RODO - czy jest się czego obawiać?

Joanna Świebocka-Więk
Katedra Informatyki Stosowanej i Fizyki Komputerowej

SEMINARIUM WYDZIAŁOWE WFiIS AGH, 11.05.2018

Plan prezentacji

1. Kluczowe definicje
2. Dane osobowe i ich przetwarzanie
3. Projektowanie systemów przetwarzania danych
4. Zgoda na przetwarzanie danych
5. Prawa obywatela UE wynikające z RODO
6. Kontrola zewnętrzna
7. Zgłaszanie incydentów utraty danych
8. Odpowiedzialność w RODO
9. Podsumowanie

RODO

ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych

Rozporządzenie o Ochronie Danych Osobowych (RODO)

General Data Protection Regulaton (GDPR)

Co wiesz o RODO?

1. Datą graniczną wprowadzenia przepisów RODO jest:

a) 1 marca 2018 r.
b) 23 maja 2018 r.
c) 25 maja 2018 r.
d) 11 czerwca 2018 r.

1. Datą graniczną wprowadzenia przepisów RODO jest:

a) 1 marca 2018 r.
b) 23 maja 2018 r.
c) 25 maja 2018 r.
d) 11 czerwca 2018 r.

2. Po wejściu RODO bazę klientów

a) należy zgłosić do właściwego organu na dotychczasowych zasadach
b) należy zgłosić do właściwego organu z podaniem miejsca przechowywania danych
c) należy zgłosić przez specjalnie utworzony formularz na stronie Inspektora Danych Osobowych
d) nie trzeba zgłaszać

2. Po wejściu RODO bazę klientów

a) należy zgłosić do właściwego organu na dotychczasowych zasadach

b) należy zgłosić do właściwego organu z podaniem miejsca przechowywania danych

c) należy zgłosić przez specjalnie utworzony formularz na stronie Inspektora Danych Osobowych

d) nie trzeba zgłaszać

3. Kara w przypadku nieprzestrzegania wymogów RODO może wynieść

a) 4% rocznego obrotu lub 20 mln Euro
b) nie jest to określone
c) 200% wartości powstałej szkody
d) każdy kraj UE określa to wewnętrznie

3. Kara w przypadku nieprzestrzegania wymogów RODO może wynieść

a) 4% rocznego obrotu lub 20 mln Euro
b) nie jest to określone
c) 200% wartości powstałej szkody
d) każdy kraj UE określa to wewnętrznie

4. Baza Klientów...

a) musi być na komputerze bez dostępu do internetu
b) musi być przechowywana w siedzibie firmy
c) musi być zabezpieczona przed niepożądanym dostępem
d) nie może być prowadzona w programach typu Excel

4. Baza Klientów...

a) musi być na komputerze bez dostępu do internetu

b) musi być przechowywana w siedzibie firmy

c) musi być zabezpieczona przed niepożądanym dostępem

d) nie może być prowadzona w programach typu Excel

5. W przypadku wycieku danych...

a) należy wysłać maila do wszystkich osób z bazy z informacją o wycieku
b) należy utworzyć kopię zapasową bazy
c) nie ma określonych procedur działania
d) w ciągu 72 godzin należy złożyć autodonos do Inspektora Danych Osobowych

5. W przypadku wycieku danych...

a) należy wysłać maila do wszystkich osób z bazy z informacją o wycieku
b) należy utworzyć kopię zapasową bazy
c) nie ma określonych procedur działania
d) w ciągu 72 godzin należy złożyć autodonos do Inspektora Danych Osobowych

6. Jeśli wykonujesz wysyłkę maili do swoich klientów przy pomocy systemu mailingowego, to jesteś:

a) Administratorem danych osobowych
b) Procesorem danych osobowych
c) Weryfikatorem danych osobowych
d) Agentem Bezpieczeństwa Informacji

6. Jeśli wykonujesz wysyłkę maili do swoich klientów przy pomocy systemu mailingowego, to jesteś:

a) Administratorem danych osobowych
b) Procesorem danych osobowych
c) Weryfikatorem danych osobowych
d) Agentem Bezpieczeństwa Informacji

7. Czego **NIE MA** w RODO?

a) prawa do bycia zapomnianym
b) prawa do uzupełnienia danych
c) prawa do samodzielnej edycji swoich danych osobowych
d) prawa do modyfikacji

7. Czego **NIE MA** w RODO?

a) prawa do bycia zapomnianym
b) prawa do uzupełnienia danych
c) prawa do samodzielnej edycji swoich danych osobowych
d) prawa do modyfikacji

8. RODO nakłada obowiązek informowania o:

a) profilowaniu
b) wielkości obrotów firmy
c) tym, kto jest procesorem danych osobowych
d) odpowiedzialności administratora danych

8. RODO nakłada obowiązek informowania o:

a) profilowaniu
b) wielkości obrotów firmy
c) tym, kto jest procesorem danych osobowych
d) odpowiedzialności administratora danych


PRAWO PODMIOTU DANYCH
- rozbudowane prawo do informacji, prawo do bycia zapomnianym
ZGŁASZANIE INCYDENTÓW
- do 72 godzin, wysokie kary za brak zgłoszenia
Obowiązywanie od 25.05.2018
2018
Prawo do bycia zapomnianym
Wysokie kary finansowe
RODO
Szybkie zgłaszanie incydentów
Zasięg globalny
Narzędzia do zapewnienia zgodności z RODO
KARY FINANSOWE
- do 20 mln euro lub 4% wartości rocznego obrotu
ZASIĘG GLOBALNY
- wszędzie tam, gdzie przetwarzane są dane osobowe obywateli EU

Przepisy obowiązujące obecnie

- **Ustawa** z dnia 29 sierpnia 1997 r. o ochronie danych osobowych
- **Rozporządzenie Ministra Spraw Wewnętrznych i Administracji** z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- **Rozporządzenie Ministra Administracji i Cyfryzacji** z dnia 11 maja 2015 r. w sprawie sposobu prowadzenia przez administratora bezpieczeństwa informacji rejestru zbiorów danych
- **Rozporządzenie Ministra Administracji i Cyfryzacji** z dnia 11 maja 2015 r. w sprawie trybu i sposobu realizacji zadań w celu zapewniania przestrzegania przepisów o ochronie danych osobowych przez administratora bezpieczeństwa informacji
- **ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY** (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych. Obowiązek dostosowania do dnia 25 maja 2018r.

Ważne pojęcia i skróty

- **GIODO - G**eneralny **I**nspektor **O**chrony **D**anych **O**sobowych – po 25 maja 2018 – Prezes Urzędu Ochrony Danych Osobowych (**PUODO**).
- **ADO** - **A**dministrator **D**anych **O**sobowych (Administrator) - osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi **ustala cele i sposoby przetwarzania** danych osobowych.
- **Podmiot przetwarzający** – (Procesor) osoba fizyczna lub prawna, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe **w imieniu administratora**

Ważne pojęcia i skróty

- **ABI** - Administrator Bezpieczeństwa Informacji po 25 maja – (IOD) Inspektor Ochrony Danych - osoba powołana przez Administratora, nadzorująca przestrzeganie ochrony danych osobowych
- **ASI** – Administrator Systemu Informatycznego osoba zarządzająca systemem informatycznym przetwarzającym dane osobowe, odpowiedzialna za jego funkcjonowanie oraz stosowanie technicznych i organizacyjnych środków ochrony,
- **Osoba upoważniona do przetwarzania danych osobowych** - osoba upoważniona pisemnie co do sposobu i zakresu przetwarzania danych osobowych

3 etapy tworzenia prawa w UE

1. Etap dziecięcy (niewiążące zalecenia i opinie)
2. „Klonowanie” norm dyrektyw przez państwa członkowskie (obecny 95/46/WE)
3. Rozporządzenie (wiąże wszystkie państwa członkowskie)

Jak wielka jest skala zmian?

95/46/WE
(UODO)

RODO
(GDPR)

Jak wielka jest skala zmian?

62 artykuły

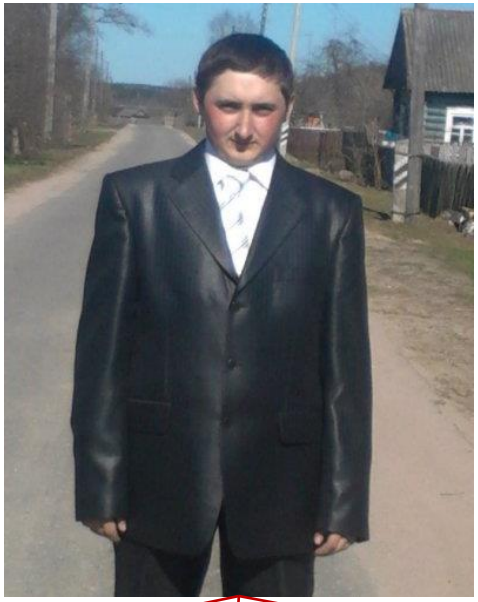
- 99 artykułów
- 173 motywy preambuły
- polska ustawa
- „dobre praktyki”

RODO

WG

MINISTERSTWA ADMINISTRACJI I CYFRYZACJI

OBECNIE



RODO

Audyt

Czym są dane osobowe? (art. 4 RODO)

„**dane osobowe**” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”);

Dane osobowe przed RODO

UE: „Dane osobowe to informacje, które umożliwiają w sposób pośredni lub bezpośredni identyfikację osoby”

(Dyrektywa 95/46/WE, art. 2: *Ochrona osób fizycznych w zakresie przetwarzania danych oraz swobodnego przepływu tych danych*)

Polska: Ustawa z dnia 29.08.1997 o ochronie danych osobowych, Dz. U. z 1997 nr 133 poz. 883 z późniejszymi zmianami: jeżeli koszty identyfikacji (także czasowe i działaniowe) byłyby zbyt wysokie wówczas **nie uważa się** że na podstawie zebranych danych można ustalić dane osobowe.

Czym są dane osobowe? (art. 4 RODO)

możliwa do zidentyfikowania osoba fizyczna to osoba, **którą można bezpośrednio lub pośrednio zidentyfikować**, w szczególności na podstawie identyfikatora takiego jak:

- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji,
- identyfikator internetowy
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Przykłady danych osobowych

- **Joanna.Swiebocka@fis.agh.edu.pl**
- **84011712345 - PESEL**
- **pawel1234@wp.pl**
- **Zapisy rozmów telefonicznych**
- **86 10203040 0000 1111 2222 3333**
- **Adres IP, MAC-adres**
- **+48 111 222 333**

Każda informacja – potencjalnie – może mieć charakter danych osobowych, jeśli:

1. odnosi się do osoby fizycznej,
2. umożliwia identyfikację tej osoby – samodzielnie lub wraz z innymi informacjami, do których dany podmiot ma dostęp lub zgodnie z prawem może mieć dostęp.

Dane wrażliwe

Dyrektywa WE/95/46: wprowadzenie w państwach członkowskich kategorii danych szczególnie chronionych, które mogą być przetwarzane tylko wtedy gdy zajdzie taka konieczność przewidziana w ustawie (art. 8 i 23)

- Poglądy polityczne
- Informacje o zdrowiu
- Informacje o życiu płciowym (orientacja)
- Pochodzenie rasowe

Dane biometryczne
ART.4 PKT 14 RODO

Dane biometryczne - dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne

Dane wrażliwe: Polska

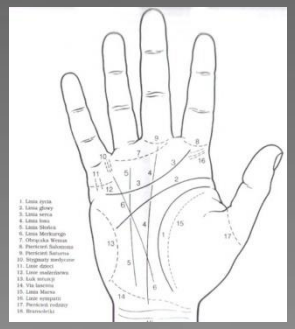
Rozszerzenie zakresu danych wrażliwych o:

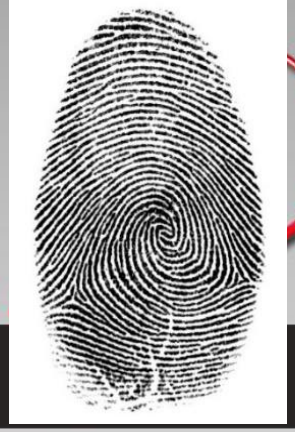
- **Kod genetyczny**
- Nałogi
- Wyroki skazujące w postępowaniu karnym
- Przynależność wyznaniowa
- Przynależność partyjna

DANE BIOMETRYCZNE PODLEGAJĄ OGÓLNYM WYMOGOM OCHRONY USTAWOWEJ ALE ADMINISTRATOR DANYCH MOŻE SAMODZIELNIE PODNIESĆ ICH PRIORYTET BEZPIECZEŃSTWA

Rodzaje danych biometrycznych

- **FIZJOLOGICZNE, FIZYCZNE** – skutek zachodzenia (najczęściej w okresie prenatalnym) zmian fizykochemicznych formujących tkankę
- **BEHAWIORALNE** wykształcone lub wyuczone przez człowieka cechy/umiejętności o silnie indywidualnym charakterze, zależne od aktualnego stanu umysłu, zmienne w czasie i podatne na zamierzone zmiany



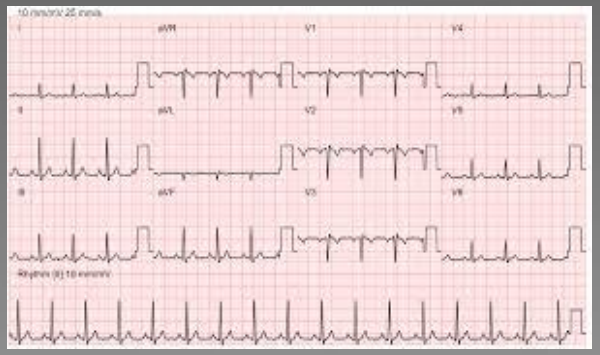


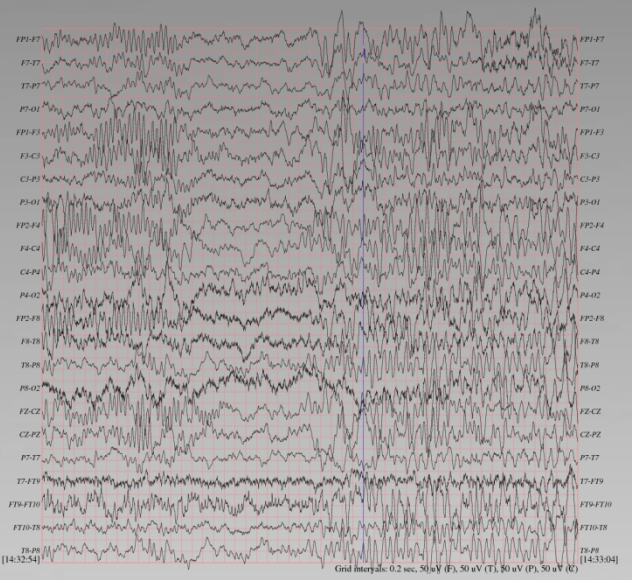
Biometryki fizyczne

- tęczówka oka,
- siatkówka (dno oka)
- linie papilarne,
- układ naczyń krwionośnych na dłoni lub przegubie ręki,
- kształt dłoni, kształt linii zgięcia wnętrza dłoni,
- kształt ucha,
- twarz,
- rozkład temperatur na twarzy,
- kształt i rozmieszczenie zębów,
- zapach, stopień zasolenia ciała
- DNA itp.

Biometryki behawioralne

- sposób chodzenia, ruch gałek ocznych
- tempo pisania na klawiaturze (nacisk)
- modulacja głosu
- rytm serca
- wzorzec oddychania
- EEG
- ECG





Czy fotografia jest daną biometryczną?

- informacje dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej,
- informacje mają charakter danych osobowych,
- informacje są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

Żeby wizerunek został uznany za dane biometryczne, taka możliwość identyfikacji musi wynikać z technologii przetwarzania wizerunku

Przetwarzanie danych osobowych dotychczas

Przetwarzanie danych osobowych – jakakolwiek operacja wykonywana na danych osobowych, taka jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie (Ustawa o ochronie danych osobowych, art.7 pkt. 3)

Art. 51 Konstytucji RP(przetwarzanie danych osobowych)

Art. 47 Konstytucji RP (prawo do prywatności)

GROMADZENIE DANYCH TYLKO W SYTUACJACH USTAWOWO PRZEWIDZIANYCH I NIEZBEDNYCH DO FUNKCJONOWANIA DEMOKRACJI

Przetwarzanie danych osobowych ART.4 RODO

„**przetwarzanie**” - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany

Przetwarzanie danych osobowych ART.4 RODO

- zbieranie,
- utrwalanie,
- organizowanie,
- porządkowanie,
- przechowywanie,
- adaptowanie lub modyfikowanie,
- pobieranie,
- **przeglądanie,**
- wykorzystywanie,
- ujawnianie poprzez przesłanie,
- rozpowszechnianie lub innego rodzaju udostępnianie,
- dopasowywanie lub łączenie,
- ograniczanie,
- usuwanie
- niszczenie;

Wymogi wobec przetwarzania danych osobowych

- **Zgodne z prawem;**
- **W jasno określonym celu (cel określa ADO);**
- **Z upoważnienia lub powierzenia (przez ADO);**
- **Wyłącznie na polecenie ADO;**
- **Adekwatne (minimalizacja);**
- **Bezpieczne dla osoby której dotyczy.**

Art. 29 RODO

Podmiot przetwarzający oraz **każda osoba** działająca z upoważnienia administratora lub podmiotu przetwarzającego i **mająca dostęp** do danych osobowych **przetwarzają je wyłącznie na polecenie administratora**, chyba że wymaga tego prawo Unii lub prawo państwa członkowskiego

Art. 28 RODO

1.Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą.

2.Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.

3.Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający:

Art. 28 RODO

a)przetwarza dane osobowe wyłącznie na udokumentowane polecenie administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający; w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny;
b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy;
c) podejmuje wszelkie środki **wymagane na mocy art. 32**;
d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4;
e) biorąc pod uwagę charakter przetwarzania, w miarę możliwości pomaga administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III;
f) uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi wywiązać się z obowiązków określonych w art. 32–36;
g) po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji administratora usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych;
h) udostępnia administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia administratorowi lub audytorowi upoważnionemu przez administratora przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich. 4.5.2016 L 119/49 Dziennik Urzędowy Unii Europejskiej PL

W związku z obowiązkiem określonym w h) **podmiot przetwarzający niezwłocznie informuje administratora, jeżeli jego zdaniem wydane mu polecenie stanowi naruszenie niniejszego rozporządzenia** lub innych przepisów Unii lub państwa członkowskiego o ochronie danych.

Art. 28 RODO

4.Jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii lub prawu państwa członkowskiego – te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, o których to obowiązkach mowa w ust. 3, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia. Jeżeli ten inny podmiot przetwarzający nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków tego innego podmiotu przetwarzającego spoczywa na pierwotnym podmiocie przetwarzającym.

Art. 32 RODO

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:

a) pseudonimizację i szyfrowanie danych osobowych;

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

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

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

Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności 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.

Pseudonimizacja

- przetwarzanie danych osobowych w taki sposób, aby nie było możliwe zidentyfikowanie, do kogo one należą, bez dostępu do innych informacji, przechowywanych bezpiecznie w innym miejscu.
- polega ona na zastępowaniu jednego atrybutu (bardzo często nietypowego) w zapisie innym atrybutem.
- powinna być odwracalna (dane, które zostały “zaszyfrowane”, można odszyfrować za pomocą odpowiedniego klucza).

Pseudonimizacja

- **szyfrowanie kluczem tajnym** - obecność klucza pozwala jednocześnie utajnić zbiór danych i w razie konieczności ponownie go odczytać, przypisując konkretne informacje do konkretnych osób (jedynie posiadanie klucza daje możliwość odszyfrowania danych);
- **tokenizacja** - jest to technika szyfrowania jednokierunkowego i polega na zastąpieniu fragmentów danych ciągiem losowych liczb, co sprawia, że informacje te stają się bezużyteczne dla osób postronnych. Metoda ta często jest wykorzystywana w branży finansowej.
- **skracanie** - czyli skrócenie wybranych wartości, tak aby odczytanie ich faktycznego znaczenia stało się niemożliwe;

Bezpieczeństwo informacji

- **poufność danych** — dane nie są udostępniane nieupoważnionym podmiotom;
- **dostępność danych** — dane są udostępniane upoważnionym podmiotom, kiedy tego potrzebują;
- **integralność danych** —dane były modyfikowane w sposób świadomy przez uprawniony podmiot;
- **rozliczalność** — działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

Wdrożenie art. 32

Parametr bezpieczeństwa	Poziom zapewnienia - *przykłady*
pseudonimizację	*na poziomie logowania*
szyfrowanie	*Brak*
zapewnienie poufności	*Dostęp wyłącznie po zalogowaniu*
zapewnienie integralności	*logowanie działań użytkowników*
zapewnienie dostępności	*Backup co 24 godziny*
zapewnienie odporności systemów	*Monitorowanie wydajności*
zapewnienie odporności usług przetwarzania	*Trzy kanały zgłaszania (system, email. Telefon)*
zdolność do szybkiego przywrócenia	*Testy odzyskiwania backup (co pół roku) – dwie godziny po awarii*
regularne testowanie	**brak**
mierzenie i ocenianie skuteczności	**brak,** *analiza ryzyka raz w roku*

Podstawowe obowiązki ADO

- Sporządzenie rejestru procesów przetwarzających dane osobowe, zarówno własne jak i powierzone przez klientów - art. 30
- Wykonanie analizy zagrożeń, oszacowanie ryzyka, ocena skutków przetwarzania dla osób których dane dotyczą – art. 35
- Na podstawie analizy - właściwy i adekwatny dobór zabezpieczeń (rozliczalność) – art. 32
- Wyznaczenie Inspektora Ochrony Danych – art. 37
- Opracowanie i wdrożenie procedury powiadomienia Urzędu Ochrony Danych Osobowych o naruszeniu bezpieczeństwa – art.33
- Przeszkolenie i upoważnienie pracowników do przetwarzania danych
- Właściwe powierzenie przetwarzania (art.28)

Rejestrowanie czynności przetwarzania

1.Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się **wszystkie następujące informacje:**

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych;

b) cele przetwarzania;

c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych; 4.5.2016 L 119/50 Dziennik Urzędowy Unii Europejskiej PL

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;

e) gdy ma to zastosowanie, przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, **ogólny opis technicznych i organizacyjnych środków bezpieczeństwa**, o których mowa w art. 32 ust. 1.

Rejestrowanie czynności przetwarzania

2.Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:

a) imię i nazwisko lub nazwa oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie – przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych;

b**) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów**;

c) gdy ma to zastosowanie –przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń;

d) **jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.**

3.Rejestry, o których mowa w ust. 1 i 2, mają formę pisemną, w tym formę elektroniczną.

4.Administrator lub podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel administratora lub podmiotu przetwarzającego udostępniają rejestr na żądanie organu nadzorczego

3 naczelne zasady

- Protection (privacy) by design
- Privacy by default
- Risk based approach

Protection by design

Potrzeba precyzyjnego zapisu, z którego wynika wprost, **że nie tylko** same przetwarzanie danych osobowych **ale również projektowanie** systemów, urządzeń, aplikacji, procesów, a więc podejmowanie wszelkiego rodzajów działań przygotowawczych **wymaga szczególnego nadzoru nad bezpieczeństwem przetwarzania** danych.

Zasada „protection by design” obejmuje również: **„konserwacje” i „serwisowanie”** aplikacji służących do przetwarzania danych osobowych zgodnie z RODO, **w tym prowadzeniu wszelkich testów** i działań zorientowanych na wymierzenie poziomów bezpieczeństwa i ryzyka.

Protection by design

- obowiązek stosowania mechanizmów zapewniających zgodność z RODO powstaje **na każdym etapie** prac/działań związanych z przygotowaniem/projektowaniem prac zorientowanych do przetwarzania danych.

- Zapisy RODO jasno wskazują, że cały proces przetwarzania danych, **począwszy od fazy projektowania** winien podlegać szczególnej dbałości aby sprostać wymaganiom RODO.

Privacy-by-default

Zbierając dane, należy domyślnie założyć, że klient **NIE wyraża zgody** na ich przetwarzanie w żaden sposób

Zgoda

- Jednoznaczna (celowe działanie),
- Świadoma (jasny język, niezbędne informacje),
- Konkretna (cel i zakres przetwarzania),
- Dobrowolna (realny wybór, brak konsekwencji).

ZGODA OGÓLNA JEST NIEDOPUSZCZALNA

(także na przekazywanie danych innym podmiotom)

Ale….

Zgody pozyskane w oparciu o Ustawę o Ochronie Danych Osobowych pozostaną ważne

(pod warunkiem że zostały zebrane zgodnie z RODO)

Dane osobowe w stosunku pracy

Art. 22[1]. § 1. Pracodawca ma prawo żądać od osoby ubiegającej się o zatrudnienie podania danych osobowych obejmujących:

1) imię (imiona) i nazwisko,

2) imiona rodziców,

3) datę urodzenia,

4) miejsce zamieszkania (adres do korespondencji),

5) wykształcenie,

6) przebieg dotychczasowego zatrudnienia.

„brak równowagi w relacji pracodawca pracownik stawia pod znakiem zapytania dobrowolność wyrażeniu zgody na pobieranie i przetworzenie danych osobowych (biometrycznych). Z tego względu ustawodawca ograniczył przepisem art. 221 [Kodeksu pracy] katalog danych, których pracodawca może żądać od pracownika. Uznanie faktu wyrażenia zgody na podstawie art. 23 ust. 1 pkt 1 [u.o.d.o.], jako okoliczności legalizującej pobranie od pracownika innych danych niż wskazane w art. 221 [Kodeksu Pracy], stanowiłoby obejście tego przepisu”

(wyrok Naczelnego Sądu Administracyjnego z 1.12.2009 r., I OSK 249/09, opubl. ONSAiWSA 2011, Nr 2, poz. 39)

„[w] prawie państwa członkowskiego lub w porozumieniach zbiorowych, w tym zakładowych porozumieniach z przedstawicielami pracowników, mogą być przewidziane przepisy szczegółowe o przetwarzaniu danych osobowych pracowników w związku z zatrudnieniem, w szczególności warunki, na których dane osobowe w związku z zatrudnieniem można przetwarzać za zgodą pracownika do celów procedury rekrutacyjnej, wykonywania umowy o pracę, w tym wykonywania obowiązków określonych w przepisach lub w porozumieniach zbiorowych, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.”.

(Motyw 155 preambuły RODO)

Ocena ryzyka
ART. 35 RODO

1. 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, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.

2. Dokonując oceny skutków dla ochrony danych, administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.

3. Ocena skutków dla ochrony danych, o której mowa w ust. 1, jest wymagana w szczególności w przypadku:

a) 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;

b) 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; lub

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Inspektor Ochrony Danych
ART. 37, 38, 39

1.Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2.Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

Kontrola zewnętrzna

Nowa ustawa powoła nowy **Urząd Ochrony Danych Osobowych – „UODO”**

UODO może nas kontrolować, czy przestrzegamy zasad ochrony danych osobowych (**RODO)**

- ✓ **kontrolować planowo**
- ✓ **z powodu skargi osoby postronnej**
- ✓ **z powodu skargi klienta**

UODO będzie mógł kierować niektóre naruszenia do procedowania karnego (więzienie/grzywna).

Incydenty bezpieczeństwa informacji

Zdarzenie, które stwarza możliwość zakłócenia ważnych procesów biznesowych albo **ujawnienia informacji** ważnych dla firmy lub **chronionych z mocy prawa**.

Incydent krytyczny – taki którego skutki mogą mieć istotny wpływ na funkcjonowanie firmy, grozić karami i sankcjami.

Incydenty krytyczne, w przypadku których reakcja musi zostać podjęta natychmiast, obsługiwane są na bieżąco i muszą być **zgłaszane bezzwłocznie** poprzez kontakt bezpośredni (telefon, kontakt osobisty) z Inspektorem Ochrony Danych lub z własnym przełożonym.

Przykłady

- ✓ ujawnienie hasła, kodu dostępu,
- ✓ wygląd aplikacji inny niż zwykle,
- ✓ inny zakres danych niż zwykle dostępny dla użytkownika,
- ✓ znaczne spowolnienie działania systemu informatycznego,
- ✓ pojawianie się niestandardowych komunikatów generowanych przez system informatyczny,
- ✓ ślady włamania lub prób włamania do pomieszczeń,
- ✓ włamanie lub próby włamania do szafek,
- ✓ kradzież sprzętu (np. komputer przenośny, telefon),
- ✓ pozostawienie wydruków poza strefami chronionymi,
- ✓ zagubienie lub kradzież nośnika (karty zbliżeniowej, karty kryptograficznej, tokena, nośnika z hasłami/kluczami, itp.),
- ✓ informacja z systemu antywirusowego

Więcej przykładów….

- ✓fizyczne zniszczenie lub podejrzenie zniszczenia elementów systemu,
- ✓podejrzenie nieautoryzowanej modyfikacji danych,
- ✓znalezienie lub zgubienie kluczy do pomieszczeń,
- ✓zauważenie dostępu osoby nieuprawnionej do przebywania,
- ✓przechowywanie na stacji roboczej lub dysku sieciowym plików bez praw autorskich lub nielegalnego oprogramowania,
- ✓ujawnienie informacji chronionej,
- ✓zidentyfikowanie urządzeń podsłuchowych,
- ✓sabotaż systemów zabezpieczeń technicznych,
- ✓naruszenie zasad bezpieczeństwa.

Co należy zgłaszać?

„przypadkowe lub niezgodne z prawem zniszczenie, utracenie, zmodyfikowanie, nieuprawnione ujawnienie lub nieuprawniony dostęp do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzany przez firmę”

Co robić w razie incydentu?

Każdy biorący udział w przetwarzaniu danych w systemie informacyjnym, jest odpowiedzialny za ich bezpieczeństwo oraz zgłaszanie ewentualnych incydentów bezpieczeństwa informacji.

Wszyscy pracownicy/współpracownicy i w każdym przypadku naruszenia lub uzasadnionego podejrzenia możliwości naruszenia bezpieczeństwa informacji powinni:

- powstrzymać się od rozpoczęcia lub kontynuowania jakiejkolwiek czynności mogącej spowodować zatarcie śladów bądź dowodów naruszenia bezpieczeństwa,
- podjąć stosownie do zaistniałej sytuacji niezbędne działania dla zapobieżenia dalszym konsekwencjom zagrożenia,
- **powiadomić upoważnione osoby o zaistniałym incydencie**.

Incydenty **krytyczne muszą być zgłaszane bezzwłocznie**.

Jak zgłaszać incydent?

- opis zdarzenia,
- miejsce wystąpienia zdarzenia,
- (opcjonalnie) dane osoby zgłaszającej.

Kontakt telefoniczny lub osobisty z **Inspektorem Ochrony Danych**

O STRACIE DANYCH NALEŻY POWIADOMIĆ TAKŻE „KLIENTA”

(jak również o konsekwencjach i zastosowanych środkach zaradczych)

Czy zawsze?

NIE!

Tylko gdy istnieje ryzyko naruszenia praw i wolności ludzkich:

- Kradzież lub sfałszowanie tożsamości
- Strata finansowa
- Naruszenie dobrego imienia
- Naruszenie tajemnic prawnie chronionych

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu. Art. 33 RODO

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
    a) opisywać charakter naruszenia ochrony danych osobowych, 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;
    b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
    c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
    d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki
5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

Kary administracyjne
ART. 83 RODO

Administracyjne kary pieniężne *(projekt ustawy o ochronie danych osobowych)*

Art. 82. Prezes Urzędu może nałożyć na podmioty nie będące organami publicznymi w rozumieniu w art. 5 § 2 pkt 3 ustawy z dnia 14 czerwca 1960 r. - Kodeks postępowania administracyjnego albo podmiotami publicznymi w rozumieniu w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, w drodze decyzji, administracyjne kary pieniężne na podstawie i na warunkach określonych w **art. 83 rozporządzenia** 2016/679.

Ogólne warunki nakładania administracyjnych kar pieniężnych *(**RODO**)*

Art. 83 Każdy organ nadzorczy zapewnia, by stosowane na mocy niniejszego artykułu za naruszenia niniejszego rozporządzenia administracyjne kary pieniężne, o których mowa w ust. 4, 5 i 6, były w każdym indywidualnym przypadku **skuteczne, proporcjonalne i odstraszające**.

3) Jeżeli **administrator lub podmiot przetwarzający** narusza umyślnie lub nieumyślnie w ramach tych samych lub powiązanych operacji przetwarzania kilka przepisów niniejszego rozporządzenia, całkowita wysokość administracyjnej kary pieniężnej nie przekracza wysokości kary za najpoważniejsze naruszenie.

4) Naruszenia przepisów dotyczących obowiązków podmiotu, podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości **do 10 000 000 EUR**, a w przypadku przedsiębiorstwa – w wysokości do 2 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

5) Naruszenia przepisów dotyczących podstawowych zasad i praw, podlegają zgodnie z ust. 2 administracyjnej karze pieniężnej w wysokości **do 20 000 000 EUR**, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa.

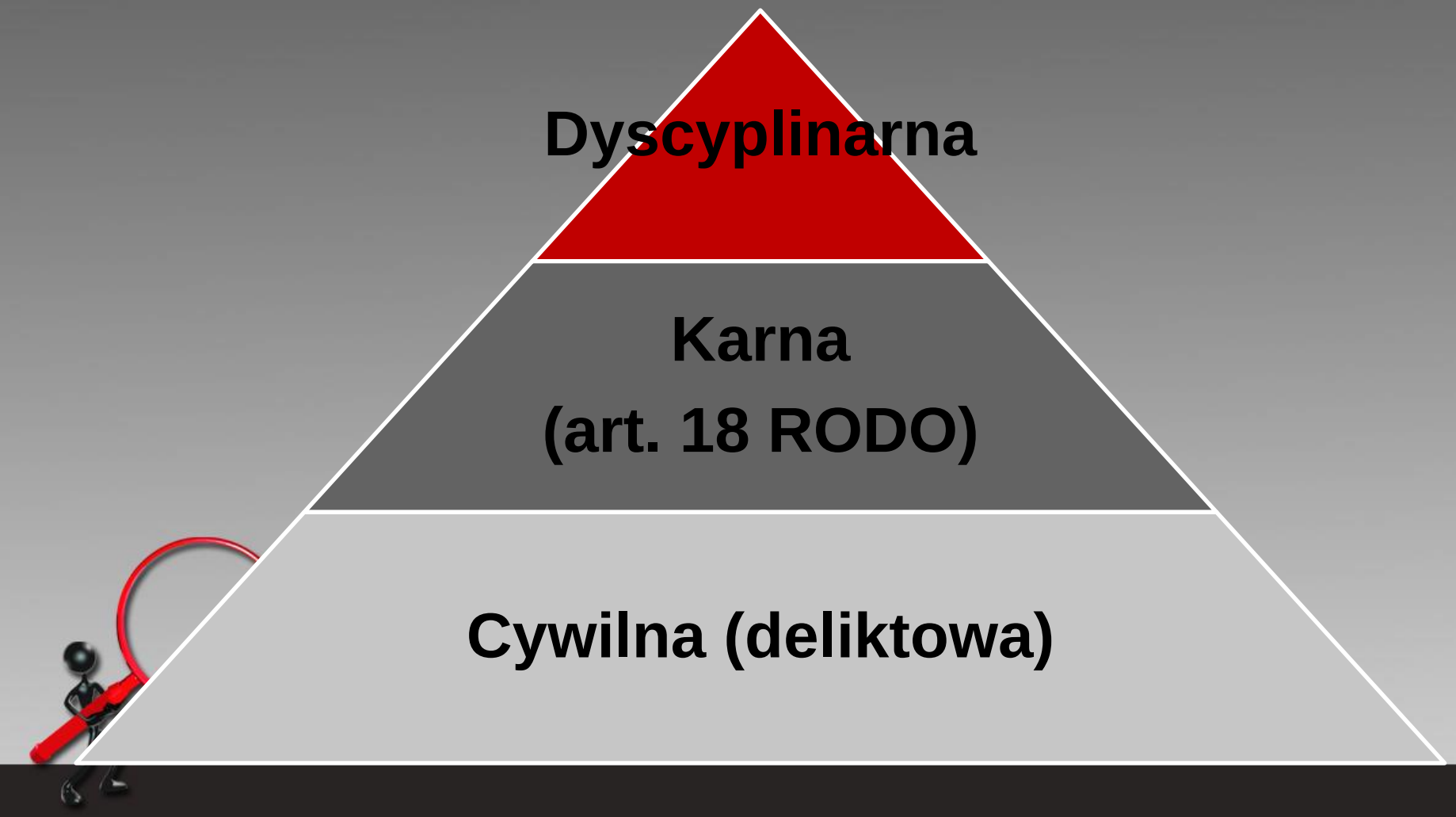
Art. 85. *(projekt ustawy o ochronie danych osobowych)*

1. **Środki finansowe pochodzące z kar pieniężnych stanowią dochód budżetu państwa.**

Skąd wiedzieć że dane są dobrze chronione?

- Audyt
- Urząd Ochrony Danych Osobowych (certyfikat)
- Polskie Centrum Akredytacji (prawdopodobnie certyfikat)

Odpowiedzialność w ODO



Odpowiedzialność w ODO

Odpowiedzialność **dyscyplinarna**

- kary - regulamin pracy

Odpowiedzialność **karna** (obecnie do 24.05)

- *nieuprawnione przetwarzanie - 2 lata (3 lata)*
- *brak ochrony danych przez ADO - 2 lata (1 rok)*
- *niedopełnienie obowiązku informacyjnego - 1 rok*
- *brak rejestracji zbiorów - 1 rok*

Odpowiedzialność **RODO - od 25 maja 2018**

Odpowiedzialność **cywilna**

- deliktowa (art. 415 kodeksu cywilnego: „kto z winy swej wyrządził drugiemu szkodę, obowiązany jest do jej naprawienia”),
- z tytułu naruszenia dóbr osobistych (art. 24 kodeksu cywilnego: "...poszkodowany może żądać naprawienia szkody na zasadach ogólnych").

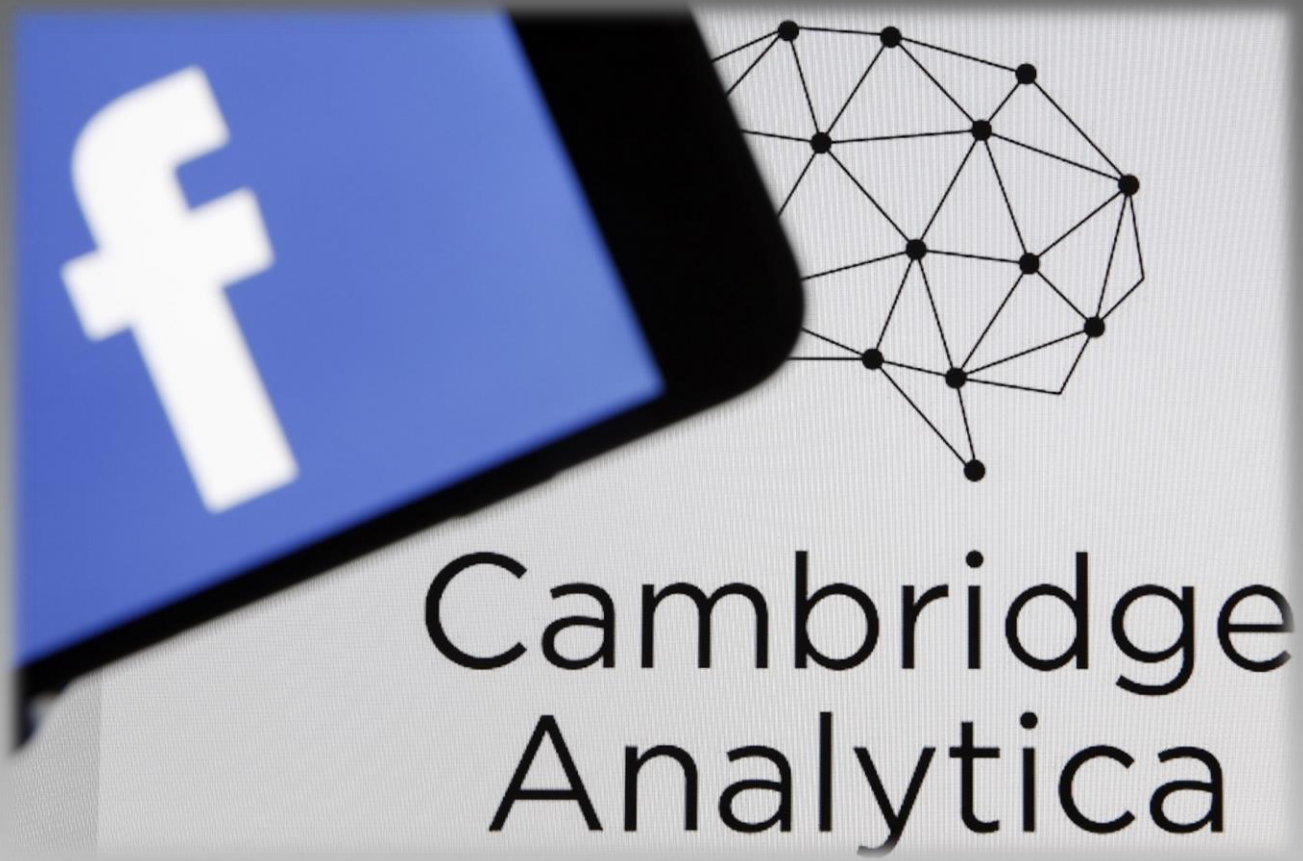
Obywatel UE ma prawo do:

1. bycia poinformowanym o przetwarzaniu jego danych osobowych
2. dostępu do własnych danych osobowych
3. sprostowania i uzupełnienia danych
4. całkowitego usunięcia danych (**bycia zapomnianym**)
5. ograniczenia przetwarzania
6. przenoszenia danych
7. sprzeciwu (cofnięcia zgody)
8. by nie podlegać profilowaniu

Prawo do bycia zapomnianym

https://gallery.dpcdn.pl/imgd/News/51558/g_-_-x-_-_-_x20140530100526_0.jpg

Facebook i Cambridge Analytica



Zalety RODO

- Zniesienie obowiązku zgłaszania bazy do GIODO
- Konsorcjum (łatwiejsze procedury)
- Profesjonalizacja
- Lepsza ochrona danych
- Elastyczność (różna wielkość instytucji, różny stopień zabezpieczeń)

Wady RODO

- KARY! (do 4% obrotów lub 20 mln euro)
- Ciągłość doskonalenia procedur ODO
- Więcej zgód (wydłużenie procesów interakcji, zniechęcenie)
- Prawo do bycia zapomnianym (problemy techniczne i organizacyjne)
- „Autodonos” (72h na zgłoszenie wycieku do PUODO)

DZIĘKUJĘ ZA UWAGĘ

jsw@agh.edu.pl

Art. 28 RODO

7.Komisja może określić standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z procedurą sprawdzającą, o której mowa w art. 93 ust. 2.

8.Organ nadzorczy może przyjąć standardowe klauzule umowne dotyczące kwestii, o których mowa w ust. 3 i 4 niniejszego artykułu, zgodnie z mechanizmem spójności, o którym mowa w art. 63.

9.Umowa lub inny akt prawny, o których mowa w art. 3 i 4, mają formę pisemną, w tym formę elektroniczną.

10.Bez uszczerbku dla art. 82, 83 i 84, jeżeli podmiot przetwarzający naruszy niniejsze rozporządzenie przy określaniu celów i sposobów przetwarzania, uznaje się go za administratora w odniesieniu do tego przetwarzania.

Filary ochrony danych osobowych

1. LEGALNOŚĆ PRZETWARZANIA
2. ŚWIADOMOŚĆ OSÓB PRZETWARZAJĄCYCH DANE
3. ZABEZPIECZENIA TECHNICZNE I ORGANIZACYJNE
4. NOTYFIKACJA DO REGULATORA
5. PRAWA I OBOWIĄZKI OSÓB KTÓRYCH DANE SĄ PRZETWARZANE