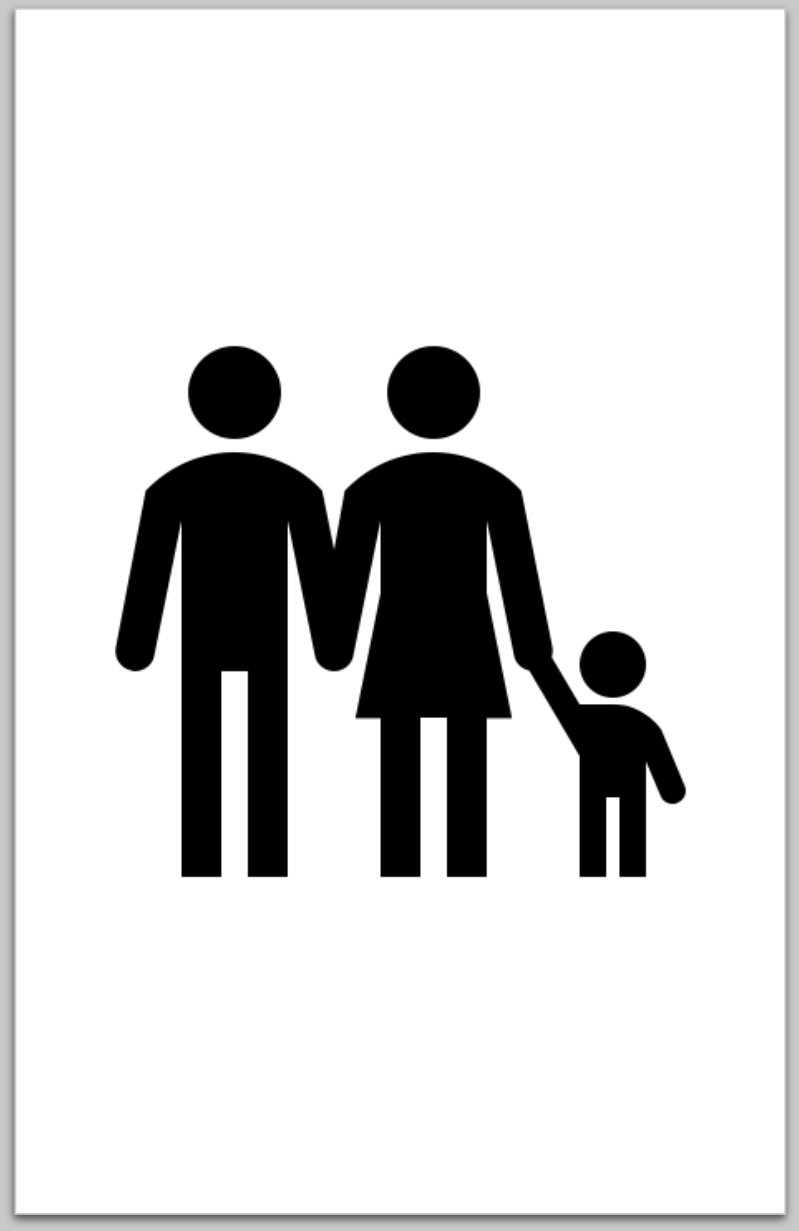
Kontekst Przetwarzania Danych

KPD = A + B

A – rodzaj i poziom wrażliwości danych	Dane podstawowe = 1
	Dane dotyczące zachowań osoby = 2
	Dane finansowe = 3
	Dane szczególne = 4
B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę	Szeroki zakres danych/wolumen danych (+)
	Charakter danych (+/-)
	Specyfika podmiotu danych lub administratora (+/-)
	Możliwe negatywne skutki dla podmiotu danych (+)
	Publiczna dostępność danych przed naruszeniem (-)
	Nieważność danych (-)

Prawdopodobieństwo identyfikacji - **PI**

Prawdo-podobieństwo identyfikacji	Znikome	= 0,25
	Ograniczone	= 0,5
	Wysokie	= 0,75
	Maksymalne	= 1

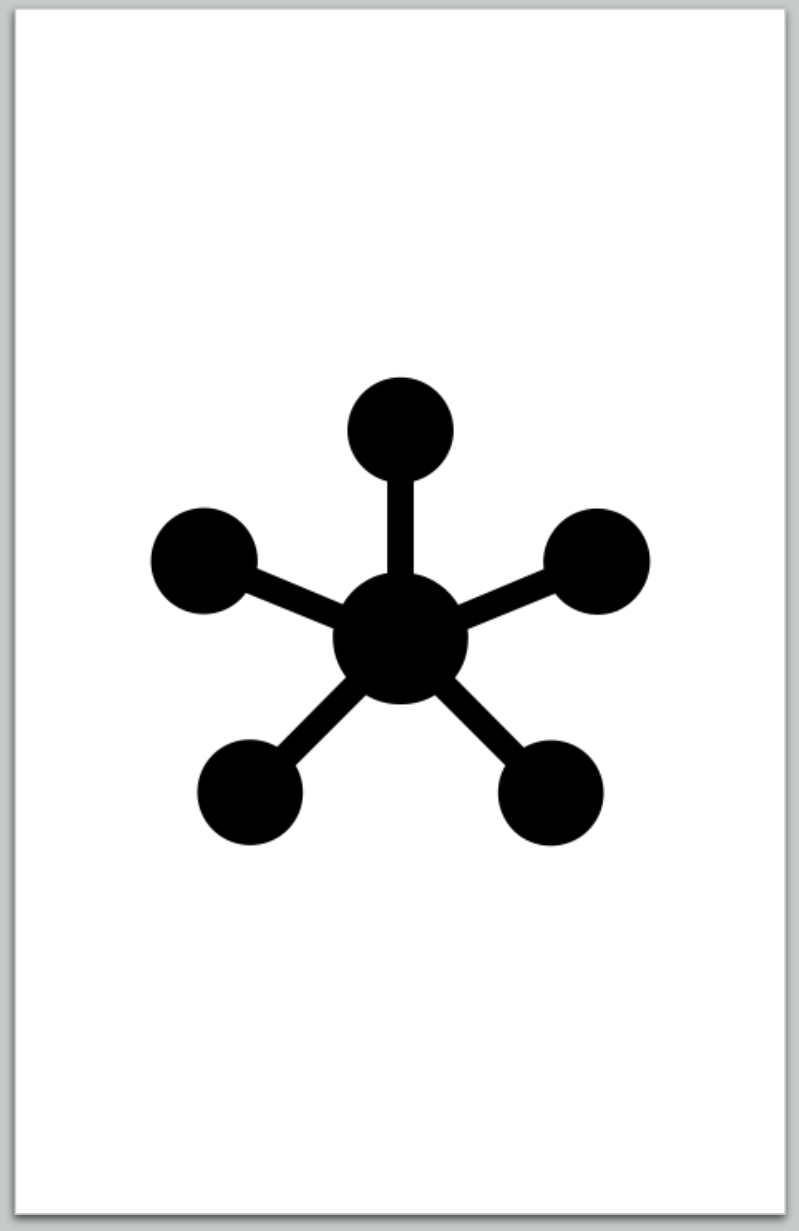


Okoliczności Naruszenia - **ON**

ON = NP + NI + ND + IDS

Naruszenie Poufności – Dane ujawnione	znanym odbiorcom danych (+0,25)
	nieznanej liczbie odbiorców danych (+0,5)
Naruszenie Integralności - Dane zmienione i	możliwe jest ich odzyskanie (+0,25)
	brak jest możliwości ich odzyskania (+0,5)
Naruszenie Dostępności - Niedostępność danych	czasowa (+0,25)
	pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)

Intencjonalne Działanie Sprawcy (+0,5)



Ocena wagi naruszenia

Wynik	Waga naruszenia	Opis
WN<2	Niska	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<=**WN**<3	Średnia	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=**WN**<4	Wysoka	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=**WN**	Bardzo wysoka	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

Przykłady oceny naruszenia

Zgubienie niezaszyfrowanego pendrive z listą 250 uczestników konferencji

Konferencja naukowa

Zakres danych: imię, nazwisko, e-mail, firma

- **KPD** = A + B = 1 + 0 = 1
  A = 1 (dane podstawowe)
  B = 0
- **PI** = 1
- **ON** = NP+NI+ND+IDS =
  = 0,5 (nieznana liczba odbiorców)+0
  +0,25(czasowa niedostępność)+0 = 0,75
- **WN** = KPD * PI + ON = 1 * 1 + 0,75 = 1,75

Niska waga naruszenia

Konferencja dla rodziców dzieci chorych na …..

Zakres danych: imię, nazwisko, e-mail

- **KPD** = A + B = 1 + 2 = 3
  A = 1 (dane podstawowe)
  B = 2 (Specyfika administratora i możliwe negatywne skutki dla podmiotu danych)
- **PI** = 1
- **ON** = NP+NI+ND+IDS =
  = 0,5 (nieznana liczba odbiorców)+0
  +0,25(czasowa niedostępność)+0 = 0,75
- **WN** = KPD * PI + ON = 3 * 1 + 0,75 = 3,75

Wysoka waga naruszenia

Przykłady oceny naruszenia

Wysłanie e-maila do 500 osób z widocznymi adresami mailowymi wszystkich odbiorców

Informacje wysłana przez restaurację do swoich Klientów.

Zakres danych: e-mail

- **KPD** = A+B = 1 + 0 = 1
  A = 1 (dane podstawowe)
  B = 0
- **PI** = 0,5
- **ON** = NP+NI+ND+IDS
  = 0,25(znana liczba odbiorców)+0+0+0 = 0,25
- **WN** = KPD*PI+ON = 1*0,5+0,25 = 0,75

Niska waga naruszenia

Informacja wysłana ze szpitala z prośbą o stawienie się na badania ze względu na wykrycie zakażenia niebezpiecznym wirusem podczas hospitalizacji w grudniu 2018.

Zakres danych: e-mail

- **KPD** = A+B = 1 + 3 = 4
  A = 1 (dane podstawowe)
  B = 3 (Specyfika administratora + charakter informacji)
- **PI** = 1 (osoby łatwo zidentyfikować w powiązaniu z informacją o czasie hospitalizacji i szpitalu)
- **ON** = NP+NI+ND+IDS
  = 0,25(znana liczba odbiorców)+0+0+0 = 0,25
- **WN** = KPD*PI+ON = 4*1+0,25=4,25

Bardzo wysoka waga naruszenia

Dziękuję za uwagę

Mariola Więckowska
Dyrektor ds.
Innowacyjnych Technologii Ochrony Danych
Mariola.Wieckowska@LexDigital.pl
Lex Digital