# Zmiany i wyzwania w ochronie danych osobowych związane z wprowadzeniem RODO

**Czy i jak *Kancelarie Notarialne powinny dostosować swoją działalność ?***

Maciej Kołodziej

*maciej.kolodziej@e-detektywi.pl*

*Tworzymy standardy i dobre praktyki …*

*Lublin, 14 kwietnia 2018*

**WWW.E-DETEKTYWI.PL**

Maciej Kołodziej

Wiceprezes „SABI - Stowarzyszenia Inspektorów Ochrony Danych”
ABI m.in. w ZPBI IAB Polska i Zespole Zarządców Nieruchomości
Wykładowca, doradca, specjalista informatyki śledczej e-Detektywi.pl i FHU MatSoft
Konsultant ds. ochrony danych osobowych, bezpieczeństwa informacji i systemów IT
Audytor wiodący i trener/wykładowca ISO/EIC 27001 (PECB)

## Źródła wymagań dotyczących bezpieczeństwa informacji

- **Konstytucja Rzeczypospolitej Polskiej**
  (tekst uchwalony 2 kwietnia 1997r., Dz.U. 1997 nr 78 poz. 483 ze zm.)

art.47
Każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym

art.51
1. Nikt nie może być obowiązany inaczej niż na podstawie ustawy do ujawniania informacji dotyczącej jego osoby
2. Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji niż niezbędne w demokratycznym państwie prawnym
3. Każdy ma prawo do dostępu do dotyczących go urzędowych dokumentów i zbiorów danych. Ograniczenie tego prawa może określić ustawa
4. Każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą
5. Zasady i tryb gromadzenia oraz udostępniania informacji określa ustawa

## Źródła wymagań dotyczących bezpieczeństwa informacji

- **Karta Praw Podstawowych Unii Europejskiej**

Art.8 Ochrona danych osobowych
1. Każdy ma prawo do ochrony danych osobowych, które go dotyczą.
2. Dane te muszą być przetwarzane rzetelnie **w określonych celach** i **za zgodą** osoby zainteresowanej **lub na innej uzasadnionej podstawie przewidzianej ustawą**. Każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania.
3. Przestrzeganie tych zasad podlega kontroli niezależnego organu.

## Źródła wymagań dotyczących bezpieczeństwa informacji

- **Dyrektywa 95/46/WE**

ROZDZIAŁ I PRZEPISY OGÓLNE

Artykuł 1 Cel dyrektywy

1. Zgodnie z przepisami niniejszej dyrektywy, Państwa Członkowskie zobowiązują się chronić podstawowe **prawa i wolności osób fizycznych**, w szczególności ich **prawo do prywatności** w odniesieniu do przetwarzania danych osobowych.
2. Państwa Członkowskie nie będą ograniczać ani zakazywać swobodnego przepływu danych osobowych między Państwami Członkowskimi ze względów związanych z ochroną przewidzianą w ust. 1.

## Źródła wymagań dotyczących bezpieczeństwa informacji

- **Ustawa** z dnia 29 sierpnia 1997 r. o **ochronie danych osobowych**
  (tekst jednolity Dz. U. z 2016 r. poz. 922; UODO)

  art.1 Każdy ma prawo do ochrony dotyczących go danych osobowych

- **Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych**, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
  (Dz. U. z 2004 r. Nr 100, poz. 1024; RT/O)

- **Rozporządzenia wykonawcze MAiC**
  - wzór zgłoszeń powołania i odwołania ABI (Dz. U. z 2014 r. poz. 1934)
  - sposób prowadzenia przez ABI rejestru zbiorów (Dz. U. z 2015 r. poz. 719)
  - tryb i sposób realizacji zadań przez ABI (Dz. U. z 2015 r. poz. 745)

## Źródła wymagań dotyczących bezpieczeństwa informacji

- **Rozporządzenie w sprawie Krajowych Ram Interoperacyjności**, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 2012 r. poz. 526; KRI)
  wydane na podstawie art. 18 Ustawy z dnia 17 lutego 2005r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2005 r. Nr 64, poz. 565, z późn. zm)

System Zarządzania Bezpieczeństwem Informacji w KRI:
§ 20 1. Podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system zarządzania bezpieczeństwem informacji zapewniający poufność, dostępność i integralność informacji z uwzględnieniem takich atrybutów, jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.
2. Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie następujących działań: {1)-14)}

## Zarządzanie bezpieczeństwem SZBI KRI cz.1

Kierownictwo podmiotu publicznego zobowiązane jest umożliwić realizację i egzekwować wykonywanie działań dotyczących:

1. aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmian procesu;
2. aktualności inwentaryzacji sprzętu i oprogramowania oraz ich konfiguracji;
3. prowadzenia okresowych analiz ryzyka oraz działań je minimalizujących;
4. przyznawania osobom przetwarzającym informacje uprawnienia odpowiednie do wykonywanych zadań i obowiązków w zakresie bezpieczeństwa;
5. bezzwłocznej modyfikacji uprawnień w przypadku zmiany obowiązków;
6. zapewnienia szkolenia osób przetwarzających informacje;
7. ochrony informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniami lub zakłóceniami poprzez monitorowanie dostępu do informacji, wykrywanie nieautoryzowanych działań oraz uniemożliwienie nieautoryzowanego dostępu do systemów, usług sieciowych i aplikacji;
8. zasad bezpiecznej pracy przy przetwarzaniu mobilnym i w pracy na odległość;
9. zabezpieczenia informacji przed jej nieuprawnionym ujawnieniem, modyfikacją, usunięciem lub zniszczeniem;

## Zarządzanie bezpieczeństwem SZBI KRI cz.2

Kierownictwo podmiotu publicznego zobowiązane jest umożliwić realizację i egzekwować wykonywanie działań dotyczących:

10. zawierania w umowach serwisowych zapisów gwarantujących odpowiedni poziom bezpieczeństwa informacji;
11. minimalizacji ryzyka kradzieży informacji i środków przetwarzania informacji, w tym urządzeń mobilnych;
12. odpowiedniego poziomu bezpieczeństwa systemów teleinformatycznych poprzez aktualizację oprogramowania, zapobieganie awariom, ochronę przed błędami i nieuprawnioną modyfikacją, stosowanie mechanizmów kryptograficznych, redukcję ryzyk wynikających z wykorzystania opublikowanych podatności technicznych, reagowanie po dostrzeżeniu nieujawnionych podatności oraz kontrolę ich zgodności z normami i politykami bezpieczeństwa;
13. bezzwłocznego zgłaszania incydentów naruszania bezpieczeństwa informacji umożliwiającego szybkie podjęcie działań korygujących;
14. **zapewnienia audytu wewnętrznego bezpieczeństwa informacji, nie rzadziej niż raz na rok**;
15. ustanowienia dodatkowych zabezpieczeń w systemach teleinformatycznych, w przypadkach uzasadnionych wynikami analizy ryzyka;
16. wiarygodnego dokumentowania rozliczalności w systemach teleinformatycznych poprzez elektroniczne zapisy w dziennikach systemów.

## Regulacje branżowe w Kancelarii Notarialnej

- Prawo o notariacie (od art. 79)
- Rozporządzenie ministra sprawiedliwości z 12.04.1991 r. w sprawie prowadzenia ksiąg notarialnych oraz przekazywania na przechowanie dokumentów sądom rejonowym.
- Rozporządzenie Ministra Sprawiedliwości z dnia 27 sierpnia 2001 r. w sprawie pobierania przez notariuszy opłat sądowych od wniosków o wpis do księgi wieczystej zamieszczanych w aktach notarialnych
- Ustawa z dnia 9 września 2000 r. o podatku od czynności cywilnoprawnych (Art. 10)
- Ustawa z dnia 28 lipca 1983 r. o podatku od spadków i darowizn (Art. 18)
- Ustawa Prawo o notariacie
- Ustawa z dnia 17 maja 1989 r. Prawo geodezyjne i kartograficzne (Art. 23)
- Ustawa z dnia 27 marca 2003 r. o planowaniu i zagospodarowaniu przestrzennym (Art. 37)
- Rozporządzenie Ministra Sprawiedliwości z dnia 25 lutego 2009 roku zmieniające rozporządzenie w sprawie określenia rodzajów i zakresu informacji przekazywanych organom podatkowym przez sądy, komorników sądowych i notariuszy oraz terminu, formy, z uwzględnieniem formy wypisu aktu i sposobu ich przekazywania
- Ustawa z dnia 15 grudnia 2000 r. o spółdzielniach mieszkaniowych (Art. $17^{2)}$
- Ustawa z dnia 24 marca 1920 r. o nabywaniu nieruchomości przez cudzoziemców (Art. 8a.)
- Ustawa z dnia 17 listopada 1964 r. kodeks postępowania cywilnego (Art. 640, Art. 652, Art. 665)
- Ustawa z dnia 15 września 2000 roku kodeks spółek handlowych (art.210§2 ksh, art.379§2 ksh)
- Ustawa o „praniu pieniędzy” i zapobieganiu terroryzmowi

## Inne przepisy i regulacje

- Ustawa Prawo Pracy (art. $22^1$)

- Ustawy samorządowe (województwo, gmina, powiat)
- Przepisy szczególne w administracji publicznej (np. Centra Usług Wspólnych)
- Ustawa Prawo zamówień publicznych
- Ustawa o dostępie do informacji publicznej *{o jawności życia publicznego}*

- Ustawa o świadczeniu usług drogą elektroniczną (art.9-10, 16-22) *{ePrivacy}*
- Ustawa Ordynacja Podatkowa
- Ustawa Prawo Telekomunikacyjne (art.173-174)
- Ustawa o swobodzie działalność gospodarczej
- Ustawa o Ochronie Baz Danych
- Ustawa o Prawie Autorskim i Prawach Pokrewnych
- Pakiet przepisów konsumenckich
- Kodeksy: Karny, Administracyjny i Cywilny
- Przepisy i normy branżowe np. medyczne, szkolnictwo, ubezpieczeniowe, …

## Źródła wymagań dotyczących bezpieczeństwa informacji

- Normy ISO - przykłady
  - grupa norm z serii 27000 –Bezpieczeństwo Informacji
    - PN-ISO/IEC 27001:2017-06 – „Systemy zarządzania bezpieczeństwem informacji – wymagania”
    - PN-ISO/IEC 27002:2017-06 – „Praktyczne zasady zabezpieczania informacji”
    - PN-ISO/IEC 27005:2014-01 – „Zarządzanie ryzykiem w bezpieczeństwie informacji”
    - PN-ISO/IEC 27017:2017-07 – „Praktyczne zasady zabezpieczania informacji dla usług w chmurze”
    - PN-ISO/IEC 27018:2017-07 – „Praktyczne zasady ochrony danych identyfikujących osobę w chmurach“
  - PN-ISO/IEC 20000-1,-2 - zarządzanie usługami
  - PN-ISO/IEC 29100 - ramy prywatności, ochrona danych identyfikujących osobę
  - ISO/IEC 29134:2017 - Guidelines for privacy impact assessment, ocena skutków
  - PN-ISO/IEC 24762 - odtwarzanie w ramach ciągłości działania
  - PN-ISO 31000 - wytyczne dotyczące zarządzania ryzykiem, techniki oceny ryzyka

- Informacje prawnie chronione
  - Tajemnice zawodowe, przedsiębiorstwa, pracodawcy
  - Tajemnica pracownika samorządowego, skarbowa,
  - Informacje niejawne

## Źródła wymagań dotyczących bezpieczeństwa informacji

Regulacje wewnętrzne

- Polityka Bezpieczeństwa Danych Osobowych
  - Upoważnienia i oświadczenia dot. przetwarzania danych i zachowania poufności
  - Ewidencja/wykaz osób upoważnionych przetwarzających dane osobowe (konta, dopuszczenia)
  - Wzory umów o powierzenie przetwarzania danych osobowych
  - Wykaz umów związanych z przetwarzaniem danych osobowych
  - Wykaz zbiorów danych osobowych z bazami oraz programami
  - Wykaz systemów informatycznych wykorzystywanych do przetwarzania danych
  - Wykaz obszarów przetwarzania danych osobowych
  - Opis struktury zbiorów danych osobowych
  - Opis przepływu danych pomiędzy zbiorami danych osobowych
  - Opis zastosowanych środków technicznych i organizacyjnych
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
- Instrukcja postepowania w sytuacji naruszenia ochrony danych osobowych
- Polityka Bezpieczeństwa IT

## Źródła wymagań dotyczących 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 oraz uchylenia dyrektywy 95/46/WE

(Dz. U. UE 2016 poz. L119)

RODO - Rozporządzenie o Ochronie Danych Osobowych
GDPR - General Data Protection Regulation

***już obowiązuje, ale ma zastosowanie od 25 maja 2018 r.***

## Źródła wymagań dotyczących bezpieczeństwa informacji

Wytyczne Grupy Artykułu 29 do RODO

- WP242 Guidelines on the right to "data portability„
  Wytyczne dotyczące prawa do przenoszenia danych
- WP243 Guidelines on Data Protection Officers ('DPOs')
  Wytyczne dotyczące inspektorów ochrony danych
- WP244 Guidelines on The Lead Supervisory Authority
  Wytyczne dotyczące ustalenia wiodącego organu nadzorczego właściwego dla administratora lub podmiotu przetwarzającego
- WP248 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk„
  Wytyczne dotyczące oceny skutków dla ochrony danych oraz pomagające ustalić, czy przetwarzanie „może powodować wysokie ryzyko"
- WP250 Guidelines on Personal data breach notification
  Wytyczne dotyczące powiadomienia o naruszeniu ochrony danych osobowych
- WP251 Guidelines on automated individual decision-making and profiling
  Wytyczne dotyczące automatycznego indywidualnego podejmowania decyzji i profilowania
- WP253 Guidelines on the application and setting of administrative fines
  Wytyczne dotyczące stosowania i ustalania kar administracyjnych

## Stan prawny teraz i po 25.05.2018

- UODO to 55 artykułów
- 4 rozporządzenia

- RODO to 99 artykułów i 173 motywy
- nUODO, było: 92 (12.9.17), 158 (8.02.18), 170 (20.3.18) artykułów
- Ustawa „wprowadzająca RODO" miała 147 artykułów, miało być 170, obecnie (28.3.18) jest ok. 210. Modyfikuje, na 280 stronach, ponad 140 ustaw krajowych i ma 450 stron uzasadnienia
- Ogłoszono 7 wytycznych Grupy art. 29, będą kolejne publikacje
- Będą wytyczne Prezesa Urzędu Ochrony Danych Osobowych
- Będą Kodeksy Postępowania i Dobrych Praktyk
- Będzie Certyfikacja, a z nią normy pomocne w procesie audytu

## Rozporządzenie RODO a przepisy krajowe

- Bezpośrednia stosowalność przepisów RODO, bez konieczności dodatkowej implementacji do polskiego porządku prawnego

- Częściowa swoboda doprecyzowania/ograniczenia RODO przez prawo krajowe
- Uchylenie krajowej ustawy o ochronie danych osobowych i rozporządzeń
- Nowa ustawa „uzupełniająca" nUODO, czyli **XII Rozdział RODO**
- Konieczność przeprowadzenia nowelizacji obowiązujących przepisów krajowych pod kątem dostosowania ich do nowej unijnej regulacji

- Przepisy określają:
  - zasady postępowania przy przetwarzaniu danych osobowych
  - prawa osób fizycznych, których dane osobowe są lub mogą być przetwarzane
  - obszar stosowania do przetwarzania danych osobowych w każdej postaci
    - w kartotekach, teczkach, skorowidzach, księgach, wykazach i ewidencjach,
    - w systemach informatycznych.

## Rozporządzenie RODO
### najważniejsze zagadnienia (i problemy)

- Problem udzielenia i udokumentowania zgody (art.7), zgoda wyraźna vs jednoznaczna (motyw 32), także od osób niepełnoletnich (art. 8),
- Przenoszalność danych osobowych (art.20), a ochrona wtórnego wykorzystania
- Prawo do bycia zapomnianym (art.17) – problem nadzoru ADO nad przekazanymi danymi oraz egzekwowaniem praw podmiotu danych
- Obowiązki informacyjne (art.12-14) notyfikacja, informacje dodatkowe
- Pseudonimizacja vs anonimizacja danych
- Rejestrowanie czynności przetwarzania (art.30)
- Ochrona danych w fazie projektowania oraz domyślna ochrona danych (art. 25) {Privacy by design / Privacy by default}
- Analiza ryzyka przetwarzania danych (metodologia Risk Based Approach) Nowy obowiązek opracowania raportów zawierających ocenę skutków przetwarzania danych (art. 25 i 36),
- Wspólna odpowiedzialność, w razie istnienia wielu administratorów i podmiotów przetwarzających, wobec podmiotu danych którego prawa zostały naruszone (art. 82)
- Zwiększenie odpowiedzialności ADO w związku z naruszeniem postanowień dotyczących ochrony danych osobowych – sankcje, ostrzeżenia, dotkliwe kary finansowe wymagane bezwzględnie (art. 83)

## Rozporządzenie RODO
### Zabezpieczenia danych osobowych

- Wdrożenie środków technicznych i organizacyjnych zabezpieczenia danych na podstawie analizy ryzyka (art. 24 i 32)
- Wymóg wzięcia pod uwagę ochrony danych na etapie projektowania systemu oraz konieczność domyślnej ochrony danych (art. 25)
- Upoważnienie do przetwarzania nadawane przez administratora lub podmiot przetwarzający (art. 29)
- Prowadzenie rejestru czynności przetwarzania danych osobowych (art. 30)
- Zgłaszanie naruszeń ochrony danych organowi nadzorczemu (art. 33)
- Obowiązek powiadamiania podmiotu danych o naruszeniu ochrony (art. 34)
- Ocena skutków przetwarzania dla ochrony danych (art. 35)
- Uprzednie konsultacje z organem nadzorczym - wysokie ryzyko (art. 36)
- Inspektor Ochrony Danych (art. 37-39)
- Kodeksy postępowania i certyfikacja (art. 40-42)

## Proces ochrony danych osobowych
prawa osób których dane przetwarzamy, przykłady z RODO

- **Prawo do wiedzy i informacji**
- **Prawo do dostępu do zebranych danych osobowych**
- **Prawo do kopii danych**
- **Prawo do przeniesienia danych**
- **Prawo do usunięcia danych (wewnątrz struktur administratora danych)**

- Prawo do wiedzy i informacji o profilowaniu i jego konsekwencjach
- Prawo do udzielania zdalnego dostępu do bezpiecznego systemu zapewniającego bezpośredni dostęp do danych
- Prawo do nie naruszania tajemnicy handlowej, własności intelektualnej i praw autorskich
- Prawo do sprostowania danych
- Prawo do sprzeciwu co do przetwarzania danych osobowych
- …

## Co przyniesie RODO

**RODO to stan umysłu ;-)**

To zupełnie inne podejście do procesu ochrony danych osobowych
i nadzoru nad prywatnością podmiotów danych

RODO zaczyna się tam, gdzie kończy się UODO i jego rozporządzenia

Aby poprawnie interpretować obowiązki wynikające z RODO
konieczne jest procesowe podejście do systemu ochrony danych
oraz analiza ryzyka dla wszystkich elementów

## Proces ochrony danych osobowych

porównanie konstrukcji przepisów

**UODO**

Definicje | Zasady ochrony wymagania | Jak należy postępować zalecenia, wskazówki | Kontrola | Penalizacja

*art. 36-39 UODO*
*RTO + Rozp719 + Rozp745*

**RODO**

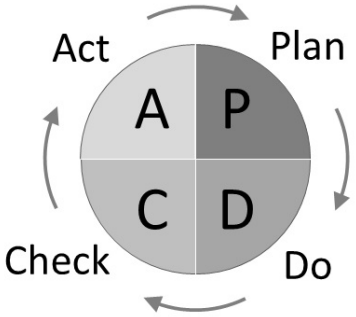
Definicje | Zasady ochrony | Co należy robić | Kontrola | Penalizacja

*art. 24, 30, 33 RODO*
*Brak konkretnych informacji jak należy postępować!*

## Proces ochrony danych osobowych

Zarządzanie ryzykiem naruszenia praw i wolności osób których dane są przetwarzane

- Ustanowienie kontekstu
- Szacowanie ryzyka
  - Identyfikowanie ryzyka
  - Analiza ryzyka
  - Ocena ryzyka
- Postępowanie z ryzykiem
- Akceptowanie ryzyka




## Proces ochrony danych osobowych

przykład przenikania się świata cyfrowego i analogowego

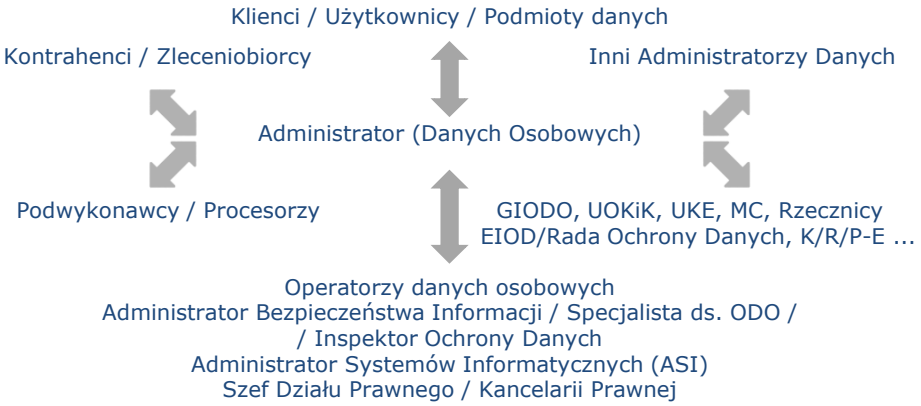
mail, aplikacja, drukarka, papier, długopis, skaner, aplikacja, mail

vs

papier, skaner, program, operator, program, drukarka, papier

## Ochrona danych osobowych - aktorzy

Kto jest kim i za co odpowiada ?




## Dane osobowe

**UODO art.6**

**Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej** (także wykonującej „osobową" działalność gospodarczą!), bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości osoby

**RODO art.4.1, motyw 30 i 26**

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

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 (adres IP, identyfikator plików cookies) lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej

„informacje anonimowe, czyli „informacje, 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.„

## Dane osobowe ?

*Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (także wykonującej „osobową" działalność gospodarczą!), bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby*

***Imię, nazwisko, nazwisko panieńskie matki, adres, numer telefonu ...***

## Dane osobowe ?

*Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (także wykonującej „osobową" działalność gospodarczą!), bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby*

***Czy samodzielnie występujący adres e-mail może być daną osobową***

nazwapodmiotu@domenapodmiotu
dział@domenapodmiotu, adreskontaktowy@domenapodmiotu
nazwapodmiotu@innadomena
stanowisko@domenapodmiotu, funkcja@domenapodmiotu
imie.nazwisko@domenapodmiotu
imie.nazwisko.podmiot@innadomena
imie.nazwisko@jakasdomena
jakas.nazwa@innadomena

## Dane osobowe ?

*Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej*
*(także wykonującej „osobową" działalność gospodarczą!),*
*bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby*

**Czy samodzielnie występujący adres IP może być daną osobową ?**
**Czy jesteśmy w stanie wskazać konkretnego użytkownika komputera w Internecie ?**

127.0.0.1, 192.168.1.3, 218.180.130.3

## Dane osobowe ?

*Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (także wykonującej „osobową" działalność gospodarczą!),*
*bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby*

**Czy PESEL może być daną osobową ?**
70031290778
99081200668
14301102671

| 440514 | 0145 | 8 |
|---|---|---|

- cyfry [1-6] – data urodzenia z określeniem stulecia urodzenia
- cyfry [7-10] – numer serii z oznaczeniem płci
  - cyfra [10] – płeć
- cyfra [11] – cyfra kontrolna

*UODO Art. 28. 2. Numery porządkowe stosowane w ewidencji ludności mogą zawierać tylko oznaczenie płci, daty urodzenia, numer nadania oraz liczbę kontrolną.*
*3. Zabronione jest nadawanie ukrytych znaczeń elementom numerów porządkowych w systemach ewidencjonujących osoby fizyczne.*

## Dane osobowe ?

*Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej (także wykonującej „osobową" działalność gospodarczą!), bez ponoszenia nadmiernych kosztów, czasu, działań w celu ustalenia tożsamości tej osoby*

**Czy zwierzę może być nośnikiem danych osobowych ?**

Chip
Lyssetka
Identyfikator



dogid
wyszukiwarka numerów chipów, lyssetek i identyfikatorów dog id

## Dane osobowe ?

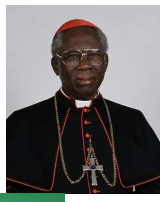
06281200642 13302102675



Ola – 09.2006/3,4kg/57cm Jasio – 11.2013/4,6kg/61cm

## Dane osobowe ?

Uwaga na dane wrażliwe !!
wymóg zgody na piśmie lub pozyskania z publicznych źródeł



Zabrania się przetwarzania
danych osobowych ujawniających:

- pochodzenie rasowe lub etniczne
- przekonania religijne lub filozoficzne
- poglądy polityczne
- przynależność wyznaniową, partyjną lub związkową
- dane o stanie zdrowia i kodzie genetycznym
- dane o nałogach, życiu seksualnym


## Nośniki danych osobowych

Ewidencje, rejestry, przetwarzanie na rzecz osób i podmiotów

- **Dokumentacja papierowa**
- **Systemy informatyczne**

- **Poczta konwencjonalna {SNAIL}** – wysyłka dedykowana oraz inserty;
- **Poczta elektroniczna {EMAIL}** – mailing, oferty, zapytania;
- **Serwisy WWW {DISPLAY}** – bannery, dedykowane informacje, promocja, zniżki;
- **Platformy mobilne {SMS, MMS, TELEFON}** – komunikacja dwustronna, SMSC;
- **Call Center, Telemarketing, BOK** – kontakt „na zewnątrz” i klient dzwoniący;

## Administrator Danych Osobowych w UODO art.7.4

**Administrator Danych** (organ, jednostka organizacyjna, podmiot lub osoba, …, **decydujące o celach i środkach przetwarzania danych osobowych**) ma obowiązek przed rozpoczęciem przetwarzania:

- określić cele, strategie i politykę zabezpieczania systemów informatycznych, w których przetwarzane są DO
- zidentyfikować i przeanalizować zagrożenia i ryzyko, na które może być narażone przetwarzanie DO
- określić potrzeby w zakresie zabezpieczenia zbiorów danych osobowych i systemów informatycznych, z uwzględnieniem potrzeby kryptograficznej ochrony danych osobowych, w szczególności podczas ich przesyłania za pomocą urządzeń teletransmisji danych
- określić zabezpieczenia adekwatne do zagrożeń i ryzyka
- monitorować działanie zabezpieczeń wdrożonych w celu ochrony danych osobowych i ich przetwarzania
- opracować i wdrożyć program szkolenia w zakresie zabezpieczeń systemu informatycznego
- wykrywać i właściwie reagować na przypadki naruszenia bezpieczeństwa danych osobowych i systemów informatycznych je przetwarzających

## Administrator i inni w RODO art.4.7-8; art.26

„**Administrator**" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania

„**Podmiot przetwarzający**" (potocznie „**procesor**") oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;

„**Współadministrator**" Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania, są oni współadministratorami. W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz ich obowiązków w odniesieniu do podawania informacji, o których mowa w art. 13 i 14, chyba że przypadające im obowiązki i ich zakres określa prawo Unii lub prawo państwa członkowskiego, któremu administratorzy ci podlegają. W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.

## Status formalny ABI/IOD

Pracownik, współpracownik, outsourcing

Rozporządzenia Ministra Pracy i Polityki Społecznej z dnia 7.8.2014 r. w sprawie klasyfikacji zawodów i specjalności na potrzeby rynku pracy oraz zakresu jej stosowania (Dz.U. 2014 r., poz. 1145).

242 Specjaliści do spraw administracji i zarządzania

2421 Specjaliści do spraw zarządzania i organizacji

**242111** Administrator Bezpieczeństwa Informacji

2422 Specjaliści do spraw administracji i rozwoju

**242212** Inspektor ochrony danych osobowych

Rozporządzenie Rady Ministrów z dnia 24 grudnia 2007 r. w sprawie Polskiej Klasyfikacji Działalności (PKD) (Dz. U. Nr 251, poz. 1885)

**PKD 70.22.Z** - Pozostałe doradztwo w zakresie prowadzenia działalności gospodarczej i zarządzania

**PKD 74.90.Z** - Pozostała działalność profesjonalna, naukowa i techniczna, gdzie indziej niesklasyfikowana

**PKD 85.59.B** - Pozostałe pozaszkolne formy edukacji, gdzie indziej niesklasyfikowane

**PKD 62.02.Z** - Działalność związana z doradztwem w zakresie informatyki

## Zadbajmy o ABI/IOD

Pracownik, współpracownik, outsourcing

Ubezpieczenie odpowiedzialności zawodowej ABI

OC dla ABI wykonującego czynności osobiście

Klasyfikacja zawodów poz. 242111/242212

Ubezpieczenie OC z tytułu prowadzenia działalności gospodarczej i użytkowania mienia

PKD 70.22.Z, 74.90.Z, 85.59.B, 62.02.Z

***OC - delikt***

*odpowiedzialność za czyn niedozwolony*

*tj. gdy jesteśmy niewinni, ale odpowiedzialni.*

***OC - kontrakt***

*odpowiedzialność za szkody wyrządzone przez niewykonanie lub nienależyte wykonanie zobowiązania.*

## Inspektor ochrony danych RODO art.37-39

Administrator (danych osobowych) i podmiot przetwarzający (procesor) wyznaczają inspektora ochrony danych

IOD - Inspektor Ochrony Danych (DPO - Data Protection Officer):

- Wyznaczenie Inspektora art. 37
- Status Inspektora art. 38
- Zadania Inspektora art. 39

## Wyznaczenie Inspektora art.37 - duże kancelarie

Inspektor będzie musiał być obowiązkowo wyznaczany przez Administratora oraz procesora, w następujących sytuacjach:

1.a) przetwarzania danych przez podmiot lub organ publiczny, z wyłączeniem sądów w ramach prowadzonych przez nie postępowań

**1.b) kiedy główna działalność polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą na dużą skalę.**

1.c) kiedy główna działalność polega na przetwarzaniu na dużą skalę szczególnych kategorii danych osobowych (danych wrażliwych), o których mowa w art. 9 ust. 1 RODO, a także danych dotyczących wyroków skazujących i naruszeń, o których mowa w art. 10 RODO.

**Nawet nie wyznaczając Inspektora należy realizować obowiązki wynikające z przepisów o ochronie danych oraz rozważyć posiadanie Specjalisty ds. Ochrony Danych Osobowych**

## Wytyczne Grupy 29 z 13.12.2016 r. dot. IOD

- „**Głównej działalności**" nie należy interpretować w sposób wyłączający działalność w zakresie przetwarzania danych nierozerwalnie związaną z działalnością główną.
- Przykładem może być spółka świadcząca usługi ochrony mienia, prowadząca monitoring w szeregu prywatnych centrów handlowych i przestrzeni publicznej. Jej działalnością główną jest ochrona, natomiast związane z tym bezpośrednio jest przetwarzanie danych osobowych, co oznacza, że takie spółki również muszą powołać IOD.
- GR Art. 29 jest świadoma, że wszystkie podmioty, spółki i inne organizacje prowadzą określone działania, np. prowadząc listę płac albo korzystając z obsługi IT.
  Są to niezbędne działania umożliwiające prowadzenie działalności głównej, jednak z racji na ich charakter uznane są za **poboczne**.

Czy przetwarzanie (w szczególności zbieranie i przechowywanie) danych osobowych Stron w Kancelariach Notarialnych można uznać za działania poboczne, nie będące Główną Działalnością Kancelarii ???

## Wyznaczenie Inspektora art.37

3. Możliwość wyznaczenia jednego Inspektora dla kilku podmiotów:

- Grupa przedsiębiorców może wyznaczyć jednego Inspektora, o ile można będzie łatwo nawiązać z nim kontakt z każdej z jednostki organizacyjnej.
- Kilka organów lub podmiotów publicznych może wyznaczyć jednego Inspektora, uwzględniając przy tym ich wielkość i strukturę organizacyjną.

## Wyznaczenie Inspektora art.37

5. Inspektor jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełniania zadań, o których mowa w art. 39 RODO.

6. Inspektor może być członkiem personelu Administratora lub procesora lub wykonywać zadania na podstawie umowy o świadczenie usług.

7. Administrator i procesor muszą opublikować dane kontaktowe do Inspektora oraz zawiadomić o nich Organ Nadzorczy (DPA, UODO=Urząd Ochrony Danych Osobowych).

## Status Inspektora art.38

3. Inspektor musi podlegać bezpośrednio pod najwyższe kierownictwo Administratora lub procesora.

1. Administrator oraz procesor muszą zapewnić aby Inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

2. Administrator oraz procesor muszą wspierać Inspektora w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do ich realizacji oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

## Status Inspektora art.38

3. Administrator oraz procesor mają zapewnić aby Inspektor nie otrzymywał instrukcji dotyczących wykonywania swoich zadań (zapewnienie niezależności).

3. Inspektor nie będzie mógł być odwoływany ani karany za wypełnianie swoich zadań.

4. Nowością, którą wprowadza RODO będzie możliwość kontaktowania się osób, których dane dotyczą, z Inspektorem we wszystkich sprawach związanych z przetwarzaniem danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

5. Dodatkowo Inspektor jest zobowiązany do zachowania tajemnicy lub poufności, co do wykonywania swoich zadań zgodnie z prawem UE lub prawem państwa członkowskiego.

## Zadania Inspektora Ochrony Danych art.39

Art.39 1.a) Informowanie ADO, procesora oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów UE lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

1.b) Monitorowanie przestrzegania RODO, innych przepisów UE lub państw członkowskich o ochronie danych oraz polityk ADO lub procesora, w dziedzinie ochrony danych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty.

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

1.d) Współpraca z Organem Nadzorczym (DPA,GIODO).

1.e) Pełnienie punktu kontaktowego dla GIODO w kwestiach związanych z przetwarzaniem danych, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszystkich innych sprawach.

Art.38 6. Inspektor będzie mógł wykonywać również inne zadania i obowiązki. ADO lub procesor będą musieli zapewnić aby takie zadania i obowiązki nie powodowały konfliktu interesów.

## Przetwarzanie danych osobowych

**UODO art.7.2**

jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych;

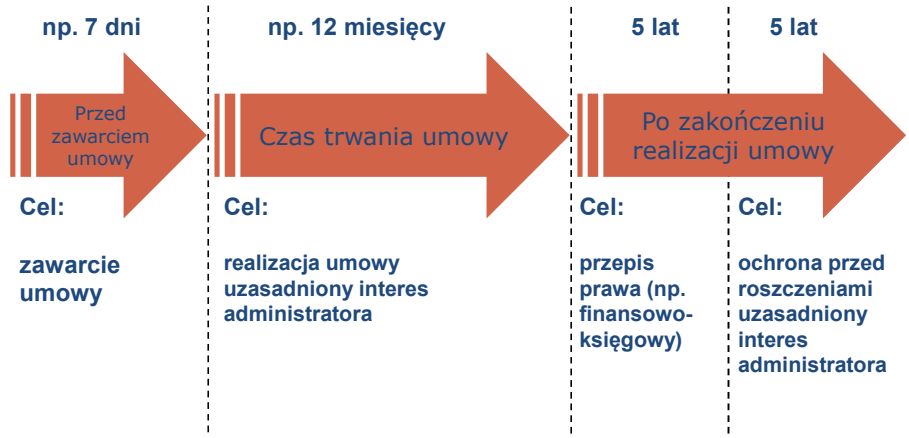
**RODO art.4.2**

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

## Zasady przetwarzania danych art. 26 UODO art. 5 RODO

1. Zasada **legalności** (zgodność z prawem, rzetelność i przejrzystość)
   *art. 26 ust. 1 pkt 1) UODO, art. 5 ust.1 a) RODO*
   *ADO musi zawsze wykazać podstawę prawną przetwarzania*
2. Zasada **celowości (**przetwarzanie zgodnie z konkretnym celem)
   *art. 26 ust. 1 pkt 2) UODO, art. 5 ust. 1 b) RODO*
   *Dane osobowe mogą być przetwarzane wyłącznie w konkretnym celu i nie poddawać ich dalszemu przetwarzaniu niezgodnemu z tym celem, a podmiot danych musi być o tym celu poinformowany*
3. Zasada **adekwatności** (minimalizacja ilości danych)
   *art. 26 ust. 1 pkt 3), art. 5 ust. 1 c) RODO*
   *Można zbierać tylko tyle danych ile jest adekwatne do realizacji celu. Nie można zbierać „na zapas" bo „może się przydadzą"*
4. Zasada **poprawności merytorycznej** (prawidłowość i aktualność)
   *art. 26 ust. 1 pkt 3), art. 5 ust. 1 d) RODO*
   *ADO musi dbać o poprawność danych i je aktualizować jak tylko podmiot danych poinformuje ADO o takiej zmianie*
5. Zasada **ograniczonego czasu** (retencja przechowywania)
   *art. 26 ust. 1 pkt 4), art. 5 ust. 1 e) RODO*
   *Można przetwarzać dane osobowe tylko tak długi jak istnieje cel*
6. **Integralność**, **poufność**, **rozliczalność** *(*§4.5 RTO, *art.5 ust.1f),2 RODO)*

## Przetwarzanie danych w czasie




**UWAGA: jeśli podmiot danych, przy zawieraniu umowy, podpisał zgodę na przetwarzanie jego danych w konkretnym celu, to pomimo zakończenia obowiązywania umowy, zgoda „biegnie" nadal – aż do odwołania !!!**

## Podstawy przetwarzania danych osobowych RODO

Art. 6 1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

## Podstawy przetwarzania danych osobowych *zmiany*

Nowe ujęcie przesłanki „usprawiedliwionego celu”

Postacie usprawiedliwionego celu (motywy nr 47-49):

- zapobieganie oszustwom
- „własny” marketing bezpośredni
- przesyłanie danych w ramach grupy kapitałowej
- bezpieczeństwo sieci

Art.6 ust.1 f) przetwarzanie jest dopuszczalne, o ile jest:

- niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią,
- z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Zmianie nie uległa sama konstrukcja tzn. można przetwarzać dane osobowe dopóki podmiot danych nie wyrazi sprzeciwu (art.21 ust.2)

## Podstawy przetwarzania danych osobowych *zmiany*

Nowa konstrukcja prawna i ogólne warunki wyrażania zgody

Art.4 pkt 11 - *„zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych*

Sposób wyrażenia zgody:

- oświadczenie woli
- wyraźne działanie potwierdzającego (zgoda „konkludentna”)
  - zaznaczenie okienka wyboru podczas przeglądania strony internetowej
  - wybór ustawień technicznych do korzystania z usług społeczeństwa informacyjnego
- milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania przez podmiot danych nie powinny oznaczać zgody (motyw nr 32)

## Podstawy przetwarzania danych osobowych *zmiany*

Nowa konstrukcja prawna i ogólne warunki wyrażania zgody

Dobrowolność wyrażenia zgody (motyw nr 42 i 43)

- zgoda nie powinna stanowić podstawy prawnej w sytuacji, w której istnieje wyraźny brak równowagi między podmiotem danych, a administratorem
- brak dobrowolności, jeżeli od zgody uzależnione jest wykonanie umowy (w tym świadczenie usługi), mimo że do jej wykonania zgoda nie jest niezbędna
- wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli podmiot danych nie może odmówić ani wycofać zgody bez negatywnych konsekwencji
- zgody nie uważa się za dobrowolną, jeżeli nie można jej wyrazić z osobna na różne operacje przetwarzania danych, mimo że w danym przypadku byłoby to stosowne

## Podstawy przetwarzania danych osobowych *zmiany*

Nowa konstrukcja prawna i ogólne warunki wyrażania zgody

Świadomość i jednoznaczność wyrażenia zgody

- osoba, której dane dotyczą musi wyrazić zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów (art.6 ust.1 a)
- w przypadku pisemnego oświadczenia składanego w innej sprawie powinny istnieć gwarancje, że osoba, której dane dotyczą, jest świadoma wyrażenia zgody oraz jej zakresu (art.7 ust.2, motyw 42)
- oświadczenie o wyrażeniu zgody powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków (motyw nr 42)
- aby wyrażenie zgody było świadome, **osoba**, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych (motyw nr 42)

## Podstawy przetwarzania danych osobowych *zmiany*

Nowa konstrukcja prawna i ogólne warunki wyrażania zgody

Oświadczenie o wyrażeniu zgody może być wyrażone pisemnie, elektronicznie lub ustnie, ale ciężar dowodu wykazania uzyskania zgody spoczywa na administratorze (art.7 ust.1)

Cofnięcie zgody (art.7 ust.3):

- osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę
- wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem; podmiot danych jest o tym informowany, zanim wyrazi zgodę.
- wycofanie zgody musi być równie łatwe jak jej wyrażenie.

## Podstawy przetwarzania danych osobowych *zmiany*

Nowe szczególne warunki wyrażenia zgody z uwagi na:

- rodzaj danych (dane wrażliwe)

**Warunki wyrażenia zgody na przetwarzanie danych wrażliwych (art.9)**

Rozszerzenie katalogu danych wrażliwych:

- dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania **danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizyczne**j lub danych dotyczących zdrowia, **seksualności** lub orientacji seksualnej tej osoby (art.9 ust.1)

Art.9 ust.2 a) – *„osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1”*

Wykładnia pojęcia „wyraźna zgoda” (*opt-in*)

- nie musi być wyrażona pisemnie (może być ustna)
- zgoda konkludentna nie wystarczy

## Prawo dostępu do danych osobowych

Nowy sposób realizacji prawa dostępu (art.15 ust.3 i 4)

- administrator dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu
- za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów.
- jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

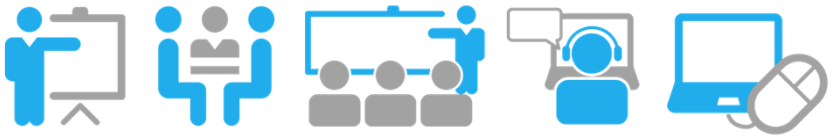
Doprecyzowanie sposobu realizacji prawa dostępu (motyw nr 63)

- jeżeli administrator przetwarza duże ilości informacji o osobie, której dane dotyczą, powinien on mieć możliwość zażądania, przed podaniem informacji, by osoba, której dane dotyczą, sprecyzowała informacje lub czynności przetwarzania, których dotyczy jej żądanie
- w miarę możliwości administrator powinien mieć możliwość udzielania zdalnego dostępu do bezpiecznego systemu, który zapewni osobie, której dane dotyczą, bezpośredni dostęp do jej danych osobowych. Prawo to nie powinno negatywnie wpływać na prawa lub wolności innych osób, w tym tajemnice handlowe lub własność intelektualną, w szczególności na prawa autorskie chroniące oprogramowanie. Względy te nie powinny jednak skutkować odmową udzielenia osobie, której dane dotyczą, jakichkolwiek informacji.

## Zapoznawanie, uświadamianie, szkolenia

- RODO art. 39 1.a) Informowanie ADO, procesora oraz pracowników, b) działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania c) Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych
- UODO Art. 36a 2. 1) c) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
- KRI § 20. 2. 6) zapewnienia szkolenia osób zaangażowanych w proces przetwarzania informacji ze szczególnym uwzględnieniem takich zagadnień, jak: a) zagrożenia bezpieczeństwa informacji, b) skutki naruszenia zasad bezpieczeństwa informacji, w tym odpowiedzialność prawna, c) stosowanie środków zapewniających bezpieczeństwo informacji, w tym urządzenia i oprogramowanie minimalizujące ryzyko błędów ludzkich;
- ISO 27001 7.2.2 Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji

## Zapoznawanie, uświadamianie, szkolenia



prezentacja warsztaty wykład film szkoleniowy e-learning

## Obowiązek informacyjny RODO art.13-14

- Pozostał podział na obowiązki informacyjne w przypadku zbierania danych bezpośrednio od podmiotu danych oraz zbierania ich w inny sposób (inni administratorzy danych, dane ogólnodostępne)
- Zachowano wyłączenie obowiązku informacyjnego, gdy podmiot danych dysponuje już tymi informacjami (art.13 ust.4 i art.14 ust.5 a)
- Rozszerzono zakres obowiązku informacyjnego w celu realizacji zasady przejrzystości (motyw nr 39 i 58):
  - wszelkie informacje i wszelkie komunikaty związane z przetwarzaniem tych danych osobowych powinny być łatwo dostępne i zrozumiałe oraz sformułowane jasnym i prostym językiem, a w stosownych przypadkach, dodatkowo wizualizowane
  - osobom fizycznym należy uświadomić ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem
  - wszelkie informacje i komunikaty, gdy przetwarzanie dotyczy dziecka, powinny być sformułowane tak jasnym i prostym językiem, by dziecko mogło je bez trudu zrozumieć.

## Obowiązek informacyjny RODO art.13-14

Znacząco zwiększono zakres informacji, które mają być przekazywane podmiotom danych, m.in. informacje o:

- podstawie prawnej przetwarzania, w tym jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – prawnie uzasadnionych interesach realizowanych przez administratora lub przez stronę trzecią
- gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej
  oraz
  o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu

## Dokumentacja systemu przetwarzania danych osobowych

Polityka, instrukcje, procedury, regulaminy na podstawie UODO i RTO

⇩

Rejestrowanie czynności przetwarzania oraz „odpowiednie” polityki RODO

## Dokumentacja systemu przetwarzania danych osobowych

- RODO art. 24.2 Obowiązki administratora,
  art. 30 Rejestrowanie czynności przetwarzania
  art. 33.5 Ewidencja naruszeń
- UODO art. 36 2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki [techn.-org. zapewniające ochronę]
  art. 36a 2. 1) b) [do zadań ABI należy] nadzorowanie (…) aktualizowania dokumentacji, o której mowa (…);
- RTO § 4 i Polityka bezpieczeństwa przetwarzania danych osobowych
  § 5 Instrukcja zarządzania systemem informatycznym służącym do przetwarzania DO
- KRI § 20 2. 1) (…) zapewnienie przez kierownictwo podmiotu publicznego warunków umożliwiających realizację i egzekwowanie (…) zapewnienia aktualizacji regulacji wewnętrznych w zakresie dotyczącym zmieniającego się otoczenia;
- ISO 27001 pkt. 7.5 Udokumentowane informacje

## Polityka bezpieczeństwa przetwarzania danych UODO

Środki techniczno-organizacyjne dla zapewnienia poufności, integralności i rozliczalności danych

Administrator danych powinien określić wykaz stosowanych w organizacji środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

Środki te (narzędzia programistyczne, procedury, umowy, dokumenty normatywne, regulacje, itp.) powinny być wdrożone i wykorzystywane zgodnie z zaleceniami, w szczególności zawartymi w Rozporządzeniu Techniczno-Organizacyjnym.

Dla każdego ze środków może zostać wskazana osoba odpowiedzialna za jego stosowanie, procedura reagowania w przypadku problemów z korzystaniem lub zaniedbań w zakresie wykorzystania środka. Zalecane jest też określenie sankcji za zaniedbania w zakresie stosowania środków niezbędnych dla ochrony danych osobowych.

Celem zabezpieczenia zbiorów danych osobowych przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne

## Dokumentacja ochrony danych osobowych UODO

Ustawa o ochronie danych osobowych

art. 36.

1. Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną {…}.

2. Administrator danych prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki, o których mowa w ust. 1.

art. 36a. 2. Do zadań ABI należy: b) nadzorowanie opracowania i aktualizowania dokumentacji, o której mowa w art. 36 ust. 2, oraz przestrzegania zasad w niej określonych,

art. 39a. Minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, sposób prowadzenia i zakres dokumentacji, o której mowa w art. 36 ust. 2, oraz podstawowe warunki techniczne i organizacyjne, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, uwzględniając zapewnienie ochrony przetwarzanych danych osobowych odpowiedniej do zagrożeń oraz kategorii danych objętych ochroną, a także wymagania w zakresie odnotowywania udostępniania danych osobowych bezpieczeństwa przetwarzanych danych.

## Dokumentacja ochrony danych osobowych UODO

**Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r (Rozporządzenie Techniczno-Organizacyjne)**

Na podstawie Rozporządzenia w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych **Administrator Danych Osobowych wdraża Politykę Bezpieczeństwa DO** prowadzoną w formie pisemnej, która zawiera w szczególności (§ 4.):

1) wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe;

2) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;

2a) wykaz systemów informatycznych wykorzystywanych do przetwarzania danych;

3) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi;

4) sposób przepływu danych pomiędzy poszczególnymi systemami;

5) wskazanie środków techniczno-organizacyjnych wykorzystywanych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

## Prowadzenie rejestru zbiorów danych UODO

§ 3. 1. W rejestrze prowadzonym przez Administratora Bezpieczeństwa Informacji znajdują się następujące informacje dotyczące każdego zbioru danych

*1) nazwa zbioru danych;*
*2) oznaczenie administratora danych i adres jego siedziby lub miejsca zamieszkania oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej, jeżeli został mu nadany;*
*3) oznaczenie przedstawiciela administratora danych, o którym mowa w art. 31a ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku wyznaczenia takiego podmiotu;*
*4) oznaczenie podmiotu, któremu powierzono przetwarzanie danych ze zbioru na podstawie art. 31 ustawy, i adres jego siedziby lub miejsca zamieszkania – w przypadku powierzenia przetwarzania danych temu podmiotowi;*
*5) podstawa prawna upoważniająca do prowadzenia zbioru danych;*
*6) cel przetwarzania danych w zbiorze;*
*7) opis kategorii osób, których dane są przetwarzane w zbiorze;*
*8) zakres danych przetwarzanych w zbiorze;*
*9) sposób zbierania danych do zbioru, w szczególności informacja, czy dane do zbioru są zbierane od osób, których dotyczą, czy z innych źródeł niż osoba, której dane dotyczą;*
*10) sposób udostępniania danych ze zbioru, w szczególności informacja, czy dane ze zbioru są udostępniane innym podmiotom niż upoważnione na podstawie przepisów prawa;*
*11) oznaczenie odbiorcy danych lub kategorii odbiorców, którym dane mogą być przekazywane;*
*12) informacja dotycząca ewentualnego przekazywania danych do państwa trzeciego.*

## RODO a zbiory danych i ich rejestry

**Od 25 maja 2018r.** przestają obowiązywać przepisy obecnej Ustawy o Ochronie Danych Osobowych, w związku z tym
**nie będzie:**
**obowiązku rejestracji zbiorów danych osobowych w GIODO**
**oraz**
**konieczności prowadzenia rejestrów przez ABI**

Przestaje być również stosowana formalna definicja „zbiór danych osobowych”

## Dokumentacja w RODO
Zadania Administratora

art. 24 1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.

2.Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

3.Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.

## Zadania Administratora (Danych)
## Rejestr czynności przetwarzania RODO art.30

1.Każdy administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada.

W rejestrze tym zamieszcza się wszystkie następujące informacje:

a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współ administratorów, 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;
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 kategorii danych;
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1.

## Zadania Procesora (Danych)
## Rejestr czynności przetwarzania RODO art.30

2.Każdy podmiot przetwarzający prowadzi 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.

## Zadania Administratora (Danych) i Procesora
## Rejestr czynności przetwarzania RODO art.30

3.Rejestry, mają formę pisemną, w tym formę elektroniczną.

4.Administrator lub podmiot przetwarzający udostępniają rejestr na żądanie organu nadzorczego.

5.Obowiązki {dot. Rej. czynności przetwarzania}, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób,

chyba że przetwarzanie, którego dokonują,

**może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą**,

nie ma charakteru sporadycznego lub

obejmuje szczególne kategorie danych osobowych (art.9) lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa (art.10)

Czyli ze względu na wątpliwości interpretacyjne oraz konieczność prowadzenia odpowiedniej dokumentacji zapewniającej rozliczalność procesów przetwarzania danych osobowych **każdy Administrator powinien prowadzić rejestr czynności przetwarzania**

## Przeznaczenie rejestru czynności przetwarzania danych

Zgodnie z Wytycznymi Grupy Roboczej Artykułu 29 – pkt 4.4:

- W każdym przypadku rejestr wymagany na mocy art. 30 winien być także postrzegany jako narzędzie pozwalające administratorowi i organowi nadzorczemu, na ich żądanie, uzyskać ogląd czynności przetwarzania danych osobowych wykonywanych w ramach organizacji.
- Jest on zatem warunkiem wstępnym uzyskania zgodności i, jako taki, skutecznym środkiem zapewnienia rozliczalności.

## Rejestr czynności przetwarzania

1. Każdy Administrator prowadzi rejestr
2. Rejestr, jako narzędzie pracy IOD/SODO, przydaje się również w kadrach gdyż porządkuje proces „dane osobowe", jest przydatny przy kontroli uprawnień i zmianach w zakresach obowiązków na stanowiskach pracy
3. Rejestr stanowi realizację obowiązku rozliczności (art. 5 us.t 2) oraz wypełnienie klauzuli generalnej art. 24 ust. 1 (obowiązki Administratora)
4. Motyw 82 wskazuje konieczność zachowania zgodności z RODO dla Administratora i podmiotu przetwarzającego –
5. Katalog informacji wymienionych w art. 30 nie jest zamknięty - stanowi minimum informacji, które powinny znaleźć się w rejestrze
6. Jeżeli zachodzi współadministrowanie danymi osobowymi, to rejestr w tych zakresach prowadzony jest wspólnie i pozwala na koordynację prac
7. Pozycja - opis kategorii osób, których dane dotyczą, oraz kategorii ich dotyczących - tutaj nie możemy pominąć fundamentalnej zasady minimalizacji danych osobowych (art. 5 ust. 1 lic. c). Określając kategorie zachowuję dychotomiczny podział (dane zwykłe i sensytywne).

## Rejestr czynności przetwarzania

8. Problematyczne okazuje się wskazanie planowanych terminów usunięcia danych osobowych (retencja danych) (należy przeanalizować po co są te dane i odnieść się do przepisów szczególnych - Prawo Pracy, Kodeks Cywilny - wierzytelności, Prawo Telekomunikacyjne, przepisy Ordynacji Podatkowej itp.). Pomocne jest posiłkowanie się np. terminem wygaśnięcia umowy, wycofania zgody, zakończenia współpracy itp.
9. Określenie środków bezpieczeństwa w rejestrze powinno być tożsame z oceną ryzyka posiadanych aktywów.
10. W umowie powierzenia danych osobowych należny zobowiązać Procesora do umożliwienia kontroli prowadzonego przez niego rejestru czynności kategorii przetwarzania oraz jego aktualizowania ze względu na art. 32 RODO 11.
11. Rejestr czynności, czy kategorii czynności przetwarzania winien być aktualizowany, szczególnie gdy decydujemy się na zmianę oprogramowania, outsourcingu, zmianę siedziby, poszerzenie zakresu naszej działalności, nawiązanie współpracy z pośrednictwem pracy, itp.
12. Należy przewidzieć procedurę aktualizacji rejestru

## Rejestr czynności przetwarzania

*Przykład czynności dla procesu Pracownik 1/2*

REKRUTACJA

- ogłoszenie - z klauzulą i prośbą o zgodę
- przyjmowanie aplikacji , także z wykorzystaniem pośredników
- analiza aplikacji i wybór osób które zostaną zaproszone na rozmowę rekrutacyjną (w tym sposób komunikowania się z kandydatami i przekazania lub nie informacji do niezakwalifikowanych)
- rozmowa rekrutacyjna (osoby uczestniczące i sposób przekazania im aplikacji/CV, protokołów/ankieta rekrutacyjna, notatki), info że poinformujemy o wynikach
- podjęcie decyzji, informacja do wybranych, zniszczenie lub archiwizacja dokumentacji z rekrutacji
- ew. szkolenie wstępne i umowa szkoleniowa (szkolenie stanowiskowe oraz z ochrony danych)
- proces przed zatrudnieniem (w tym ankieta kandydata)

ZATRUDNIENIE i ZAKOŃCZENIE PRACY

PO ZAKOŃCZENIU PRACY

- program lojalnościowy lub inicjatywy towarzyskie dla byłych pracowników, np. „klub pracownika”, „klub sympatyka”, „stowarzyszenie byłych pracowników”

## Rejestr czynności przetwarzania - przykład

https://giodo.gov.pl/pl/1520281/10449

Jak można prowadzić rejestr czynności przetwarzania danych oraz rejestr kategorii czynności?

http://blogs.dlapiper.com/privacymatters/belgium-belgian-dpa-provides-guidance-on-gdpr-article-30-publishing-template-for-records-of-processing-activities/

Belgijski organ ochrony danych osobowych (Komisja Ochrony Prywatności) opublikował wzór rejestru czynności przetwarzania danych osobowych.

Prowadzenie rejestru jest, zgodnie z art. 30 RODO, obowiązkiem administratorów danych lub podmiotów przetwarzających.

Wzór jest dostępny w języku niderlandzkim i francuskim.

wzór: https://www.privacycommission.be/nl/node/20441 ze strony
https://www.privacycommission.be/nl/model-voor-een-register-van-de-verwerkingsactiviteiten

## Rejestr czynności i kategorii przetwarzania
***przykład w pliku excell***

***ze strony GIODO***

https://giodo.gov.pl/pl/1520281/10449

## Rejestr czynności przetwarzania

*Przykład czynności dla procesu Pracownik 1/2*

**REKRUTACJA**

- ogłoszenie - z klauzulą i prośbą o zgodę
- przyjmowanie aplikacji , także z wykorzystaniem pośredników
- analiza aplikacji i wybór osób które zostaną zaproszone na rozmowę rekrutacyjną (w tym sposób komunikowania się z kandydatami i przekazania lub nie informacji do niezakwalifikowanych)
- rozmowa rekrutacyjna (osoby uczestniczące i sposób przekazania im aplikacji/CV, protokołów/ankieta rekrutacyjna, notatki), info że poinformujemy o wynikach
- podjęcie decyzji, informacja do wybranych, zniszczenie lub archiwizacja dokumentacji z rekrutacji
- ew. szkolenie wstępne i umowa szkoleniowa (szkolenie stanowiskowe oraz z ochrony danych)
- proces przed zatrudnieniem (w tym ankieta kandydata)

**ZATRUDNIENIE i ZAKOŃCZENIE PRACY**

**PO ZAKOŃCZENIU PRACY**

- program lojalnościowy lub inicjatywy towarzyskie dla byłych pracowników, np. „klub pracownika”, „klub sympatyka”, „stowarzyszenie byłych pracowników”

## Rejestr czynności przetwarzania

*Przykład czynności dla procesu Pracownik 2/2*

**ZATRUDNIENIE**

- zatrudnienie (w tym ankieta pracownika) i skierowanie na badania wstępne, szkolenie BHP, ew. szkolenie z ochrony danych, dokumenty związane z przyjęciem (oświadczenia, zgody, formularze), zlecenia związane z przyjęciem (obiegówka przyjęcia), przygotowanie stanowiska pracy, założenie kont, dostępów, przygotowanie zasobów
- rozpoczęcie pracy
- zmiany w zakresie wykonywanych obowiązków i zajmowanego stanowiska
- zaświadczenia, potwierdzenia, dokumenty wydawane pracownikowi lub uzyskiwane od pracownika
- delegacje, wyjazdy służbowe
- szkolenia
- eventy integracyjne

**ZAKOŃCZENIE PRACY**

- odejście z pracy (obiegówka odejścia)
- świadectwo pracy
- akta pracownicze (brakowanie, archiwum)

## Zabezpieczenia danych osobowych

zmiany wynikające z RODO

| Obecnie w UODO | od 25 maja 2018 w RODO |
|---|---|
| **Dobór środków zabezpieczenia technicznego i organizacyjnych w zależności od zagrożeń (ryzyka) i kategorii przetwarzanych danych osobowych** | |
| art. 36 ust. 1 UODO | art. 24 i 32 |
| **Status i zadania osoby wykonującej czynności nadzoru nad procesem ochrony DO** | |
| ABI | IOD |
| art. 36a UODO | art. 37-39 |
| **Obowiązek zgłaszania informacji o naruszeniach ochrony danych osobowych** | |
| Podmioty telekomunikacyjne | Administratorzy i procesorzy |
| UKE + GIODO + podmioty danych | DPA + podmioty danych |
| Art. 174 PT | Art. 33 i 34 |

## Zagadnienia techniczne i organizacyjne przetwarzania danych

UODO

- Dokumenty elektroniczne i ich ochrona
- Kopie zapasowe danych osobowych
- Ochrona danych i informacji przetwarzanych w systemach sieciowych
- Kontrola dostępu do danych
- Bezpieczeństwo stanowiska pracy
- Poczta elektroniczna
- Sprzęt i rozwiązania służące do przetwarzania danych osobowych
- Szyfrowanie danych
- Sieci, usługi sieciowych, dostęp do zasobów

RODO

- Nowe wymogi zabezpieczania danych osobowych

## Słowniczek dotyczący procedur IT ;-)

BCM/BCP
Business Continuity Management / Plan - zapewnienie ciągłości działania organizacji
DRP
Disaster Recovery Plan - procedury postępowania po utracie istotnych zasobów

Intranet, Extranet, Internet, PAN, LAN, MAN, WAN

kablowo czy bezprzewodowo, Ethernet, WiFI

switch, modem, access point, router, firewall

dysk, pendrive, macierz dyskowa

terminal, komputer, urządzenie przenośne, urządzenia sieciowe, sterownik

serwer: domenowy, plikowy, pocztowy, proxy, www

aplikacja/program, webserwis/serwis www, „zero, null, cienki i gruby klient”

połączenie SSL, VPN, WebVPN, OpenVPN, IPSec

## Prowadzenie dokumentacji przetwarzania danych UODO

Przykład dokumentacji na podstawie UODO i RTO

1) **Polityka bezpieczeństwa przetwarzania danych osobowych**,
2) Skrót polityki i list intencyjny w sprawie jej stosowania,
3) Dokument powołania ABI lub wyznaczenia Specjalisty ds. ochrony danych osobowych,
4) Wykaz obszarów przetwarzania danych osobowych,
5) Wykaz zbiorów danych osobowych z bazami oraz programami,
6) Wykaz systemów informatycznych wykorzystywanych do przetwarzania danych osobowych,
7) Opis struktury zbiorów danych osobowych,
8) Opis przepływu danych pomiędzy zbiorami danych osobowych,
9) Opis zastosowanych środków technicznych i organizacyjnych,
10) **Wykaz osób i systemów upoważnionych do przetwarzania danych osobowych**,
11) Wykaz umów związanych z przetwarzaniem danych osobowych,
12) Ewidencja korespondencji dotyczącej ochrony danych osobowych,
13) Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych,
14) **Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych**,
15) Opis procesu zapoznawania osób przetwarzających dane z przepisami o ochronie danych,
16) Opis techniczny systemów bezpieczeństwa na platformach hostingowych
17) Polityki prywatności i bezpieczeństwa platform hostingowych
18) Wzory dokumentów:
    a) Upoważnienie i oświadczenie dotyczące przetwarzania danych osobowych,
    b) Oświadczenie w sprawie zachowania poufności informacji,
    c) Umowa o powierzenie przetwarzania danych osobowych,
    d) Wniosek o nadanie uprawnień do przetwarzania danych osobowych.

# Polityka bezpieczeństwa przetwarzania danych osobowych

# na podstawie UODO i RTO

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.1) Obszar, w którym przetwarzane są dane osobowe

Obszar podzielono na cztery strefy, dla których obowiązują różne reguły dostępu i uprawnień do przetwarzania danych, wynikające z przydzielanych pracownikom i współpracownikom upoważnień:

1. strefa przetwarzania danych osobowych, czyli **pomieszczenia biurowe** w którym dane przetwarzane są przez ADO,
2. strefa specjalna, w skład której wchodzą **serwerownie *(IT i papieru)*** w których dane przetwarzane są przez ADO,
3. strefa w której przetwarzane są **dane osobowe powierzone przez ADO** do przetwarzania innym podmiotom, w tym w oparciu o pełnomocnictwo do dalszego powierzania przetwarzania,
4. strefa w której przetwarzane są **dane osobowe powierzone** do Przedsiębiorcy/Procesora do przetwarzania **przez innego ADO**.

Wydzielenie obszarów 3. i 4. ma na celu podział odpowiedzialności i uprawnień w zakresie przetwarzania danych powierzanych do i od ADO

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.2) Wykaz zbiorów DO ze wskazaniem programów służących do przetwarzania

Administrator Danych, bez względu na to czy powołał Administratora Bezpieczeństwa Informacji, prowadzi wykaz zbiorów, który zawierać powinien informacje o wszystkich przetwarzanych przez ADO zbiorach danych osobowych (przetwarzanych w systemach informatycznych i poza nimi).

Rodzaje zbiorów w wykazie:
- należące do ADO, przez niego przetwarzane,
- należące do ADO, powierzone do przetwarzania innym,
- należące do innego podmiotu, przetwarzane przez ADO w związku z powierzeniem mu przetwarzania danych osobowych,

- przetwarzane w systemach informatycznych,
- przetwarzane bez wykorzystywania systemów informatycznych,

- zawierające dane zwykłe,
- zawierające dane wrażliwe,

- przetwarzane na terytorium EOG,
- przetwarzane w państwach trzecich.

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.2) Wykaz zbiorów DO ze wskazaniem programów służących do przetwarzania

Mimo że przepisy nie stawiają takiego wymogu warto prowadzić również

„**Wykaz systemów informatycznych wykorzystywanych do przetwarzania danych osobowych**”

w którym, na zlecenie ADO, osoby odpowiedzialne za IT powinny prowadzić aktualną dokumentację przetwarzania informacji wykorzystaniem aplikacji, narzędzi i systemów komputerowych.

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.3) Opis struktury zbiorów

Nazwa zbioru

Opis aplikacji:
Dane w zbiorze przetwarzane są z wykorzystaniem aplikacji: …

Wykaz przetwarzanych danych osobowych:
W zbiorze przetwarzane są następujące kategorie i typy danych osobowych: …

Opis bazy danych
Dane przechowywane są w bazie danych aplikacji …

Struktura bazy danych
Dane znajdują się w tabelach … w bazie …

Miejsce przetwarzania danych
Bazy działają na … serwerach, a ich kopie znajdują się na … serwerach zapasowych umieszczonych w …

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.4) Opis przepływów danych pomiędzy systemami

Opis relacji pomiędzy rekordami danych w zbiorach

Zalecenia:
- podział na dane źródłowe i wtórne,
- oznaczenie miejsca wprowadzania danych,
- określenie uprawnień w dostępie do danych,
- wskazanie aplikacji przetwarzających dane,
- specyfikacja interfejsów komunikacyjnych (np. API, DBaccess, …)

## Prowadzenie przez ADO dokumentacji przetwarzania danych

RTO § 4.4) Opis przepływów danych pomiędzy systemami - przykład

| rodzaj danych | dane | Macierz przepływów danych między aplikacjami | | | | |
|---|---|---|---|---|---|---|
| | | FK | Kadry | ERP | CRM | Płatnik |
| Dane osobowe | Imię | 1 | 1 | 2 | 0 | 2 |
| | Nazwisko | 1 | 1 | 2 | 0 | 2 |
| | Data urodzenia | 1 | 0 | | | 2 |
| | PESEL | 1 | 0 | 2 | | 2 |
| | zdjęcie | | 0 | | 1 | |
| Dane zamieszkania | Miejscowość | | 1 | | 0 | 2 |
| | Ulica nr domu nr lokalu | | 0 | | | 2 |
| | Kod pocztowy | | 0 | | | 2 |
| | Poczta | | 0 | | | 2 |
| | Województwo | | 0 | | | 2 |
| | Powiat | | 0 | | | 2 |
| | Gmina | | 0 | | | 2 |
| | Konto pocztowe | | 1 | | 0 | |
| | Tel. służbowy | | 0 | | | |

## Zadania Administratora
## Prowadzenie dokumentacji w RODO art.24

Art. 24 *1. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.*

2.Jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

*3.Stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.*

## Analiza ryzyka

- RODO Art. 25 Uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych, Art. 35 Ocena skutków dla ochrony danych, Art. 36 Uprzednie konsultacje
- UODO Art. 36. 1. Administrator danych jest obowiązany **zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną**, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
- KRI § 20. 2. 3) Zarządzanie bezpieczeństwem informacji realizowane jest w szczególności przez (…) przeprowadzanie okresowych analiz ryzyka utraty integralności, dostępności lub poufności informacji oraz podejmowanie działań minimalizujących to ryzyko, stosownie do wyników przeprowadzonej analizy;
- PN-EN ISO IEC 27001:2014-12 pkt. 6 Planowanie i pkt. 8 Działania operacyjne

## Analiza ryzyka RODO art.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.

## Analiza ryzyka w RODO wymagania art. 32

Art. 32 ust. 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

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.

## Analiza ryzyka RODO art.32

**Bezpieczeństwo przetwarzania**

2. 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.

3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

## Analiza ryzyka

Opisz, udokumentuj dla każdego rozpoznanego ryzyka:

- Źródło ryzyka (Występuje z powodu…)
- Ryzyko (Istnieje zagrożenie, że…)
- Potencjalne skutki (W związku z ryzykiem może …)
- Istniejące środki bezpieczeństwa (Stosujemy …)
- Poziom prawdopodobieństwa i wpływ skutków przy obecnych środkach bezpieczeństwa (ocena)
- Rekomendowane środki mitygacji ryzyka (porada)
- Poziom prawdopodobieństwa i wpływ skutków po zastosowaniu rekomendowanych środków (może się zdarzyć)

Dobierz odpowiednie środki zaradcze, opierając się na ocenie skuteczności poszczególnych rozwiązań. Wybierz te, które są najbardziej korzystne dla podmiotów danych, projektu i administratora danych.

## Analiza ryzyka w RODO
## Jak wykorzystać doświadczenia?

- Ustalenie kontekstu (RODO: ochrona praw i wolności osób)
- Identyfikowanie ryzyka
  - Identyfikacja aktywów (określenie ich wartości)
  - Identyfikacja zagrożeń
  - Identyfikacja podatności
  - Identyfikacja zabezpieczeń
  - Identyfikowanie następstw
- Analiza ryzyka
  - Szacowanie następstw (skutków ewentualnych naruszeń)
  - Szacowanie prawdopodobieństwa naruszeń
  - Ocena ryzyka
- Postępowanie z ryzykiem
- Monitorowanie ryzyka

## Analiza ryzyka w RODO
## Identyfikacja aktywów

Aktywa to wszystko, co ma wartość dla organizacji i z tego względu wymaga ochrony.

- Dane osobowe i informacje o zabezpieczeniach
- Procesy / usługi
- Sprzęt, oprogramowanie, nośniki danych i sieć
- Systemy służące do przetwarzania danych i zabezpieczenia
- Personel
- Siedziba

- Środki finansowe
- Reputacja / wizerunek organizacji
- Prawa i wolności osób, których dane są przetwarzane

## Analiza ryzyka w RODO
## Identyfikacja zagrożeń

Zagrożenia mają swoje źródła: naturalne lub ludzkie, przypadkowe lub umyślne (atrakcyjność aktywów, zatarg), wewnętrzne lub zewnętrzne

- Nieautoryzowane lub nieprawidłowe działanie
  - Kradzież informacji lub urządzenia
    - Dokonana przez pracownika
    - Włamanie (do siedziby lub hackerskie)
  - Szpiegostwo / podsłuch
  - Błąd administratora systemu lub lekkomyślność
- Terroryzm (atak bezpośredni lub cyberprzestępczość)
- Zniszczenia fizyczne (np. pożar, korozja, zanieczyszczenie, wypadek)
- Awaria techniczna (np. elementu systemu lub utrata dostaw prądu)
- Zjawiska naturalne (np. pogodowe lub klimatyczne)

Norma ISO 27005
załącznik C

## Analiza ryzyka w RODO
## Identyfikacja podatności

Podatność aktywów na zagrożenia identyfikuje się w następujących obszarach:

- Organizacja (np. brak przypisania odpowiedzialności, procedur, umów o zachowania poufności, planów ciągłości działania itp.),
- Procesy i procedury (np. brak stosowania, niejednoznaczność),
- Personel (np. brak szkoleń, nieobecność, sytuacja rodzinna),
- Konfiguracja systemów (np. błędy w uprawnieniach dostępu),
- Sprzęt (np. brak kontroli zmian lub kontroli dostępu),
- Oprogramowanie (np. znane luki, brak kodu lub dokumentacji, skomplikowany interfejs, brak uwierzytelniania),
- Urządzenia telekomunikacyjne (np. brak kontroli ruchu),
- Zależność od dostawców zewnętrznych (np. przerwanie dostaw),
- Siedziba (np. brak fizycznej ochrony, lokalizacja).

## Analiza ryzyka w RODO
## Identyfikacja zabezpieczeń

Zabezpieczenia mogą zmniejszać zarówno prawdopodobieństwo wystąpienia negatywnego zdarzenia, jak i jego skutek:

- Przeszkolenie pracowników może zwiększyć ich świadomość i zmniejszyć prawdopodobieństwo lekkomyślnych zachowań lub zminimalizować liczbę błędów przy obsłudze systemów;
- Redundancja urządzeń zmniejsza skutki ich awarii;
- Monitoring i ochrona może działać zarówno prewencyjnie, jak i reakcyjnie.

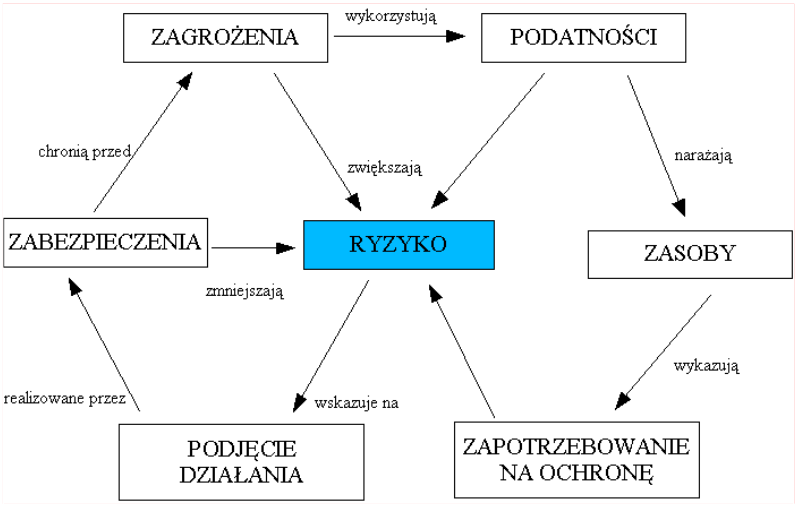
Istnienie zabezpieczeń wpływa na wartość ryzyka, zatem ich nieuwzględnienie spowoduje jego przeszacowanie i może doprowadzić do duplikacji zabezpieczeń.

Istotna jest też wiedza nt. skuteczności zabezpieczenia – wdrożony nieskutecznie mechanizm sam może powodować podatność.

## Analiza ryzyka
## Identyfikowanie następstw (skutków)

| Zagrożenia<br>**Aktywa** | Nieautoryzowane działanie (Z1) | Awaria techniczna (Z2) | Katastrofa naturalna (Z3) |
|---|---|---|---|
| Baza marketingowa (A1) | Podatność na szantaż -> Wyciek danych (kradzież) | Brak sprzętu zapasowego -> Niedostępność | Brak kopii zapasowej -> Utrata danych |
| System kadrowy (A2) | Pomieszczenie zamykane -> Brak podatności | Procedury awaryjne -> Brak podatności | Brak zastępstwa kadrowej -> Proces zaburzony |
| Serwer bazodanowy (A3) | Niezamykana serwerownia -> Zniszczenie danych | Serwer zapasowy -> Brak podatności | Nieprzetestowane procedury awaryjne -> Chaos |
| Usługi internetowe dla klientów (A4) | Błędy w konfiguracji firewall'a -> Wyciek danych (haker) | Komunikat o awarii -> Chwilowa niedostępność | Brak środowiska zapasowego -> Niedostępność |

## Ryzyko i relacje



## Zarządzanie ryzykiem w ochronie danych osobowych
## Postępowanie z ryzykiem

- Unikanie ryzyka
- Podejmowanie ryzyka w celu wykorzystania okazji
- Usuwanie źródeł
- Zabezpieczenia – zmniejszanie prawdopodobieństwa lub konsekwencji
- Podzielenie (transfer) ryzyka z trzecią stroną
- Retencja ryzyka

Uwaga: Postępowanie z ryzykiem może powodować powstanie nowych ryzyk

# Instrukcja zarządzania systemem informatycznym

# na podstawie UODO i RTO

## Środki techniczno-organizacyjne dla zapewnienia poufności, integralności i rozliczalności danych osobowych

Administrator danych powinien określić wykaz stosowanych w organizacji środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych.

Środki te (narzędzia programistyczne, procedury, umowy, dokumenty normatywne, regulacje, itp.) powinny być wdrożone i wykorzystywane zgodnie z zaleceniami, w szczególności zawartymi w Rozporządzeniu Techniczno-Organizacyjnym. Dla każdego ze środków może zostać wskazana osoba odpowiedzialna za jego stosowanie, procedura reagowania w przypadku problemów z korzystaniem lub zaniedbań w zakresie wykorzystania środka. Zalecane jest też określenie sankcji za zaniedbania w zakresie stosowania środków niezbędnych dla ochrony danych osobowych.

Celem zabezpieczenia zbiorów danych osobowych przed dostępem osób nieupoważnionych wprowadza się odpowiednie rozwiązania techniczne i organizacyjne

## Prowadzenie przez ADO dokumentacji przetwarzania danych

§ 4.5) Instrukcja zarządzania systemem informatycznym

W § 5 RTO podane są najważniejsze elementy Instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych.
Należy w niej opisać:

1. procedury nadawania i rejestracji uprawnień do przetwarzania danych w systemach, wskazując osobę odpowiedzialną za ten proces – najczęściej zajmuje się tym, pod nadzorem ABI, Administrator Systemów Informatycznych (ASI) lub osoba odpowiedzialna za IT,
2. obowiązujące metody i środki zarządzania procesem uwierzytelnienia operatorów,
3. zasady rozpoczęcia, zawieszenia i zakończenia pracy przez operatorów danych,
4. mechanizmy tworzenia kopii zapasowych ze wskazaniem procedur i narzędzi,
5. sposób, miejsce i okres przechowywania nośników zawierających dane oraz kopie,
6. sposób zabezpieczenia systemów przed oprogramowaniem, którego celem może być uzyskanie nieuprawnionego dostępu do danych,
7. sposób realizacji wymogów, związanych z odnotowaniem udostępniania danych,
8. procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych.

Powyższe procesy powinny uzyskać przed wdrożeniem akceptację Administratora Danych.

## Bezpieczeństwo teleinformatyczne

analiza ryzyka, atrybuty informacji

W systemach teleinformatycznych wprowadza się zabezpieczenia techniczno-organizacyjne zapewniające:

- Poufność informacji (ang. ***C**onfidentality*)
  Dostęp do informacji dla uprawnionych użytkowników
- Integralność (ang. ***I**ntegrity*)
  Informacja jest w postaci oryginalnej, niezmienionej
- Dostępność (ang. ***A**vailability*)
  Informacja jest dostępna dla uprawnionych użytkowników kiedy jej potrzebują

- Rozliczalność (ang. *Accountability*)
  Możliwość jednoznacznej identyfikacji osoby uzyskującego dostęp do informacji
- Autentyczność (ang. *Authenticity*)
  pochodzenie informacji jest takie jak deklarowana
- Niezawodność (ang. *Reliability*)
  zachowanie (działanie systemu) i skutki działania są poprawne, takie jak zamierzone

## Postępowanie z nośnikami danych

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

- ISO 27002 pkt. 8.3 Postępowanie z nośnikami

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

## Postępowanie z dokumentami elektronicznymi

Nośniki elektroniczne zawierające dane osobowe:

- dyski oraz korespondencję zawierająca istotne informacje **należy szyfrować**
- dokumenty oraz nośniki należy **przechowywać w sposób bezpieczny**
- przeznaczone do likwidacji, jeśli nie podlegają procedurom archiwizacyjnym, **pozbawia się wcześniej zapisu informacji**, a gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający odczytanie
- przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymania informacji, **pozbawia się wcześniej zapisu tych danych**
- przeznaczone do naprawy **pozbawia się przed naprawą zapisu informacji lub naprawia się ja pod nadzorem osoby upoważnionej**

## Dokumenty elektroniczne i ich ochrona

systemy DLP

Jednym z rozwiązań, które pozwala na pełną, zautomatyzowaną kontrolę dokumentów elektronicznych jest zastosowanie systemów **DLP (Data Leak/Leakage/LossProtection/ Prevention)**, które nadzorują większość dostępnych operacji, które można wykonać z dokumentem.

Systemy DLP wdraża się tam, gdzie ujawnienie lub nieuprawniona modyfikacja może narazić podmiot na odpowiedzialność karną lub cywilną.

Systemy DLP mogą wykorzystywać wiele technik kontroli przetwarzania danych:

- **wykrywanie danych** wrażliwych i według wzorca,
- **klasyfikację** i przypisanie wag plikom w lokalnym systemie na podstawie zawartości,
- **kontrolowanie przesyłania dokumentów** przez sieć lub zapisywania ich na nośniki,
- **blokowanie zapisu** na nośniki zewnętrzne,
- **transparentne szyfrowanie i deszyfrowanie wrażliwych dokumentów** tak, by nigdy nie opuszczały one organizacji w formie niezaszyfrowanej

## Sprzęt służący do przetwarzania danych osobowych

**Komputery PC i notebooki** służące do przetwarzania danych osobowych
- dane przechowywać na serwerach sieci lokalnej, a lokalnie szyfrować
- dostęp do komputera zabezpieczyć hasłem i stosować automatyczny wygaszacz ekranu
- nie zezwalać na używanie komputera osobom nieupoważnionym
- stosować oprogramowanie antywirusowe i chroniące spójność danych
- instalować i użytkować oprogramowanie zgodnie z licencjami

Korzystając z dostępu VPN pracownik odpowiada za ochronę komputera

Użytkując przenośny komputer należy zachować szczególną ostrożność podczas transportu i przechowywania tego komputera

## Serwery

**Serwery**
- Należy je zabezpieczyć przed utratą danych osobowych z powodu awarii zasilania lub zakłóceń w sieci zasilającej
- Zabezpieczamy zarówno urządzenia jak i całe systemy informatyczne

**Różnorodność**
- druku i wydruku – drukarki, skanery, kserokopiarki
- plikowe / „dyski sieciowe” – czy zawsze na serwerze ?
- nazewnictwo urządzeń
- kopie zapasowe
- Uprawnienia dostępu dla:
  - Użytkowników (aplikacje, ale czy tylko ?)
  - Administratorów
  - Serwisu technicznego
- Czy wszystko jest u nas ?
  - A może coś kolokujemy ?
  - Czy tylko kolokujemy ?
  - A co robimy dla innych ?

## Sprzęt służący do przetwarzania danych osobowych

Wygaszacze ekranu, osobisty firewall i kontrola transmisji na interfejsach

Nośniki informacji oraz wydruki z danymi osobowymi, które nie są przeznaczone do udostępnienia, **przechowuje się w warunkach uniemożliwiających dostęp do nich osobom niepowołanym**.

Jeżeli istnieją odpowiednie możliwości techniczne, **ekrany stanowisk** dostępu do danych osobowych **powinny być automatycznie wyłączane** po upływie ustalonego czasu nieaktywności **(wygaszacze) a ponowne włączenie powinno nastąpić po podaniu hasła użytkownika**.

W pomieszczeniach, gdzie przebywają osoby postronne, monitory stanowisk dostępu do danych osobowych powinny być ustawione w taki sposób, by uniemożliwić tym osobom wgląd w dane.

Aby ograniczyć i kontrolować dostęp do komputerów od strony sieci LAN zalecane jest skonfigurowanie osobistych zapór na wszystkich interfejsach sieciowych (Ethernet, WiFi, Bluetooth, modemy telefoniczne …), a interfejsy niewykorzystywane powinny zostać wyłączone.

## Usuwanie danych osobowych

**UODO art.7.3**

Anonimizacja - zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

**RODO art.17.1**

Prawo do usunięcia danych, „prawo do bycia zapomnianym”
1.Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności: {…}

## Anonimizacja

- Anonimizacja danych to przekształcenie danych osobowych, po którym nie można(w rozsądnym wymiarze czasowym) już przyporządkować poszczególnych informacji osobistych lub rzeczowych określonej lub możliwej do zidentyfikowania osobie fizycznej
- Proces anonimizacji musi być trwały i nieodwracalny

- 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).

- Zasady ochrony danych nie powinny 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.

RODO nie dotyczy więc przetwarzania takich anonimowych informacji, w tym przetwarzania do celów statystycznych lub naukowych. (motyw 26)

## Pseudonimizacja
dodatkowa ochrona danych osobowych

**RODO art. 4.5**

- przetworzenie danych osobowych w taki sposób,
- by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji,
- pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej"

Pseudonimizacja danych osobowych może ograniczyć ryzyko dla osób, których dane dotyczą, oraz pomóc administratorom i podmiotom przetwarzającym wywiązać się z obowiązku ochrony danych„ (motyw nr 28)

## Pseudonimizacja
dodatkowa ochrona danych osobowych

## Dane pseudonimizowane (pseudonimy) jako nowy rodzaj danych osobowych

- **Psuedonimizacja to środek zwiększający bezpieczeństwo przetwarzania** danych osobowych. Zastosowanie tego zabezpieczenia będzie powinno wynikać z **analizy ryzyka** dla systemu informatycznego uwzględniającej ryzyko naruszenia praw i wolności osoby fizycznej.
- Pseudonimizacja to proces **odwracalny**, który polega na zastąpieniu jednego atrybutu innym atrybutem, co nadal umożliwia wyodrębnienie konkretnej osoby fizycznej i tworzenie w odniesieniu do tej osoby powiązań między różnymi zbiorami.
- Pseudonimizacja skutecznie podwyższa bezpieczeństwo przetwarzania danych, poprzez ograniczenie możliwość tworzenia powiązań zbioru danych z prawdziwą tożsamością osoby, której dane dotyczą. Nie jest to jednak równoznaczne z anonimizacją, w związku z czym te dane **dalej podlegają przepisom o ochronie danych osobowych.**

## Dane pseudonimizowane (pseudonimy) jako nowy rodzaj danych osobowych

RODO przewiduje następujące korzyści związane z pseudonimizacją:

- pseudonimizacja stanowi **techniczny środek ochrony danych** w fazie projektowania oraz domyślnej ochrony danych (art.25 ust.1),
- w razie wdrożenia odpowiednich zabezpieczeń, w tym ew. szyfrowania lub pseudonimizacji oraz pod warunkiem spełnienia pozostałych wymogów przewidzianych przez art. 6 ust. 4 RODO, dane osobowe mogą być przetwarzane **w celu innym niż cel, dla którego dane osobowe zostały zebrane,**
- pseudonimizacja jest istotnym zabezpieczeniem w razie przetwarzania danych osobowych do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych (Art. 89 ust. 1 RODO),
- szansa na **uniknięcie, w przypadku naruszenia ochrony danych osobowych, powiadomienia**:
  - organu nadzorczego (art. 33 ust. 1 RODO),
  - podmiotu danych (art. 34 ust. 1 RODO)

## Dane pseudonimizowane (pseudonimy) jako nowy rodzaj danych osobowych

**Znane techniki pseudonimizacji to:**

- Szyfrowanie z kluczem tajnym – dobry klucz daje dużą gwarancję bezpieczeństwa, jednak administrator może odszyfrować dane.
- Funkcja skrótu – dla każdej wartości dodaje się stałej wielkości wynik, którego nie można odwrócić (często stosowana do przechowywania haseł). Technika podatna na złamanie atakiem siłowym przy znajomości treści podlegającej funkcji skrótu, np. próba pozyskania nieautoryzowanego dostępu poprzez wielokrotne (nawet do kilkudziesięciu tysięcy prób) sprawdzanie wszelkich możliwych kombinacji hasła.
- Funkcja skrótu z dodaniem losowego ciągu znaków (ang. salt) ogranicza prawdopodobieństwo uzyskania wartości treści lub odczytania zasobu.
- Funkcja skrótu z dodanym kluczem, który jest przechowywany – łatwiejsze odzyskanie treści lub odczytania zasobu 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.

## Dane pseudonimizowane (pseudonimy) jako nowy rodzaj danych osobowych

- **Zalecenia:**
  - Należy na bieżąco **śledzić obowiązujące standardy** stosowanych technik anonimizacji i pseudonimizacji. Warto wziąć pod uwagę zastosowanie nowych technik lub podjąć odpowiednie działania w przypadku odkrycia nowych podatności,
  - **Nie należy traktować pseudonimizacji jako równoważną z anonimizacją**. Anonimizacja jest nieodwracalna, a pseudonimizacja jest procesem możliwym do odwrócenia z wykorzystaniem dodatkowych informacji (np. tabeli przyporządkowań, kluczy szyfrujących, danych źródłowych itp.)
  - Dane poddane pseudonimizacji **po usunięciu informacji pozwalającej na przyporządkowanie osoby fizycznej** (np. wiersza tabeli przyporządkowań, kluczy szyfrujących, danych źródłowych itp.) w szczególnych przypadkach i po analizie można traktować jako zanonimizowane.

## Różnica pomiędzy anonimizacją i pseudonimizacją

Anonimizacja bezpowrotnie usuwa dane

W przypadku pseudonimizacji istnieje możliwość, przy użyciu „wszelkich rozsądnie możliwych sposobów", reidentyfikacji danych osobowych, czyli przywrócenie ich treści z pseudonimu

**Dane spseudonimizowane uważane są za dane osobowe**

## Kopie zapasowe

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

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

## Kopie zapasowe w UODO

obowiązki w Rozporządzeniu Techniczno-Organizacyjnym

Załącznik do RTO, rozdział A - Środki bezpieczeństwa na poziomie podstawowym

Par. III

System informatyczny służący do przetwarzania danych osobowych zabezpiecza się, w szczególności przed:

2. utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.

Par. IV

3. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych **zbiorów danych** oraz **programów** służących do przetwarzania danych.

4. Kopie zapasowe:

a) przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem;

b) usuwa się niezwłocznie po ustaniu ich użyteczności

## Backup vs archiwizacja danych

Określenia „backup" i „archiwizacja" są, często błędnie, stosowane zamiennie. Angielskim „backup" i „data archiving" określają różne działania, tłumaczone jako „kopia bezpieczeństwa" i „archiwizacja danych".

„**Backup**" to tworzenie kopii bezpieczeństwa/zapasowej danych w celu ich odtworzenia po utracie lub uszkodzeniu.

„**Archiwizacja**" oznacza proces tzw. specjalizacji danych, czyli ich podziału na dane operacyjne (aktywne), historyczne (nieaktywne) i referencyjne, a następnie zapisywanie ich w odpowiednich obszarach systemów archiwizacyjnych lub produkcyjnych. Dostęp do tak sklasyfikowanych danych można zróżnicować w systemach IT, np. dane transakcyjne będą miały krótki (szybki), a dane historyczne długi czas dostępu, co ma swoje uzasadnienie np. biznesowe lub organizacyjne.

## Reguła 3-2-1 (zasady poprawnego backupu danych) 1/3

**Zasada 3**
**W trzech kopiach (oryginał i dwie kopie zapasowe** na różnych nośnikach**)** należy przechowywać dane. Doświadczony administrator przechowuje dane na serwerze, na dysku zewnętrznym i w innym systemie, aby zminimalizować skutki usterki nośnika oraz przyspieszyć proces odzyskiwania danych

Prawdopodobieństwo awarii dwóch nośników jest większe niż prawdopodobieństwo awarii trzech nośników jednocześnie …

Brak drugiej kopii, w wypadku awarii nośnika z backupem, powoduje że system pozostaje bez zabezpieczenia. Dodatkowa kopia daje komfort i czas na wykonanie kolejnej kopii, a zarazem znacząco zmniejsza ryzyko utraty danych.

## Reguła 3-2-1 (zasady poprawnego backupu danych) 2/3

**Zasada 2**

**Kopie należy przechowywać na dwóch różnych nośnikach.**

Backup nie spełnia wymogów bezpieczeństwa, jeśli wszystkie kopie przechowywane są na jednym dysku twardym, gdyż w przypadku awarii nośnika utracone zostaną wszystkie dane.

Zaleca się rozszerzenie wymogów bezpieczeństwa a zarazem użyteczności przez przechowywanie kopii na dwóch nośnikach różnych typów, na przykład na dysku zewnętrznym i płycie DVD (na wypadek usterki interfejsu lub urządzenia albo niedostępności czytnika CD/DVD), lub na dysku lokalnym i w chmurze, by mieć do danych dostęp z dowolnego miejsca, także spoza organizacji albo w przypadku problemów z działaniem sprzętu lub np. z zasilaniem systemów backupowych.

## Reguła 3-2-1 (zasady poprawnego backupu danych) 3/3

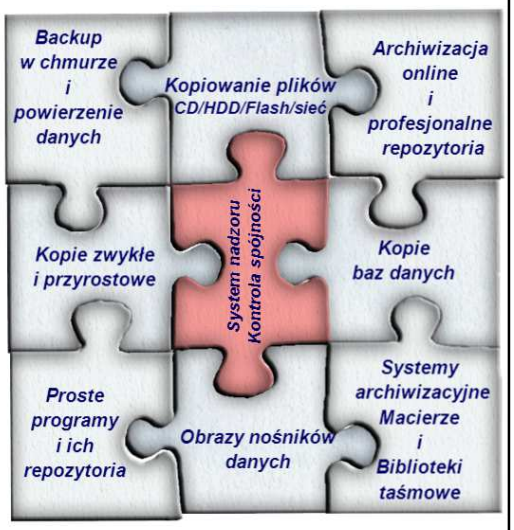
**Zasada 1**

**Jedna kopia powinna być przechowywana w innej lokalizacji**, aby zabezpieczyć dane na wypadek pożaru, kradzieży komputera/serwera lub fizycznych nośników.

Można rozważyć przechowywanie kopii w formie depozytu offline nośników danych, do którego dostęp ograniczono proceduralnie, a odczyt danych byłby możliwy po podłączeniu nośników do urządzeń w systemie informatycznym administratora danych lub w innym, odpowiednio przygotowanym, systemie zapasowym.

## Kompleksowe rozwiązania archiwizacyjne
co powinno znaleźć się w kopiach zapasowych

Gdzie dane są przechowywane ?
Jak są chronione ?
Optymalnie inwestycje
Poszukiwać rozwiązań alternatywny




W archiwach przechowywane są:
- Dane
- Binaria programów
- Wersje instalacyjne
- Dane konfiguracyjne
- Pliki konfiguracyjne serwerów
- Konfiguracja pamięci masowych
- Pliki konfiguracyjne urządzeń sie
- Instrukcje
- Procedury postępowania

## Kompleksowe rozwiązania archiwizacyjne
o czym nie powinno się zapominać

- BACKUP
  czyli zabezpieczamy dane
- RESTORE
  czyli odzyskujemy dane
- CONTROL
  czyli sprawdzamy czy to działa

Problemy, błędy:
- Najwięksi architekci zapominają o uwzględnieniu w projektach kopii zapasowych
- Kopie zapasowe przechowywane są razem z oryginałami
- Jedni backupy wykonują, inni będą wykonywać, niektórzy sprawdzają czy to działa
- Wielu administratorów bezgranicznie wierzy brakom błędów w logach
- Regularna kontrola funkcjonowania mechanizmów to nieuzasadnione wydatki

## Kontrola dostępu do danych

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

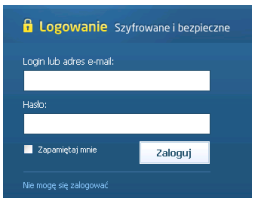
## Jak sprawdzić użytkownika i jego uprawnienia

Ważna jest weryfikacja osób pragnących skorzystać z systemu
**Model AAA+**
**A**utentykacja, **A**utoryzacja, **A**ccounting + **A**uditing
Kto ?, Do czego jest uprawniony ?, Co zrobił ? + Kontrola

Weryfikacja może się odbywać w oparciu o trzy rodzaje kryteriów:
- *„coś, co masz”* klucze, karty magnetyczne lub chipowe, tokeny,
- *„coś, co wiesz”* PIN, hasła, poufne dane
- *„kim jesteś”* metody biometryczne

Problem „kopert z hasłami” – są przydatne, gdy zawiedzie człowiek

## Identyfikacja „coś co wiesz” i „coś co masz”




Logowanie

Tokeny


Sprawdzanie kart magnetycznych lub chipowych

## Identyfikacja „kim jesteś” - biometria

## Uwierzytelnienie użytkownika w UODO

reguły zarządzania hasłami użytkowników na podstawie RTO

- Hasło każdego użytkownika musi być zmieniane raz na miesiąc
- Długość hasła to co najmniej 8 znaków
- Hasło zawiera małe i wielkie litery oraz cyfry lub znaki specjalne
  Rozporządzenie MSWiA (Dz. U. z 2004 r. Nr 100, poz. 1024, załącznik A, paragraf VIII w związku IV, pozycja 2)
- Hasła nie mogą się powtarzać w cyklach czterech zmian
- Treść hasła kontrolowana jest w sposób automatyczny (aby wyeliminować hasła trywialne i powtarzające się)
- Hasła, umożliwiające dostęp do systemu informatycznego, utrzymuje się w tajemnicy, również po upływie ich ważności
- Każda osoba ma odrębny identyfikator i hasło,

**Czy w RODO z tego zrezygnujemy,**
**czy tylko zmodyfikujemy i zoptymalizujemy zasady ?**

## Polityka haseł - przykład

A. hasła administratorów do systemów i serwerów o znaczeniu strategicznym
B. hasła do laptopów/desktopów administratorów i użytkowników HelpDesk (użytkownicy zaawansowani)
C. hasła użytkowników domeny (desktopy, email) „konta zwykłe”
D. hasła do urządzeń mobilnych (pendrive, blackberry itp.)

| | | Kategoria | | | |
|---|---|---|---|---|---|
| Parametr jakości hasła | | A | B | C | D |
| Ilość znaków | | 14 | 12 | 8 | 4 |
| Wymagane znaki | Duże litery | 2 | 2 | 1 | |
| | Cyfry | 2 | 2 | 1 | |
| | Specjalne (?><{}][*&^%$#@!) | 4 | 2 | 1 | |
| Ważność [dni] max. (dane osobowe) | | 60 (30) | 60 (30) | 60 (30) | |

dopuszczalny czas pomiędzy zmianami: 3 dni;
system pamięta 10 haseł;
kontrola pomyłek i prób złamania

## Hasła dostępu do zasobów teleinformatycznych

Skoro hasło ma nas ochronić, to jakie hasła stosować ?


Codzienna higiena komputera

E-hasła są jak majtki ;-)

Trzeba je często zmieniać,
nie zostawiać na widoku
i nie pożyczać obcym.

cytat z **niebezpiecznik.pl**

## Uwierzytelnienie użytkownika

jak stworzyć i zapamiętać „mocne" hasło – dla użytkownika lub do szyfrowania danych

Hasła nietrywialne,

często zmieniane,

niezapisywane

***PKdG,dG.AKzn,jzmp...***

***JdnWZbd,TdnWdGpw.***

## Uwierzytelnienie użytkownika

jak stworzyć i zapamiętać „mocne" hasło – dla użytkownika lub do szyfrowania danych

Hasła nietrywialne,

często zmieniane,

niezapisywane

***PKdG,dG.AKzn,jzmp...***

***Poszła Karolinka do Gogolina, do Gogolina.***
***A Karliczek za nią, jak za młodą panią ...***

***JdnWZbd,TdnWdGpw.***

***Ja długo na Wawelu Zygmunta bije dzwon,***
***Tak długo nasza Wisła do Gdańska płynie wciąż.***

***Mnemotechnika - pierwsze litery/cyfry i znaki interpunkcyjne***

## Poczta elektroniczna

dobre praktyki

- Zasada działania poczty elektronicznej, przekazywanie informacji, ze szczególnym uwzględnieniem konfiguracji serwerów i stosowania w nich **szyfrowania transmisji**
- Zabezpieczanie treści przesyłek, także przez stosowanie mechanizmów **szyfrowania załączników**
- **Zasady** dotyczące obsługi załączników, w tym ich **szyfrowanie oraz sposoby wymiany haseł**
- **Korzystanie z treści aktywnych i odsyłaczy (linków) do zasobów, czyli higiena internetowego stanowiska pracy oraz rozsądek i czujność operatorów**

## Bezpieczeństwo sprzętu i aktywów poza siedzibą

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

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

## Urządzenia mobilne

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

*Realizacja – wykaz urządzeń mobilnych; szyfrowanie dysków; zasady zdalnego dostępu*

## Nadzór nad urządzeniami przenośnymi

Usuwanie przechowywanej informacji w przypadku utraty lub nieużywania urządzenia

Dużą popularność, oprócz komputerów przenośnym, zdobywają urządzenia spełniające funkcje „biurowe", w tym urządzenia prywatne użytkowników (**B**ring **Y**our **O**wn **D**evice)

Ze względu na utrudnione zarządzanie i brak możliwości stałego nadzoru zalecane jest aby urządzenia przenośne zostały skonfigurowane tak, aby w przypadku utraty urządzenia nie doszło do:

- naruszenia integralności danych służbowych
- utraty danych osobowych lub innych informacji przetwarzanych na komputerze
- zagrożenia nieuprawnionego dostępu do danych
- narażenia użytkownika na kradzież tożsamości i podszywanie się innej osoby

Zalecane jest stosowanie oprogramowania umożliwiającego automatyczne usunięcie wskazanych informacji z utraconego (lub nieużywanego przez określony czas) komputera lub urządzenia.

## Ochrona przed szkodliwym oprogramowaniem

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

*Stosowanie odpowiednio skonfigurowanego oprogramowania antywirusowego*
*(a najlepiej równolegle dwóch różnych narzędzi);*
*Podnoszenie na szkoleniach świadomości pracowników nt. zagrożeń;*
*izolowanie środowisk szczególnie wrażliwych*

## Szyfrowanie danych

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

## Szyfrowanie transmitowanych danych

SSL – realizacja programowa i akceleratory

Zgodnie z wykładnią przepisów dostęp do danych osobowych za pośrednictwem systemów teleinformatycznych powinien być ograniczony do uprawnionych odbiorców danych, a informacje dotyczące atrybutów dostępu (np. identyfikator użytkownika i hasło) podlegają obowiązkowemu szyfrowaniu.

Ze względu na konieczność odpowiedniej wydajności (kryterium dostępności usługi) może okazać się, że konieczne jest wsparcie sprzętowe dla procesów transparentnego szyfrowania transmitowanej informacji.

## Szyfrowanie transmitowanych danych
ochrona treści przesyłek e-mail

Przepisy wskazują także na konieczność zabezpieczenia treści przesyłanych pomiędzy podmiotami danych osobowych, w sposób gwarantujący dostęp do nich jedynie osób uprawnionych, dlatego konieczne jest wdrożenie systemów szyfrowania korespondencji e-mail lub powstrzymanie się od wykorzystania tego kanału komunikacji dla danych objętych ochroną.

## Szyfrowanie transmitowanych danych
powszechna i stosowana, bezpieczna transmisja informacji

Systemy informatyczne oferują szerokie możliwości ochrony, transmitowanych w sieciach komputerowych, danych.
Systemy katalogowe, portale informacyjne, repozytoria danych itp.

Najbardziej powszechnym rozwiązaniem jest zastosowanie do przesyłania danych mechanizmów opartych o:
- protokół SSL (Secure Sockets Layer),
- TLS (Transport Layer Security),
- certyfikaty bezpieczeństwa SSL wystawiane i gwarantowane przez instytucje zaufania internetowego (zaufane strony trzecie lub systemy autonomiczne)

## Nadzór nad zawartością komputerów

szyfrowanie i skuteczne usuwanie informacji na nośnikach danych

Oprócz zagadnień związanych z szyfrowaniem nośników przepisy definiują także wymagania stawiane technologii kasowania/usuwania/anonimizacji informacji.

W zależności od przyjętych zasad konieczne jest stosowanie technologii trwałego usuwania informacji, najczęściej jako wielokrotny zapis wzorca kasującego na czyszczonym nośniku lub poprzez silne, jednokierunkowe szyfrowanie z losowym kluczem kodującym dane.

## Komputery osobiste

podstawowy, standardowy pakiet użytkowy

Konto administratora tylko dla admina, ew. konto użytkownika *

| | |
|---|---|
| *Administrator* | *root* |
| *Local admin* | *Grupa staff/admin* |
| *Konto z uprawnieniami* | *Konto administratora* |
| *Konto użytkownika* | *Konto użytkownika* |

Ustalony i aktualizowany system operacyjny (Windows, Linux w IT)
Pakiet biurowy (Microsoft Office lub Open Office lub Libra Office)
Zarządzalny antywirus
Programy użytkowe (według standardu)
Instalacja ze wsparciem administratora
Zdalny dostęp administracyjny (VNC, rconsola,TeamViever itp..)
Specjalistyczne aplikacje
Domena AD + konta użytkowników
(grupy, poczta, dysk sieciowy, ustawienia, drukarki, wpis do książki adresowej)
Szyfrowany dysk lokalny (nie tylko foldery), dostępny za hasłem
Kopie zapasowe: regularne, pełne (PC + SRV), kontrolowane

## Bezpieczeństwo stanowiska pracy

zasady ogólne

- Powinno być włączone i zaktualizowane oprogramowanie antywirusowe
- Niedopuszczalne jest modyfikowanie przez użytkownika systemów bezpieczeństwa,
- Należy uniemożliwić instalację programów przez użytkowników, ponieważ może stanowić zagrożenie dla prawidłowego działania komputera, systemu i ochrony danych.
  Najczęściej wykorzystywanym oprogramowaniem, które obniża poziom bezpieczeństwa komputera są:
  - narzędzia służące do wymiany plików w sieci (programy P2P),
  - komunikatory internetowe
  - szkodliwe oprogramowanie (malware) trafiające do komputerów w czasie nieostrożnego korzystania z zasobów teleinformatycznych.
- Odchodząc od stanowiska należy zawsze blokować dostęp, a system powinien automatycznie blokować komputer/terminal (np. wygaszacz ekranu chroniony hasłem)

Generalna zasada

**operator/pracownik nie jest uprawniony do samodzielnego zarządzania komputerem, jego konfiguracją i oprogramowaniem**

## System informatyczny

jego funkcjonalność i wymagania formalne dotyczące rozliczalności

System informatyczny zapewnia odnotowanie dla każdego rekordu:

- czasu wprowadzenia danych (data, godzina, minuta),
- źródła pochodzenia danych (pisemnie, adres IP, nr telefonu, …),
- nazwy użytkownika wprowadzającego dane,
- informacji komu, kiedy i w jakim zakresie dane były udostępnione,
- sprzeciwów, o których mowa w Ustawie.
- udostępnianie na piśmie, w powszechnie zrozumiałej formie, treści danych o każdej osobie, której dane są przetwarzane

Nośniki informacji oraz wydruki z danymi osobowymi przechowywać w warunkach uniemożliwiających dostęp osobom nieuprawnionym

Dyski oraz korespondencję zawierająca DO należy szyfrować, chronić, rejestrować dostęp, dokumenty zamykać, a niepotrzebne niszczyć

Urządzenia przetwarzające dane (nie tylko komputery !) należy zarządzać, zabezpieczyć i kontrolować

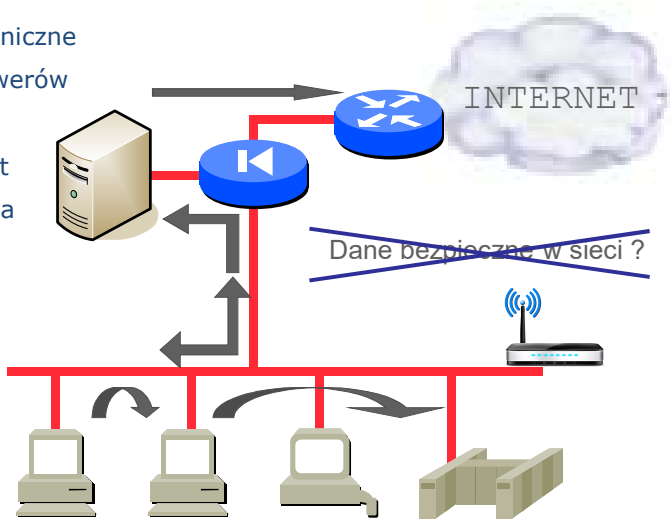
## Sieci, usługi sieciowych, dostęp do zasobów

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

## Ochrona danych i przetwarzanych informacji

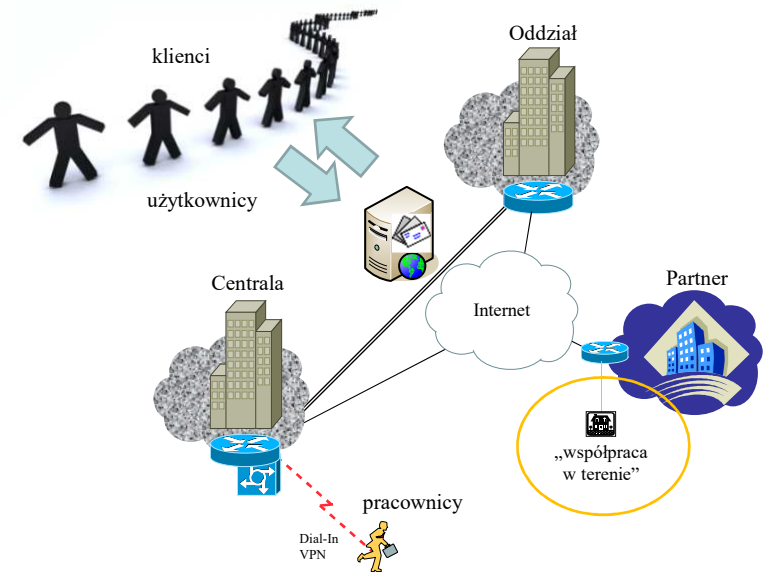
typowa struktura systemu teleinformatycznego

Dokumenty elektroniczne
Dyski lokalne i serwerów
Dane osobowe
Hasła i wykazy kont
Poczta elektroniczna
Serwisy WWW
Aplikacje i usługi



## Struktura sieci teleinformatycznych

nowe systemy, nowe zagrożenia




## Firewall

lekarstwo na wszelkie zło ?

Firewall „osobisty” komputera

Ochrona serwerów i baz danych

Sieciowe rozwiązania typu firewall

IDS, IPS, CloudIPS, WAF

Filtracja komunikacji międzysieciowej

Nie ma skutecznych rozwiązać jeśli oprócz wykrywania nie ma nadzorowanej reakcji

## Rozliczalność

- RODO – praktycznie całe Rozporządzenie opiera się o wymóg możliwości rozliczenia czyli odpowiedniego wykazania, że we właściwy sposób realizowane są obowiązki wynikające z przepisów ochrony danych osobowych
- UODO art. 38. Administrator danych jest obowiązany zapewnić kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane.
- RT/O § 7 Obowiązek zapewnienia odnotowania w systemie informatycznym szeregu informacji dla każdej osoby, której dane osobowe są w nim przetwarzane
- KRI § 21. ust. 1. – 5.
- ISO 27002 pkt. 12.4 Rejestrowanie zdarzeń i monitorowanie

## Zabezpieczenia danych osobowych

zmiany wynikające z RODO

Nowe wymagania w zakresie:

- Prowadzenia dokumentacji przetwarzania danych osobowych (art.24.2, 30, 33.5)
- Analizy ryzyka w fazie projektowania systemów i domyślnej ochrony (art.25)
- Środków technicznych i organizacyjnych, np. pseudonimizacja (art.32)
- Oceny skutków przetwarzania danych (art.35)
- Uprzednich konsultacji z organem nadzorczym (art.36)
- Wyznaczenia Inspektora Ochrony Danych (art.37-39)

Brak konkretnych wymagań dla procedur nadawania upoważnień dla operatorów danych osobowych (art.29)

Możliwość stosowania Kodeksów postępowań - branżowych, sektorowych, indywidualnych (art.40-41)

Ustanowienie mechanizmów certyfikacji, znaków jakości i oznaczeń w zakresie ochrony danych osobowych (art.42-43)

## Przetwarzanie danych osobowych
zmiany wynikające z RODO

przetwarzanie danych jedynie przez zadeklarowany okres czasu, wynikający z przepisów prawa, regulacji branżowych, umów lub ustaleń (np. zgód) z osobami których dane są przetwarzane. Konieczne jest więc ustanowienie procesów przechowywania danych w systemach oraz archiwach, w sposób zgodny z ustalonymi, dającymi się zmieniać parametrami takimi jak: zakres przetwarzanych danych, , dostęp do danych, okres przechowywania, zasady usuwania danych {wskazują na to, m.in. motywy 39, 45 oraz artykuły 5.1.e), 6.1.b/c, 6.3, 13.1/2 RODO)

minimalizacja ilości i rodzaju przetwarzanych danych, gdy ustanie konieczność ich przetwarzania w zakresie pierwotnym. Administrator zobowiązany jest do aktywnego (zaleca się wsparcie w sposób zautomatyzowany) ograniczania przetwarzania danych, pozostawiając jedynie niezbędne informacje {art.5.1.c), art.89 RODO}

wdrożenie procedur usuwania danych (anonimizacja i pseudonimizacja), zgodnych ze stawianymi wymogami formalnymi, aby zwiększyć ochronę i zmniejszyć ryzyka związane z przetwarzaniem danych {motyw 26, 28, 29 art. 4.5, 25, 32.1.a)

## Przetwarzanie danych osobowych
zmiany wynikające z RODO

umożliwienie realizacji prawa do usunięcia danych („prawo do bycia zapomnianym") polegającego na trwałym i bezpowrotnym usunięciu wszelkich danych dotyczących konkretnej osoby z zasobów cyfrowych (systemy informatyczne) i analogowych (dokumentacja papierowa). Aby to osiągnąć konieczne będzie wdrożenie mechanizmów wyszukiwania i ewidencji danych w systemach produkcyjnych oraz archiwalnych które Administrator wykorzystuje {art. 17 RODO)

wypełnienia obowiązków informacyjnych, w tym w szczególności doprecyzowanie celu, podstawy prawnej i okresu przetwarzania danych { art. 6.3, 13.1/2, 15.d RODO}

przetwarzanie danych zgodnie z właściwymi podstawami prawnymi oraz sprawdzenie i odnotowanie w prowadzonej dokumentacji czy wszystkie dane przetwarzane są zgodnie z posiadanymi przez Administratora uprawnieniami {art. 6 RODO}

## Przetwarzanie danych osobowych

zmiany wynikające z RODO

umożliwienie osobom których dane dotyczą dostępu do przetwarzanych danych poprzez opracowanie mechanizmów pozwalających na udzielenie informacji czy Administrator posiada dane na jej temat, jakie to dane, w jakim celu i w jaki sposób dane są przetwarzane. Administrator zobowiązany będzie również udostępnić kopię wszystkich przetwarzanych danych dotyczących konkretnej osoby {art. 15 RODO}

przygotowanie mechanizmów pozwalających na realizację prawa do przenoszenia danych, czyli wyodrębnienia z zasobów informatycznych i przekazania wnioskodawcy lub innemu administratorowi kopii przetwarzanych danych. Prawo to ma duże znaczenie dla Wspólnoty w przypadku, gdy następuje zmiana podmiotu zarządzającego i konieczne jest przekazanie informacji pomiędzy zarządcami {art. 20.1/2 RODO}

nadzór nad przetwarzanymi danymi, zapewnienia ich poufności, integralności i dostępności oraz zdolność do przywrócenia zawartości zbiorów danych w przypadku incydentu fizycznego lub technicznego, których sposób realizacji planuje Administrator na podstawie prowadzonej analizy ryzyka i wdraża jako rozwiązania techniczno-organizacyjne zgodnie z podjętymi decyzjami dot. ochrony przetwarzanych danych {art. 32 RODO}

## Co jest niezbędne do właściwego przetwarzania danych osobowych w serwisie WWW

- Regulamin i ew. Polityka Ochrony Prywatności
- Polityka i uprzednia informacja o ciasteczkach (cookie)
- Spełnienie obowiązku informacyjnego
- W przypadku newslettera dopuszcza się pozyskanie adresu e-mail z informacją, ale bez zbierania zgody
- Zbieramy świadome zgody na przetwarzanie: danych osobowych w celach marketingowych, w celu udostępnienia innym
- Zbieramy niezbędne dane w formularzach rejestracyjnych
- Odnotowujemy dokładnie czas i źródło zmiany
- Wysyłamy maile aktywizacyjne oraz o istotnych zmianach
- Nie wysyłamy maili z hasłem, a jedynie linki do zmiany hasła
- Nie przechowujemy haseł tekstem jawnym (plain text)

# Instrukcja postępowania w sytuacjach naruszenia ochrony danych osobowych

## Obsługa użytkowników i reakcja na incydenty

Systemy CRM, obsługa zgłoszeń, rejestracja problemów

Obowiązujące przepisy nakładają na Przedsiębiorców świadczących usługi z wykorzystaniem Nowych Technologii szereg obowiązków dotyczących obsługi klientów i terminowego reagowania na zgłaszane wnioski i zastrzeżenia związane z przetwarzanymi danymi lub usługami.

Nie jest to wymóg formalny, ale dobra praktyka, aby stosować oprogramowanie do obsługi klientów, obiegu korespondencji i dokumentów oraz prowadzić ewidencję incydentów bezpieczeństwa lub zgłaszanych usterek w świadczonych usługach. Informacje te pozwalają na czas i z odpowiednią bazą wiedzy wypełniać obowiązki i dbać o system informatyczny.

Systemy obsługi klienta i „punkt kontaktowy" dla zgłaszania incydentów

## Prowadzenie przez ADO dokumentacji przetwarzania danych

Instrukcji postępowania w sytuacjach naruszenia ochrony danych osobowych

Dobrą praktyką jest opracowanie Instrukcji, która może zawierać:

- dane kontaktowe do uprawnionej przez ADO osoby (najczęściej jest to ABI/IOD), z którą należy kontaktować się w przypadku podejrzenia lub stwierdzenia naruszenia ochrony danych,
- zasady i plan postępowania w przypadku stwierdzenia naruszenia zabezpieczeń danych,
- określenie zasad postępowania w stosunku do osób, które mogły przyczynić się do wystąpienia problemów z ochroną danych osobowych,
- wskazówki dotyczące procesu odtworzenia danych w przypadku awarii systemu.

Pozwala ona właściwie zgłosić zawiadomienie i dotrzeć z informacją, o zagrożeniu lub podejrzeniu niewłaściwego przetwarzania danych, do osób odpowiedzialnych które mogą podjąć działania wyjaśniające, dodatkowo zabezpieczające dane lub wdrożyć plany postępowania na wypadek naruszenia ochrony danych.

## Prowadzenie przez ADO dokumentacji przetwarzania danych

Instrukcji postępowania w sytuacjach naruszenia ochrony danych osobowych

Określa tryb postępowania gdy:

- stwierdzono naruszenie zabezpieczenia systemu informatycznego
- stan urządzenia, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programy lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych

W powyższych przypadkach osoba przetwarzająca dane osobowe niezwłocznie powiadamia administratora bezpieczeństwa informacji lub inną upoważnioną przez niego osobę.

Informować ABI należy także gdy:

- niemożliwe jest zmienianie haseł chroniących dane zgodnie z ustalonymi regułami (hasło 6 znaków, zmieniane co miesiąc)
- nie działają automatyczne wygaszacze ekranów oraz hasła chroniące dostęp do komputerów (BIOS)

## Niszczenie nośników danych

Niszczarka dla papieru i CD

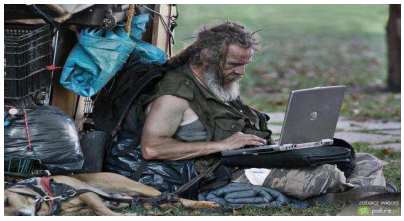
Demagnetyzer dla dysków

## Efekty niszczenia

Czy z makaronu da się uzyskać ciasto ?

Paski o szerokości 4,9 mm i długości 50 mm

## Przeznaczanie danych -> segregator okrągły …



Wydruki, płyty CD, notatki, …
trafiają do śmietnika

Aby dotrzeć do tego
„informatycznego zasobu”
nie trzeba się włamywać,
ani przechodzić obok ochrony

Wystarczy przebranie kloszarda lub licencja na wywóz śmieci.

Zezwolenia na prowadzenie działalności gospodarczej w zakresie usuwania, wykorzystywania i unieszkodliwiania odpadów komunalnych wydaje wójt (burmistrz lub prezydent miasta).

Ostatecznie zawsze można poczekać, aż zostaną wywiezione na wysypisko…

## Ewidencje dotyczące przetwarzania danych osobowych

## Prowadzenie przez ADO dokumentacji przetwarzania danych

Ewidencja osób upoważnionych do przetwarzania danych

Na podstawie art. 39 ust. 1 UODO ADO prowadzi, w wersji papierowej lub elektronicznie, ewidencję osób upoważnionych do przetwarzania danych. ADO decyduje, jakie informacje się w niej znajdują.

Najczęściej rejestrowane są:
Imię i nazwisko osoby upoważnionej, operatora danych,
Data przyznania uprawnień do przetwarzania danych,
Zbiór, którego uprawnienia dotyczą,
Identyfikator użytkownika w systemie informatycznym,
Data cofnięcia uprawnień.

Mając na uwadze konieczność zachowania rozliczalności, zaleca się, aby w przypadku cofnięcia uprawnień w ewidencji pozostawały wszystkie informacje na ich temat oraz dane osób które uprawnienia posiadały.

W RODO przetwarzanie danych odbywa się **z upoważnienia Administratora i na jego polecenie** (art.23, 32.4)

Ewidencja może być prowadzona,
a upoważnienia nadawane, elektronicznie

## Prowadzenie przez ADO dokumentacji przetwarzania danych

Inne ewidencję związane z procesem przetwarzania DO

Administrator danych powinien posiadać pełną wiedzę o procesie przetwarzania danych osobowych, dlatego oprócz wymaganych przepisami ewidencji prowadzi dodatkowe wykazy, stosowanie do potrzeb, specyfiki własnej organizacji oraz przyjętych rozwiązań organizacyjnych i technicznych. Przepisy nie wskazują na konkretną formę lub zawartość prowadzonych ewidencji, dlatego administratorzy danych prowadzą część z nich w formie papierowej, część elektronicznie jako zestawienia danych a reszta dostępna jest jako raporty lub zestawienia w systemach informatycznych służących do przetwarzania informacji.

Jako przykłady można wskazać:
1) Wykaz systemów upoważnionych / mających dostęp do przetwarzanych danych osobowych,
2) Wykaz umów związanych z przetwarzaniem danych osobowych,
3) Ewidencja korespondencji dotyczącej ochrony danych osobowych,
4) Ewidencja incydentów bezpieczeństwa związanych z ochroną danych osobowych,
5) Ewidencja dostępu fizycznego do stref przetwarzania danych,
6) Wykaz kont poczty elektronicznej wykorzystywanych w procesach przetwarzania danych,

## Prowadzenie przez ADO dokumentacji przetwarzania danych

Inne ewidencję związane z procesem przetwarzania DO

- Upoważnienie do przetwarzania danych osobowych
- Oświadczenie/zobowiązanie do przestrzegania zasad ochrony danych Oświadczenie/zobowiązanie do ochrony Tajemnicy Przedsiębiorstwa
- Szkolenie dot. Ochrony danych osobowych i lista obecności
- Zaświadczenie o powyższych

Uchwała/decyzja ADO o upoważnieniu operatorów danych
+ załączniki:
1. wzór upoważnienia
   (powołanie zakresu obowiązków, umowy i poleceń przełożonych)
2. lista osób upoważnionych

## Bezpieczeństwo zasobów ludzkich

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

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

## Bezpieczeństwo zasobów ludzkich – Kadry/HR

- Przed zatrudnieniem
  - Role i zakresy odpowiedzialności
  - Postępowanie sprawdzające
  - Warunki i zasady zatrudnienia pracownika
- Podczas zatrudnienia
  - Odpowiedzialność kierownictwa
  - Uświadamianie, kształcenie i szkolenia z zakresu bezpieczeństwa informacji
  - Postępowanie dyscyplinarne
- Zakończenie lub zmiana zatrudnienia
  - Odpowiedzialność związana z zakończeniem zatrudnienia
  - Zwrot aktywów
  - Odebranie praw dostępu

## Dane osobowe – Kadry/HR

Imię (imiona) i nazwisko
Imiona rodziców
Data urodzenia
Miejsce zamieszkania (adres do korespondencji)
Wykształcenie
Przebieg dotychczasowego zatrudnienia

Numer PESEL pracownika
Inne dane osobowe pracownika, a także imiona i nazwiska oraz daty urodzenia dzieci pracownika, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień
Dane kontaktowe do wykorzystania w przypadku wypadku

*Art. 22[1] Prawa Pracy*

## Umowa z pracownikiem/współpracownikiem

„Cykl życia" **pracownika** !

Podpisanie odpowiedniej wersji umowy
*(w tym powierzenie przetwarzania danych osobowych)*
Przygotowanie zasobów dla nowego stanowiska pracy
Założenie kont w AD, systemach i aplikacjach
Konfiguracja uprawnień
Obiegówka przyjęcia pracownika
Zmiany
Obiegówka odejścia

## „Cykl życia" danych Użytkownika w systemie internetowej obsługi Strony

Gdzie pojawiają się problemy dla IT ?

Serwis internetowy + infrastruktura IT
dostępność w sieci, ochrona, backupy, regulamin (umowa) i polityka ochrony prywatności (opis)
Rejestracja Użytkownika
bezpieczny formularz z niezbędnymi danymi, rejestracja, zbieranie zgody, notyfikacja, połączenia
Potwierdzenie danych
walidacja treści i kompletności danych, kontrola powtórzeń, mail aktywacyjny
**Kontrola dostępu**
hasła: zalecenia dla klienta, skomplikowane dla obsługi, zmiana i przypomnienie, hash+salt,
**Uprawnienia Użytkownika**
prywatność, zmiana danych, przekazywanie danych, odwołanie zgody, kontakt z usługodawcą
**Rozwiązanie umowy**
usunięcie konta ≠ usunięcie danych, okresy przechowywania informacji, odmowa usunięcia
**Obsługa incydentów**
zabezpieczenie informacji, retencja, logi z połączeń i aktywności, blokady Notice & Takedown

## Retencja danych osobowych

Zasada ograniczenia czasowego – przechowywać dane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

*Przykłady okresów retencyjnych*

- **3 dni** – logi systemów IT
- **1 rok** - logi w telekomunikacji, dokumenty dotyczące reklamacji
- **2 lata** - wygaśnięcie roszczeń jako usługodawcy w relacji pomiędzy podmiotami profesjonalnymi z tytułu umów o świadczenie usług, dokumenty dotyczące rękojmi
- **3 lata** - wygaśnięcie roszczeń w relacji pomiędzy podmiotami a klientami nieprofesjonalnymi oraz pozostałych roszczeń w relacji pomiędzy podmiotami profesjonalnymi, także dla roszczeń z zakresy prawa pracy
- **5 lat** (od końca roku podatkowego) - dokumentacja finansowo-księgowa, księgi rachunkowe
- **10 lat** - wygaśnięcie roszczeń cywilnoprawnych, dokumentacja ZUS
- **50/10 lat** - dokumentacja kadrowo-płacowa

## Identyfikacja tożsamości Klienta/Użytkownika

Udostępnianie informacji - przykłady

1. Osobiście, po okazaniu dokumentu tożsamości
   *{czy każdy może prosić o okazanie dowodu ?}*
2. Korespondencyjnie *{potencjalna możliwość fałszerstwa}*,
   na podstawie:
   - Oświadczenia osoby której sprawa dotyczy,
   - Poświadczenia tożsamości przez uprawniony podmiot lub zaufaną osobę,
   - Przekazanie kopii dokumentu poświadczającego tożsamość.
3. Telefonicznie *{problem prawny powiązania numeru z osobą}*:
   - SMS (mikropłatności lub kody aktywacyjne),
   - rozmowa telefoniczna
4. Przekaz pocztowy *{można wpisać dowolne dane nadawcy}*
5. Operacje bankowe *{tajemnica bankowa}*
   - Płatności na kontach masowych
     *{klient to tylko numer transakcji lub subkonta}*
   - Płatności indywidualne
     *{a jeśli to nie Klient płaci ?}*
   - Płatności kartą kredytową
     *{przekazywane są dane w zależności od systemu}*

Dokument potwierdzający tożsamość …


## Podstawy prawne udostępniania danych

Udostępnianie informacji

Ustawa o **Ochronie Danych Osobowych w art. 23 ust.1.5** zezwala na udostępnienie danych osobowych, ale po stronie Administratora Danych pojawia się problem interpretacyjny, gdyż udostępniający odpowiada fakt i ewentualne skutki niewłaściwego udostępnienia.

Ustawa o **Świadczeniu Usług Drogą Elektroniczną**, **art. 18 ust.6** zobowiązuje usługodawców do udzielania organom państwowym, na potrzeby prowadzonych postępowań, informacji o danych eksploatacyjnych, bez wskazania wymaganego zakresu danych, ani czasu ich przechowywania.

**Art. 236a Kodeksu Postępowania Karnego** ma zastosowanie szczególnie wtedy, gdy postanowienie dotyczy wydania treści korespondencji.

**Art. 488 § 1 Kodeksu Postępowania Karnego** jest przydatny dla wykrycia sprawcy przestępstwa prywatnoskargowego popełnionego na szkodę osoby.

W innych przypadkach pozostaje **postępowanie administracyjne w GIODO** …

# Umowa powierzenia przetwarzania danych osobowych

Umowa powierzenia przetwarzania danych osobowych

## Administrator i inni w RODO

**Relacja Administrator-Procesor**

Administrator ma obowiązek korzystania 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 (art.28 ust.1)

Obowiązek sprawdzenia, czy procesor zapewnia właściwe gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, w szczególności, gdy chodzi o wiedzę fachową, wiarygodność i dostępne zasoby (motyw 81)

Możliwość dowodzenia wystarczających gwarancji przez procesora na podstawie:

- zatwierdzonych kodeksów postępowania (art.40)
- zatwierdzonych mechanizmów certyfikacji, znaków jakości i oznaczeń (art.42)

Zakres stosowania kodeksów postępowania, certyfikacji i znaków jakości:

- rozliczalność przestrzegania przez administratora obowiązków wdrożenia odpowiednich środków technicznych i organizacyjnych
- podstawa przekazywania danych do państw trzecich i organizacji międzynarodowych niezapewniających odpowiedniego poziomu ochrony

## Administrator i inni w RODO

**Relacja Administrator-Procesor**

Podstawą przetwarzania ma być umowa, której treść została istotnie zmodyfikowana (art.28 ust.3 RODO) w stosunku do dotychczasowego stanu prawnego wynikającego z UODO, lub inny instrument prawny wiążące administratora i procesora podległością na terenie UE, określające:

- przedmiot i czas trwania przetwarzania,
- charakter i cel przetwarzania,
- rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,
- obowiązki i prawa administratora

Zapisy umowy powinny uwzględniać konkretne zadania i obowiązki podmiotu przetwarzającego w kontekście planowanego przetwarzania oraz ryzyko naruszenia praw lub wolności osób, których dane dotyczą (motyw 81)

Uwzględniając charakter przetwarzania oraz dostępne mu informacje, podmiot przetwarzający ma zobowiązywać się do pomagania administratorowi wywiązać się z obowiązków określonych w art. 32–36 (bezpieczeństwo danych, powiadamiania o naruszeniach, ocena skutków przetwarzania danych z uwagi na wysokie ryzyko dla podmiotów danych etc.)

## Administrator i inni w RODO

**Relacja Administrator-Procesor**

Komisja Europejska oraz Organ Nadzoru otrzymały kompetencje do wydawania standardowych klauzul umownych dotyczących relacji administrator – procesor, przy czym podmioty przetwarzające dane mają możliwość (ale nie obowiązek) posługiwania się nimi (art.28 ust.7 i 8)

Podpowierzenie danych (subprocessing) jest dopuszczalny wyłącznie na podstawie ogólnego lub szczegółowego pełnomocnictwa (pisemna lub równoważna jej forma elektroniczna)

W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających (subprocesorów), dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian (art.28 ust.2)

## Administrator i inni w RODO

**Relacja Procesor-Subprocesor**

Podpowierzenie danych – obowiązki i odpowiedzialność *procesora* (art.28.4)

- jeżeli do wykonania w imieniu administratora konkretnych czynności przetwarzania podmiot przetwarzający korzysta z usług innego podmiotu przetwarzającego, na ten inny podmiot przetwarzający nałożone zostają te same obowiązki ochrony danych jak w umowie lub innym akcie prawnym między administratorem a podmiotem przetwarzającym, w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom niniejszego rozporządzenia.

- jeżeli podmiot przetwarzający (podprocesor) 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 (procesorze)

## Umowa powierzenia danych osobowych RODO

**Obowiązki procesora (podprocesora) zależne od charakteru przetwarzania**

Procesor, gdy to możliwe, powinien wdrożyć środki techniczne i organizacyjne mające na celu realizację obowiązku informacyjnego oraz praw osób, których dane dotyczą (rozdział III):

- dostęp
- sprostowanie danych
- bycie zapomnianym
- ograniczenie przetwarzania
- przenoszenie danych
- sprzeciw
- niepodleganie zautomatyzowanemu podejmowaniu decyzji

Procesor powinien pomagać administratorowi w realizacji obowiązków (art.32-36):

- bezpieczeństwo przetwarzania
- zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu
- zawiadomienie podmiotu danych o naruszeniu
- ocena skutków dla ochrony danych
- uprzednie konsultacje

## Umowa powierzenia danych osobowych

**Treść umowy** została istotnie zmodyfikowana w stosunku do dotychczasowego stanu prawnego (art.31 UODO vs art.28 ust.3 RODO), procesor:

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 *(bezpieczeństwo przetwarzania)*;

d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w ust. 2 i 4 *(podpowierzenie)*;

## Umowa powierzenia danych osobowych

**Treść umowy** została istotnie zmodyfikowana w stosunku do dotychczasowego stanu prawnego (art.31 UODO vs art.28 ust.3 RODO), procesor (cd.):

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 *(bezpieczeństwo danych, powiadamianie o naruszeniach, ocena skutków przetwarzania danych z uwagi na wysokie ryzyko dla podmiotów danych etc.)*;

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.

## Powierzenie przetwarzania danych osobowych

**Do obowiązków procesora należy też prowadzenie rejestru przetwarzania danych**

Administrator i procesor prowadzą, każdy we własnym zakresie, rejestry czynności przetwarzania

- administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada
- procesor prowadzi rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora

Każdy administrator lub podmiot przetwarzający udostępnia rejestr na żądanie organu nadzorczego

Dla zachowania zgodności z RODO, administrator lub podmiot przetwarzający powinni prowadzić rejestry czynności przetwarzania, za które są odpowiedzialni. Każdy administrator i każdy podmiot przetwarzający powinni mieć obowiązek współpracować z organem nadzorczym i na jego żądanie udostępniać mu te rejestry w celu monitorowania tych operacji przetwarzania (motyw 82)

## Umowa powierzenia, czyli ...

- Każda umowa powierzenia przetwarzania danych osobowych powinna być umową staranności. Nie można ograniczyć się do umowy rezultatu.
- Umowa powierzenia powinna tak regulować zasady współpracy i kontroli, aby Administrator mógł w pełni nadzorować proces przetwarzania danych u Procesora i jego podwykonawców.
- Każda nowo zawierana umowa powinna przewidywać zbliżające się zmiany w stosowaniu przepisów dotyczących ochrony danych osobowych, w związku z tym należy w niej wskazać jak strony podchodzą do daty 25 maja 2018, czy powoduje ona zakończenie umowy, czy też jej kontynuację pod konkretnymi warunkami, do spełnienia których, z odpowiednim wyprzedzeniem, zobowiązany jest Procesor i/lub Administrator.
- W umowach należy przewidzieć zmieniające się, a dające się na chwilę obecną określić, wymogi formalno-prawne związane ze zmianami prawa oraz zakres usług świadczonych obecnie i po 24 maja 2018 na rzecz podmiotów danych, ponieważ może to wpłynąć na parametry biznesowe umów, procedury, czas i wymagane środki oraz zasoby.

## Umowa, czyli ...

1. W ramach umowy Zleceniodawca jako Administrator, zgodnie z art. 28 ust. 3 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) – zwanej (dalej „RODO"), powierza Zleceniobiorcy (dalej Procesorowi danych, Podmiotowi przetwarzającemu zgodnie z art. 28 RODO) czynności związane z przetwarzaniem danych osobowych.
2. Zleceniodawca powierza czynności przetwarzania .....
3. Zakres powierzonych danych / czynności obejmuje .....
4. Zleceniobiorca zobowiązuje się przetwarzać powierzone dane osobowe jedynie w celu i zakresie określonych odpowiednio w ust. 2 i 3.
5. Zleceniobiorca informuje Zleceniodawcę przed rozpoczęciem przetwarzania danych o realizacji ewentualnego obowiązku prawnego polegającego na przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, zgodnie z art. 28 ust. 3 lit. a RODO.
6. Zleceniobiorca zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich tajemnicy lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, zgodnie z art. 28 ust. 3 lit. b RODO.

## Umowa, czyli ...

7. Zleceniobiorca oświadcza, że podjął środki zabezpieczające, wymagane na mocy art. 32 RODO, zgodnie z art. 28 ust. 3 lit. c RODO.
8. Zleceniodawca zastrzega sobie możliwość kontroli sposobu wypełnienia przez Zleceniobiorcę wymagań wymienionych w ust. 4, 6 i 7, zgodnie z art. 28 ust. 3 lit. h RODO.
9. Zleceniobiorca pomaga Zleceniodawcy poprzez uzgodnione, wskazane w załączniku nr 1, środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw, zgodnie z art. 28 ust. 3 lit. e RODO.
10. Zgodnie z art. 28 ust. 3 lit. f RODO, Zleceniobiorca uczestniczy w realizacji obowiązków Zleceniodawcy, określonych w art. 32–36 RODO, w następującym zakresie .....
11. Zleceniodawca zastrzega sobie wyrażenie zgody w każdym przypadku dalszego powierzenia przetwarzania, a Zleceniobiorca przestrzega warunków korzystania z usług innego podmiotu przetwarzającego, o których mowa w art. 28 ust. 2 i 4 RODO.
12. Zleceniobiorca zobowiązuje się protokolarnie zwrócić lub trwale usunąć wszelkie powierzone do przetwarzania dane osobowe w terminie 14 dni od zakończenia / rozwiązania umowy, a jeden z podpisanych egzemplarzy protokołu zwrotu / usunięcia danych przekazać Zleceniodawcy, zgodnie z art. 28 ust. 3 lit. g RODO.

## Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO art.33

**Zadanie Administratora**

Art.4 pkt 12

„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”

- obowiązek powiadomienia organu nadzoru
- obowiązek powiadomienia podmiotu danych osobowych
- obowiązek powiadomienia administratora przez podmiot przetwarzający

Art. 33.5 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.

## Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO art.33/34

**Obowiązek zgłaszania naruszenia organowi nadzorczemu:**

- 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, 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.

  (art. 33 ust. 1 RODO)

**Obowiązek zawiadomienia osób, których dane dotyczą:**

- Jeżeli naruszenie ochrony danych osobowych **może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.

  (art. 34 ust. 1 RODO)

## Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu RODO art.33/34

Zawiadomienie nie jest wymagane:

- jeżeli 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
- jeżeli administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą
- jeżeli 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

## Usługi realizowane za pomocą systemów IT

z czego korzystamy ?

Z jakich serwisów korzystamy ?

| | |
|---|---|
| Poczta elektroniczna | Gmail, Outlook, Home, Onet, … |
| Pakiet biurowy | Office 365, Google Docs, … |
| Serwis WWW | hosting, np. Amazon, Home.pl, NetArt, OVH |
| Ochrona serwisów | firewall, CloudFlare CDN, … |
| Dyski sieciowe | własna siec lokalna, WD Cloud, GoogleDisk, … |
| Czat | messanger, skype, FB, GG, Signal, Telegraph, … |
| Cloud Computing | wszystkie typy usług |

## Serwerownia

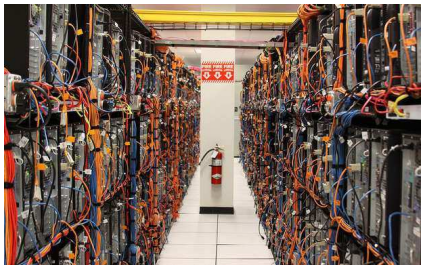
To brzmi dumnie …

- Komputer pod biurkiem – w domu, biurze, sekretariacie, u informatyka
- Komputer (zwany serwerem) w wiszącej na ścianie „szafce ileś tam U”
- Dedykowane pomieszczenie w biurze na sprzęt komputerowy
- Pomieszczenie współdzielone w budynku z innymi podmiotami

- Własne Centrum Danych
  albo
- Kolokacja
- Hoteling
- Hosting
- Hosting aplikacyjny
- Chmura obliczeniowa

## Gdzie i u kogo przechowywać dane ?

miejsca i sposób przetwarzania danych



Serwerownia, czyli:

Urządzenia
- Komputery
- Komunikacja
- Magazyny danych

Zasilanie
Klimatyzacja
Sieć komputerowa

Bezpieczeństwo fizyczne
- CCTV
- SKD
- SSWiN

Obsługa (serwis i administracja)

Optymalizacja kosztów

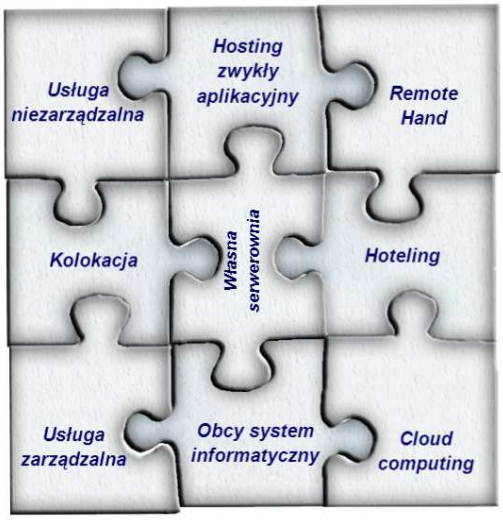
## Gdzie i u kogo przechowywać dane ?

miejsca i sposób przetwarzania danych

Szukając oszczędności przedsiębiorcy korzystają z usług mało wiarygodnych usługodawców.

Powierzenie przetwarzania danych i ocena wiarygodności i rzetelności podwykonawców.

Zalecane jest, aby dane powierzane do obcych systemów szyfrować po stronie klienta, a nie na serwerze lub u usługodawcy



## Cloud Computing - Przetwarzanie danych w chmurze

Optymalizacja kosztów i reorganizacja podejścia do systemów

IaaS - Infrastructure as a Service - Infrastruktura jako usługa
skalowalna obsługa sieci, serwerów i pamięci masowej należących do klienta

PaaS - Platform as a Service - Platforma jako usługa
usługodawca udostępnia środowisko teleinformatyczne, klient uruchamia systemy i aplikacje

SaaS - Software as a service - Oprogramowanie jako usługa
usługodawca wynajmuje pełne środowisko teleinformatyczne, łącznie z aplikacjami

BaaS - Backup as a service
TEaaS - Test Environment as a Service
STaaS - Storage as a service
SECaaS - Security as a service
DaaS - Data as a service
DBaaS - Database as a service
APIaaS - API as a service
DV - Desktop virtualization

źródło: m.in. Wikipedia/Cloud_computing

## Cloud computing - Przechowywanie danych w chmurze obliczeniowej

Czyli o tym że nie powinno się zapominać o przepisach w nowych technologiach

Technologie chmurowe należy analizować w szczególności względem:

- Deklarowanego miejsca przetwarzania informacji
  - chmura własna, budowana przez podmiot
  - chmura prywatna, dedykowana klientowi
  - chmura publiczna, współdzielona przez hostingodawcę
  - chmura europejska vs chmura globalna
- Skalowalności i stopień skomplikowania rozwiązania
- Odporności na usterki (wsparcie własnymi mechanizmami zapasowymi)
- Dostępności komponentów systemowych
- Oferowanych rozwiązań kryptograficznych

## Cloud Computing przetwarzanie danych w chmurze

Problemy związane z przetwarzaniem danych w chmurze:
- Kłopot z określeniem miejsc przetwarzania (przechowywania) danych
- Trudna pozycja negocjacyjna w zakresie obowiązków dostawcy usługi chmurowej, a z przepisów wynikają obowiązki prowadzenia dokumentacji i postępowania zgodnie z restrykcyjnymi wymaganiami techniczno-organizacyjnymi (np. hasła do systemów zmieniane co 30 dni, ewidencje użytkowników i osób mogących mieć dostęp do danych, odpowiednio realizowane kopie zapasowe, …)
- Wątpliwości w zakresie powierzenia przetwarzania danych osobowych (processing i subprocessing), szczególnie z zakresie dokumentowania relacji z podwykonawcami
- Niedoceniane zagadnienie kopii zapasowych danych przetwarzanych w chmurze
- Zmniejszenie czujności ADO w zakresie nadzoru nad systemami IT

Problemy związane z przetwarzaniem danych poza obszarem EOG:
- Eksport danych poza EOG (gdy chmura „przekracza granice" lub serwerownia znajduje się w kraju trzecim) zgoda GIODO lub podpisanie umów w oparciu o Wzorcowe/Standardowe Klauzule Umowne (ADO/ADO, ADO/Procesor)
- Rola Wiążących Reguł Korporacyjnych (BCR) w transgranicznym obrocie danymi.

## Sprawdzanie zgodności, audyt wewnętrzny

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

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

## Sprawdzanie zgodności, audyt wewnętrzny c.d.


## Co należy objąć Audytem ?

- posiadaną dokumentację ochrony danych osobowych pod kątem jej zgodności z prawem oraz aktualności,
- przesłanki legalności przetwarzania danych osobowych,
- zakres i cel przetwarzania danych,
- merytoryczną poprawność danych i ich adekwatność w stosunku do celu przetwarzania,
- zabezpieczenia infrastruktury teletechnicznej (komputer,sieć,serwer,itd.),
- procedury zarządzania upoważnieniami i uprawnieniami, backupu oraz pracy z urządzeniami przetwarzającymi dane osobowe w formie elektronicznej,
- funkcjonalności aplikacji przetwarzających dane osobowe oraz poziom ich zabezpieczeń,
- zabezpieczenia zbiorów danych osobowych przetwarzanych w formie papierowej,
- poziom wiedzy i świadomości pracowników w zakresie ochrony danych osobowych,
- zawarte umowy związane z przetwarzaniem danych osobowych.

## Zgodność

- RODO Art. 5 Zasady dotyczące przetwarzania danych osobowych, Art. 6 Zgodność przetwarzania z prawem
- UODO rozdział 3, 4, 6 i 7
  - Przesłanka legalności (podstaw prawnych), na podstawie których przetwarzane są dane osobowe (art. 23 i 27),
  - Realizacja obowiązku informacyjnego, w tym poprawności klauzul informacyjnych i oświadczeń na formularzach do zbierania danych (art. 24 i 25),
  - Realizacja obowiązków dotyczących celowości, adekwatności i czasu przetwarzania danych osobowych (art. 26),
  - Poprawność wypełnienia obowiązków związanych z powierzaniem danych innym podmiotom lub przez inny podmiot (art. 31),
  - Realizacja praw osób, których dane są przetwarzane (art. 32 i 33),
  - Realizacja obowiązku rejestracji (i aktualizacji) zbiorów danych (art. 40 i 41),
  - Poprawność procedur dotyczących udostępniania danych do państw trzecich – poza UE (art. 47 i 48).
- KRI § 20. 2. 12) h) zapewnienia odpowiedniego poziomu bezpieczeństwa w systemach teleinformatycznych, polegającego w szczególności na (…) kontroli zgodności systemów teleinformatycznych z odpowiednimi normami i politykami bezpieczeństwa;
- ISO 27002 pkt. 18.1.4 Prywatność i ochrona danych identyfikujących

## Zgodność

Odpowiednia dokumentacja !

(np. na podstawie analiza ryzyka przetwarzania danych, stwierdzonych naruszeń ochrony danych osobowych)

Przystąpienie do zatwierdzonych kodeksów postępowania

Stosowanie zatwierdzonych mechanizmów certyfikacji

## Odpowiedzialność

1. **Administracyjna**
2. **Cywilnoprawna** (dane osobowe jako dobro osobiste, roszczenia sądowe – zadośćuczynienia za doznaną krzywdę wyrządzoną wskutek udostępnienia danych).
3. **Według prawa pracy** (postępowanie w celu nałożenia kary porządkowej, postępowanie zmierzające do rozwiązania stosunku pracy)
4. **Karna**


## Penalizacja w RODO

**Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych**

Art.58 ust.2 Uprawnienia naprawcze Organu Nadzorczego:

- **wydawanie ostrzeżeń** administratorowi lub podmiotowi przetwarzającemu dotyczących możliwości naruszenia przepisów niniejszego rozporządzenia poprzez planowane operacje przetwarzania
- **udzielanie upomnień** administratorowi lub podmiotowi przetwarzającemu w przypadku naruszenia przepisów niniejszego rozporządzenia przez operacje przetwarzania
- **nakazanie** administratorowi lub podmiotowi przetwarzającemu **spełnienia żądania osoby**, której dane dotyczą, wynikającego z praw przysługujących jej na mocy niniejszego rozporządzenia;
- **nakazanie** administratorowi lub podmiotowi przetwarzającemu **dostosowania operacji przetwarzania do przepisów** niniejszego rozporządzenia, a w stosownych przypadkach wskazanie sposobu i terminu

## Penalizacja w RODO

**Sankcje cywilnoprawne**
**za naruszenie przepisów o ochronie danych osobowych**

Art.82:

- każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia niniejszego rozporządzenia, ma prawo uzyskać od administratora lub podmiotu przetwarzającego odszkodowanie za poniesioną szkodę.

- każdy administrator uczestniczący w przetwarzaniu odpowiada za szkody spowodowane przetwarzaniem naruszającym niniejsze rozporządzenie. Podmiot przetwarzający odpowiada za szkody spowodowane przetwarzaniem wyłącznie, gdy nie dopełnił obowiązków, które niniejsze rozporządzenie nakłada bezpośrednio na podmioty przetwarzające, lub gdy działał poza zgodnymi z prawem instrukcjami administratora lub wbrew tym instrukcjom.

- administrator lub podmiot przetwarzający zostają zwolnieni z odpowiedzialności wynikającej z ust. 2, jeżeli udowodnią, że w żaden sposób nie ponoszą winy za zdarzenie, które doprowadziło do powstania szkody.

## Penalizacja w RODO

**Sankcje cywilnoprawne**
**za naruszenie przepisów o ochronie danych osobowych**

Art.82:

- jeżeli w tym samym przetwarzaniu uczestniczy więcej niż jeden administrator lub podmiot przetwarzający lub uczestniczy w nim zarówno administrator jak i podmiot przetwarzający i zgodnie z ust. 2 i 3 odpowiadają za szkodę spowodowaną przetwarzaniem, ponoszą oni **odpowiedzialność solidarną za całą szkodę**, tak by zapewnić osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

- administrator lub podmiot przetwarzający, który zgodnie z ust. 4 zapłacił odszkodowanie za całą wyrządzoną szkodę, ma prawo żądania od pozostałych administratorów lub podmiotów przetwarzających, którzy uczestniczyli w tym samym przetwarzaniu, zwrotu części odszkodowania odpowiadającej części szkody, za którą ponoszą odpowiedzialność, zgodnie z warunkami określonymi w ust. 2. (**regres**)

## Penalizacja w RODO

Administracyjne kary pieniężne nakłada się, zależnie od okoliczności każdego indywidualnego przypadku, oprócz lub zamiast środków, o których mowa w art. 58 ust. 2 lit. a)–h) oraz j).

**Kary administracyjne**
**za naruszenie przepisów o ochronie danych osobowych**

Art.83 **Kary pieniężne**

Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

- charakter, wagę i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczby poszkodowanych osób, których dane dotyczą,
- rozmiaru poniesionej przez nie szkody; b) umyślny lub nieumyślny charakter naruszenia
- działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą
- stopień odpowiedzialności administratora lub podmiotu przetwarzającego z uwzględnieniem środków technicznych i organizacyjnych wdrożonych przez nich na mocy art. 25 i 32
- wszelkie stosowne wcześniejsze naruszenia ze strony administratora lub podmiotu przetwarzającego

## Penalizacja w RODO

**Kary administracyjne**
**za naruszenie przepisów o ochronie danych osobowych**

Art.83 **Kary pieniężne**

Decydując, czy nałożyć administracyjną karę pieniężną, oraz ustalając jej wysokość, zwraca się w każdym indywidualnym przypadku należytą uwagę na:

- stopień współpracy z organem nadzorczym w celu usunięcia naruszenia oraz złagodzenia jego ewentualnych negatywnych skutków
- kategorie danych osobowych, których dotyczyło naruszenie; h) sposób, w jaki organ nadzorczy dowiedział się o naruszeniu, w szczególności, czy i w jakim zakresie administrator lub podmiot przetwarzający zgłosili naruszenie
- jeżeli wobec administratora lub podmiotu przetwarzającego, których sprawa dotyczy, zostały wcześniej zastosowane w tej samej sprawie środki, o których mowa w art. 58 ust. 2 – przestrzeganie tych środków
- stosowanie zatwierdzonych kodeksów postępowania na mocy art. 40 lub zatwierdzonych mechanizmów certyfikacji na mocy art. 42 wszelkie inne obciążające lub łagodzące czynniki mające zastosowanie do okoliczności sprawy, takie jak osiągnięte bezpośrednio lub pośrednio w związku z naruszeniem korzyści finansowe lub uniknięte straty.

## Penalizacja w RODO

Art.83 **Kary pieniężne**

4. **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. **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

## Penalizacja w RODO

nUODO Art. 103. 1. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100 000 złotych, na:

l) jednostki sektora finansów publicznych, o których mowa wart. 9 pkt 1- 12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych

2) instytuty badawcze w rozumieniu ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych;

3) Narodowy Bank Polski.

2. Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 10 000 złotych na jednostki sektora finansów publicznych, o których mowa w art. 9 pkt 13 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych (państwowe i samorządowe instytucje kultury).

Nałożenie kary spowoduje odpowiedzialność urzędnika za dyscyplinę finansów publicznych

Ograniczenie nie dotyczy niektórych organów publicznych oraz państwowych i samorządowych instytucji kultury.

## Bibliografia - wykaz najważniejszych źródeł


- „Ochrona danych osobowych w ramach funduszy europejskich dot. nowej perspektywy finansowej 2014-20", M.Kołodziej, Urząd Marszałkowski, CE Compendium, Kraków, 11.2014
- „Bezpieczeństwo teleinformatyczne w jednostce samorządowej", M.Kołodziej, SNTSW, Pabianice, 09.2016r.
- „Audyt ochrony danych osobowych", W. Jakubowski, Podlaska Konferencja Informatyczna, Łomża 04.2017r.
- „Wymagania dla IT dotyczące ochrony informacji", M.Kołodziej, III Podlaska Konferencja Informatyczna, Łomża 04.2017r.
- „Zmiany i wyzwania w ochronie danych osobowych związane z wprowadzeniem RODO", M.Kołodziej, WSZiP Wałbrzych, 02.2017
- Materiały własne z ponad 50 szkoleń, warsztatów forów i konferencji, M.Kołodziej, lata 2015-2017

- „Ochrona danych osobowych w marketingu Internetowym", M.Kołodziej, wyd. WiP, 12.2015
- „Vademecum administratora bezpieczeństwa informacji", praca zbiorowa/M.Kołodziej, wyd. Beck, 01.2016r.
- **„Vademecum ABI. Część II – Przygotowanie do roli Inspektora Ochrony Danych", praca zbiorowa pod redakcją M. Kołodziej, wyd. Beck 05.2017r.**
- „Realizacja praw osób, których dane dotyczą, na podstawie RODO", Biblioteka ABI Expert, B.Fischer, M.Sakowska-Baryła, wyd. PRESSCOM, 11.2017r.
- **„Stanowisko komputerowe, na którym przetwarzane są informacje chronione, w tym dane osobowe", M. Kołodziej, Informacja w administracji publicznej, wyd. Beck 11.2016**
- Cykl artykułów dot.technicznych aspektów ochrony danych osobowych, M.Kołodziej, czasopismo ABI Expert, wyd. PRESSCOM, od 07.2017r.
- „Ochrona prywatności w miejscu pracy", komisja Europejska, Projekt Leonardo, Bruksela 2014
- „Podręcznik europejskiego prawa o ochronie danych", Agencja Praw Podstawowych UE i Rada Europy, 2014


## Bibliografia - wykaz najważniejszych źródeł