Uniwersytet Rzeszowski

OCHRONA DANYCH OSOBOWYCH

W kontekście stosowania przepisów Rozporządzenia 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 (ogólne rozporządzenie o ochronie danych) (RODO)

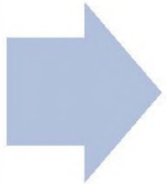
SZKOLENIE WEWNĘTRZNE

Podstawa prawna:

1. **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. – ogólne rozporządzenie o ochronie danych osobowych - określa wymagania do ochrony danych osobowych

2. Ustawa z dnia 10 maja 2018r. o ochronie danych osobowych (Dz. U. poz. 1000)

POCZĄTEK OBOWIĄZYWANIA RODO



25 MAJA 2018r.

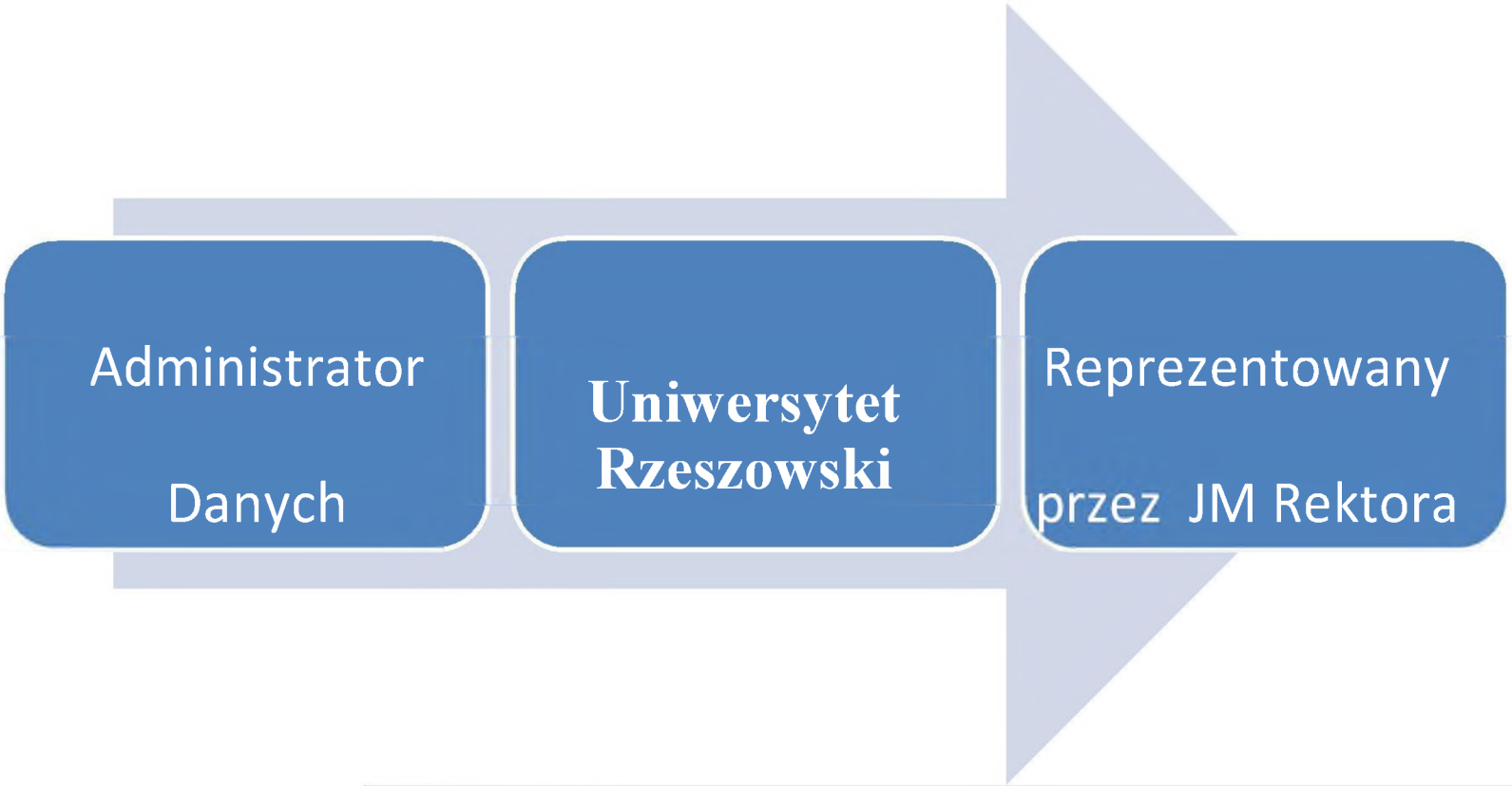
Istota i cele RODO:

- akt prawny obowiązujący we wszystkich Państwach Członkowskich Unii Europejskiej,
- lepsza ochrona danych w dobie postępu technologicznego i globalizacji,
- ujednolicenie przepisów we wszystkich krajach członkowskich UE oraz zapewnienie swobodnego przepływu danych osobowych między tymi państwami,

Urząd
Ochrony
Danych
Osobowych

Organem nadzorczym w sprawach przestrzegania przepisów RODO oraz ustawy o ochronie danych osobowych jest **Urząd Ochrony Danych Osobowych (UODO)**.

Administrator (danych) (art.4.7 RODO) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych.



Inspektor Ochrony Danych (IOD) art.37,38,39 RODO – osoba wyznaczona przez administratora w celu informowania i doradzania administratorowi, podmiotowi przetwarzającemu oraz pracownikom w zakresie obowiązującego prawa oraz wewnętrznych regulacji w zakresie ochrony danych, a także w celu monitorowania ich przestrzegania.

Inspektor pełni także funkcję punktu kontaktowego dla osób, których dane są przetwarzane w uczelni oraz dla organu nadzorczego.

Administrator Systemów Informatycznych – osoba wyznaczona przez administratora w celu zapewnienia prawidłowego funkcjonowania systemów informatycznych.

Lokalny Administrator Danych Osobowych (LADO) – osoba kierująca jednostką organizacyjną uczelni.

Lokalny Administrator Systemów Informatycznych (LASI) – osoba odpowiedzialna za realizację zadań administratora danych osobowych w systemach informatycznych, określonych w RODO, w danej jednostce organizacyjnej .

Podmiot danych – osoba fizyczna, której dane są przetwarzane.

Podmiot przetwarzający (Procesor) (art.4.8 RODO) – osoba fizyczna lub prawna, organ publiczny lub jakikolwiek inny organ przetwarzający dane osobowe w imieniu administratora.

Dane osobowe (art.4.1 RODO) – informacje, które pozwalają bezpośrednio lub pośrednio zidentyfikować osobę fizyczną, w szczególności na podstawie jej imienia i nazwiska, numeru identyfikacyjnego, danych o lokalizacji, identyfikatora internetowego lub jednego bądź kilku szczególnych czynników określających jej cechy fizyczne, fizjologiczne, genetyczne, psychiczne, ekonomiczne, kulturowe lub społeczne, np.

- Imię, nazwisko, adres korespondencji/telefon
- Imię, nazwisko, numer dokumentu tożsamości
- Imię, nazwisko, numer konta bankowego
- Pesel
- Dane o lokalizacji
- Monitoring, zapisy rozmów
- Maile

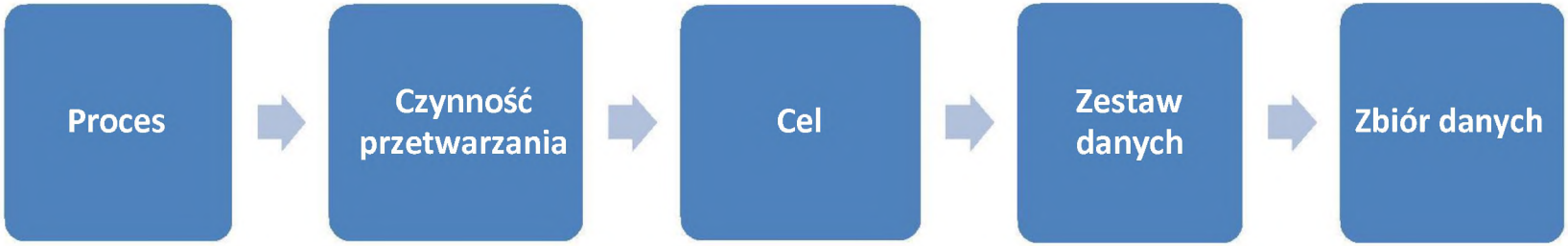
Szczególne kategorie danych osobowych (art.9 RODO) – są to następujące kategorie danych:

- stan zdrowia fizycznego i psychicznego, np. dane medyczne, stopień niepełnosprawności, dysleksja, dane z ZFŚS
- dane genetyczne, np. DNA, próbki biologiczne
- dane biometryczne, np. wizerunek, dane daktyloskopijne, głos
- wyroki skazujące i naruszenia prawa, np. zaświadczenie o niekaralności
- pochodzenie rasowe, etniczne
- poglądy polityczne, religijne i światopoglądowe
- przynależność do związków zawodowych
- orientacja seksualna

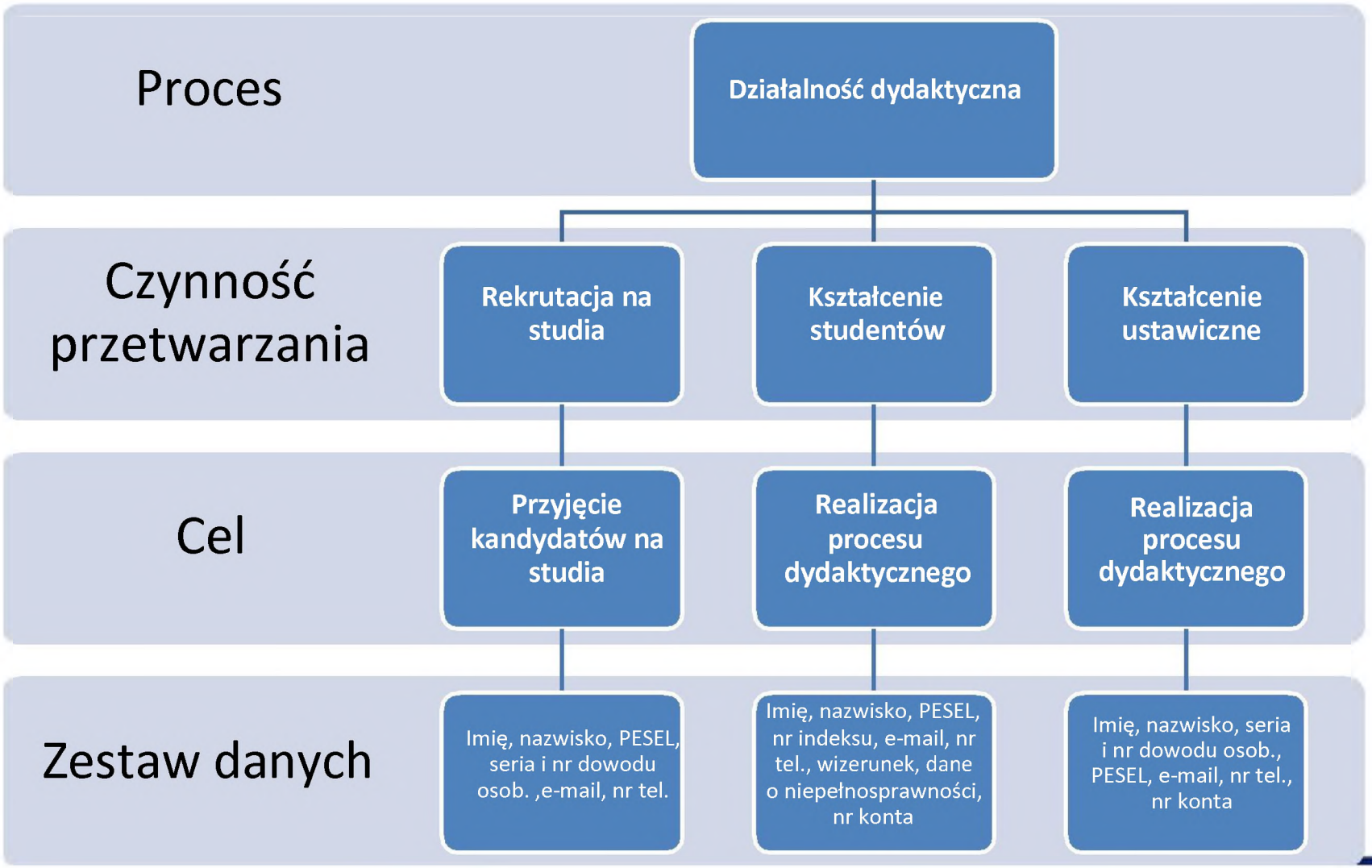
Przetwarzanie danych (art.4.2 RODO) – operacje wykonywane na danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak:

- zbieranie
- utrwalanie
- organizowanie
- porządkowanie
- przechowywanie
- adaptowanie
- modyfikowanie
- pobieranie
- przeglądanie
- wykorzystywanie
- ujawnianie
- przesyłanie
- rozpowszechnianie
- udostępnianie
- dopasowywanie
- łączenie
- ograniczanie
- usuwanie lub niszczenie

Przetwarzanie danych osobowych odbywa się w ramach procesów, które dzielą się na czynności przetwarzania wykonywane w określonym celu. Przetwarzany jest zestaw danych, który następnie zostaje uporządkowany i przechowywany w formie zbioru danych.



Przykład:


Proces
Działalność dydaktyczna
Czynność przetwarzania
Rekrutacja na studia
Kształcenie studentów
Kształcenie ustawiczne
Cel
Przyjęcie kandydatów na studia
Realizacja procesu dydaktycznego
Realizacja procesu dydaktycznego
Zestaw danych
Imię, nazwisko, PESEL, seria i nr dowodu osob. ,e-mail, nr tel.
Imię, nazwisko, PESEL, nr indeksu, e-mail, nr tel., wizerunek, dane o niepełnosprawności, nr konta
Imię, nazwisko, seria i nr dowodu osob., PESEL, e-mail, nr tel., nr konta

Zbiór danych – jest to uporządkowany zestaw danych dostępnych według określonych kryteriów.

Forma papierowa	• akta osobowe • teczki • dokumenty
Forma elektroniczna	• Programy, systemy informatyczne • pliki • foldery
Zapisy rejestratora	• zapisy monitoringu • rejestry rozmów

Główne zasady dotyczące przetwarzania danych osobowych (art.5.1 RODO)

1. ZGODNOŚĆ Z PRAWEM, RZETELNOŚĆ, PRZEJRZYSTOŚĆ
2. OGRANICZENIE CELU
3. MINIMALIZACJA DANYCH – ADEKWATNOŚĆ
4. PRAWIDŁOWOŚĆ
5. OGRANICZENIE PRZECHOWYWANIA
6. INTEGRALNOŚĆ I POUFNOŚĆ
7. ROZLICZALNOŚĆ

1. ZGODNOŚĆ Z PRAWEM, RZETELNOŚĆ, PRZEJRZYSTOŚĆ (art.5.1a RODO)

Przetwarzanie danych osobowych musi być zgodne z prawem, rzetelne i przejrzyste dla osoby, której dane dotyczą.

W tym celu Administrator danych ma obowiązek:

- zapewnić podstawę legalności przetwarzania *(art. 6, 9)*
- wykonać obowiązek informacyjny *(art. 13, 14)*
- rejestrować czynności przetwarzania *(art. 30)*

Zapewnienie legalności przetwarzania (art.6 RODO):

- osoba, której dane dotyczą wyraziła **ZGODĘ**

  Zgoda osoby – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli osoby w formie oświadczenia lub wyraźnego działania potwierdzającego *(złożenie podpisu, potwierdzenie mailowe, zaznaczenie checkboxa na formularzu internetowym).*

  Osoba, której dane dotyczą ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody musi być równie łatwe, jak jej wyrażenie.

- 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 *(**umowa: zlecenie, wykładu**, forma zatrudnienia, dostawa)*

- jest niezbędne do wypełnienia **OBOWIĄZKU PRAWNEGO** *(Kodeks Pracy, Ustawa o szkolnictwie wyższym, Ustawa o archiwach)*

- jest niezbędne do ochrony **ŻYWOTNYCH INTERESÓW** osoby, której dane dotyczą lub innej osoby fizycznej (*klęski żywiołowe, powiadomienie osoby w kryzysowej sytuacji)*

- jest niezbędne do wykonania zadania realizowanego w **INTERESIE PUBLICZNYM** *(działalność fundacji,* ***stowarzyszeń****, zrzeszeń zawodowych, instytucji zdrowia publicznego,* ***ochrony socjalnej****, opieki zdrowotnej, instytucji 500+)*

- jest niezbędne dla wypełnienia **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 *(****marketing bezpośredni****, windykacja, rejestr korespondencyjny, rejestr wejść,* ***monitoring****, obsługa klienta, współpracownicy)*

2. OGRANICZENIE CELU – zasada adekwatności i celowości (art.5.1b RODO)

Dane osobowe mogą być zbierane tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach i przetwarzane tylko zgodnie z tymi celami. Nie wolno przetwarzać danych w celach innych niż pierwotne.

Dalsze przetwarzanie możliwe jest tylko do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych.

3. MINIMALIZACJA DANYCH (art. 5.1c RODO)

Dane osobowe muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane.

Wolno zbierać tylko te dane, które są rzeczywiście niezbędne do realizacji celu, w którym są przetwarzane (minimalną ilość danych).

4. **PRAWIDŁOWOŚĆ** (art.5.1d RODO)

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane.

Dane, które są nieprawidłowe/nieaktualne powinny zostać niezwłocznie usunięte lub sprostowane.

5. OGRANICZENIE PRZECHOWANIA (art.5.1e RODO)

Dane osobowe muszą być przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane. Po tym okresie dane należy usunąć.

Dane można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych, do celów badań naukowych lub historycznych lub do celów statystycznych.

6. INTEGRALNOŚĆ I POUFNOŚĆ (art.5.1f RODO)

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

Przetwarzanie danych tylko z upoważnieniami (art.29 RODO)

Każda osoba upoważniona może przetwarzać dane osobowe wyłącznie na polecenie administratora lub na podstawie przepisu prawa.

Administrator danych nadaje odpowiednie **Upoważnienia do przetwarzania danych osobowych** (*w zbiorach papierowych, systemach informatycznych wynikającym z zakresu obowiązków*) po odbyciu szkolenia z zakresu ochrony danych osobowych oraz złożeniu oświadczenia o zachowaniu poufności.

Bez stosownego Upoważnienia przetwarzanie danych odbywa się w sposób niezgodny z prawem!

7. **ROZLICZALNOŚĆ** (art.5.2 RODO)

Administrator danych jest odpowiedzialny za przestrzeganie przepisów dotyczących ochrony danych osobowych oraz musi być w stanie wykazać ich przestrzeganie, poprzez wdrożenie wewnętrznych mechanizmów i procedur.

Obowiązek informacyjny (art.13 RODO)

W przypadku zbierania danych osobowych od osoby, której dane dotyczą, administrator danych jest zobowiązany poinformować tę osobę o tym:

- kto jest administratorem jej danych
- jakie są dane kontaktowe Inspektora Ochrony Danych
- jaki jest cel przetwarzania jej danych wraz z podstawą prawną
- czy istnieją odbiorcy jej danych
- zamiar przekazania danych osobowych do państwa trzeciego

- jaki jest okres, przez który dane osobowe będą przechowywane
- prawie dostępu do swoich danych, ich poprawiania, usunięcia, ograniczenia przetwarzania, wniesienia sprzeciwu wobec przetwarzania oraz przenoszenia danych
- prawie do cofnięcia zgody na przetwarzanie danych w dowolnym momencie
- prawie wniesienia skargi do Urzędu Ochrony Danych Osobowych (UODO)
- czy ma obowiązek podania danych, z czego to wynika i jakie są ewentualne konsekwencje ich niepodania
- czy dane będą profilowane, na jakich zasadach i jakie będą tego skutki dla osoby, której dane dotyczą

Prawo do usunięcia danych „prawo do bycia zapomnianym” (art.17 RODO)

Osoba, której dane dotyczą ma prawo żądać niezwłocznego usunięcia jej danych, jeżeli:

- dane nie są już niezbędne do celów, w których zostały zebrane
- cofnęła zgodę i nie ma innej podstawy prawnej przetwarzania
- wnosi sprzeciw wobec przetwarzania
- dane osobowe były przetwarzane niezgodnie z prawem
- dane muszą zostać usunięte z obowiązku wynikającego z przepisów prawa
- dane zostały zebrane w związku z oferowaniem usług komercyjnych

Prawo do przenoszenia danych (art.20 RODO)

Osoba, której dane dotyczą ma prawo otrzymać od administratora sformatowany dokument/plik ze swoimi danymi oraz ma prawo przesłać te dane innemu administratorowi lub zażądać by administrator przesłał je bezpośrednio innemu administratorowi.

Przenoszenie danych możliwe jest jeżeli przetwarzanie odbywa się na podstawie zgody lub na podstawie umowy lub w sposób zautomatyzowany, np. przeniesienie danych z banku do banku, od jednego operatora sieci do innego.

Profilowanie (art.22 RODO) – dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych do oceny, analizy i prognozy sytuacji materialnej, stanu zdrowia, preferencji, zainteresowań, lokalizacji przemieszczania się i wywołuje skutki prawne wobec tej osoby lub w podobny sposób istotnie na nią wpływa.

Osoba, której dane dotyczą ma prawo nie wyrazić zgody na profilowanie.

Przykłady profilowania:

- *automatyczna ocena ryzyka kredytowego lub składki ubezpieczeniowej*
- *śledzenie lokalizacji za pomocą aplikacji mobilnych, programy lojalnościowe*
- *reklama behawioralna*
- *śledzenie ruchu, treści w Internecie*

Naruszenie ochrony danych osobowych – przypadkowy lub niezgodny z prawem incydent tj.:

ZNISZCZENIE, UTRACENIE, ZMODYFIKOWANIE	• awaria • wirus • błąd ludzki
NIEUPRAWNIONE UJAWNIENIE	• wyrzucenie na śmietnik • wyciek danych
NIELEGALNY DOSTĘP	• kradzież danych

Zgodnie z art.33 RODO wszelkie incydenty naruszające prawa i wolności osób należy zgłaszać do UODO **w ciągu 72 godzin** *(sfałszowanie danych, utrata kontroli nad własnymi danymi osobowymi*).

Jeżeli skutki incydentu mogą powodować wysokie ryzyko naruszenia praw lub wolności osoby fizycznej, należy ją o tym poinformować.

Administrator ma obowiązek prowadzenia wewnętrznej rejestracji incydentów.

Zgodnie z art.35 RODO, w celu zastosowania adekwatnych środków zabezpieczających właściwe przetwarzanie danych osobowych administrator przeprowadza **ocenę skutków.**

Zawiera ona:

1. Opis czynności przetwarzania - identyfikacja procesów i czynności przetwarzania, określa m.in. *kategorie danych podlegające przetwarzaniu, cele, odbiorów danych, aktywa służące do przetwarzania,*
2. Ocenę zgodności z przepisami RODO,

3. Analizę ryzyka:
    - Wyznaczenie zagrożeń
    - Wyliczenie ryzyka – określenie prawdopodobieństwa wystąpienia poszczególnych zagrożeń
    - Porównanie wyliczonego ryzyka ze skalą
    - Planowana reakcja na wartość ryzyka
    - Ponowna analiza
4. Plan postępowania z ryzykiem


Postępowanie z ryzykiem
Ryzyko akceptowalne
Ryzyko opcjonalne (akceptujemy lub obniżamy)
Ryzyka nie akceptujemy i obniżamy

W celu obniżenia ryzyka oraz uniknięcia naruszeń ochrony danych osobowych administrator wdraża następujące środki techniczne i organizacyjne:

1. Zabezpieczenia organizacyjne
2. Zabezpieczenia fizyczne
3. Zabezpieczenia techniczne
4. Zabezpieczenia informatyczne
5. Zabezpieczenia zewnętrzne

ZABEZPIECZENIA ORGANIZACYJNE

- **PROCEDURY** – Polityka Bezpieczeństwa, Regulamin ochrony danych osobowych, Zarządzanie Upoważnieniami
- **SZKOLENIA**
- **AUDYTY**

ZABEZPIECZENIA FIZYCZNE

Zapewnienie ochrony pomieszczeń, infrastruktury i sprzętów poprzez zastosowanie m.in.

- Polityki kluczy
- Fizycznej kontroli dostępu – system kart wejściowych, system biometryczny, portiernia
- Polityki czystego biurka

ZABEZPIECZENIA TECHNICZNE

- System przeciwpożarowy – czujniki dymu, system gaszenia
- Monitoring środowiskowy – czujniki wilgotności, czujnik temperaturowy
- Klimatyzacja w serwerowni
- Monitoring wizyjny
- Systemy UPS/ agregaty prądotwórcze

ZABEZPIECZENIA INFORMATYCZNE –zapewniają ochronę danych osobowych przetwarzanych w systemach informatycznych:

- Programy antywirusowe, antyspamowe, bramki filtrujące
- Szyfrowanie danych
- Tworzenie kopii zapasowych
- Polityka haseł
- Polityka czystego ekranu (zahasłowane wygaszacze, ustawienia monitora)
- Zakaz kopiowania i instalowania niezatwierdzonego oprogramowania z Internetu
- Zakaz włączania opcji autouzupełniania i zapamiętywania haseł

ZABEZPIECZENIA INFORMATYCZNE

- Korzystając z poczty elektronicznej, celach służbowych, należy udostępniać i wykorzystywać tylko uczelniany **adres konta pocztowego**.

- Nie należy otwierać podejrzanych załączników i linków.
- Należy unikać pracy w otwartych sieciach WI-FI.
- Komputery przenośne należy przewozić w bagażniku.
- Po zakończeniu pracy należy **wylogować** się ze wszystkich systemów, z których korzystaliśmy.
- Każdy użytkownik pracuje na własnym koncie (identyfikatorze).

ZABEZPIECZENIA ZEWNĘTRZNE

Procedury dostępu podmiotów zewnętrznych:

- umowa/klauzula poufności sporządzana dla podmiotów zewnętrznych posiadających dostęp do danych osobowych na terenie organizacji,

- umowa powierzenia przetwarzania danych podpisywana z podmiotami, które przetwarzają dane osobowe „na zewnątrz” w formie outsourcingu.

Kary (art.83 RODO)

KARY do 10 mln. EUR, a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu za naruszenia w zakresie przetwarzania danych osobowych.

KARY do 20 mln. EUR, a w przypadku przedsiębiorstwa – w wysokości do 4% jego całkowitego rocznego światowego obrotu za naruszenia w zakresie przetwarzania szczególnych kategorii danych. **KARY do 100 000 PLN** dla podmiotów publicznych za naruszenia w zakresie przetwarzania danych osobowych.

KARY do 100 000 PLN dla podmiotów publicznych za naruszenia w zakresie przetwarzania szczególnych kategorii danych osobowych.

UWAGA!

Zgodnie z art. 82.1 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkowa w wyniku naruszenia ochrony jej danych, ma prawo uzyskać od administratora lub podmiotu przetwarzającego **odszkodowanie** za poniesioną szkodę.

Normy prawne związane z **bezpieczeństwem informacji** zawarte są również w niewymienionych tutaj aktach prawnych. Przepisy szczegółowe można odnaleźć także w **Kodeksach**: Cywilnym, Karnym, Postępowania Administracyjnego, oraz **przepisach regulujących poszczególne działy prawa** jak np. prawo zamówień publicznych, prawo telekomunikacyjne etc. Bogatym źródłem wiedzy w tym zakresie jest również wykładnia przepisów, instrukcje i zalecenia wydawane przez właściwe merytorycznie Ministerstwo.

W przypadku wątpliwości co do stosowania, bądź właściwego zachowania zapewniającego właściwe bezpieczeństwo informacji można zwrócić się o pomoc do

Inspektora Ochrony Danych Uniwersytetu Rzeszowskiego

mgr Krystian Antochów

ul. Cicha 4/2

+48 17 872 34 39

+48 17 872 36 46

iod@ur.edu.pl