



# Ochrona danych osobowych u beneficjentów

## Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020 w świetle przepisów Rozporządzenia Ogólnego o Ochronie Danych Osobowych (RODO)

Wykładowca: Maciej Kołodziej

*Łódź, 9 listopada 2017*



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne





# Agenda cz.1

Rejestracja; Sprawy organizacyjne;

Wprowadzenie do ochrony danych osobowych

Zbiory danych; Proces ochrony danych i jego rozliczalność; Szkolenia

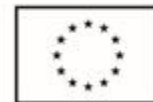
Wymagania techniczno-organizacyjno-formalne;  
Wdrażanie zabezpieczeń; Przetwarzanie danych kadrowych, podwykonawców i klientów



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Agenda cz.2

Powierzanie danych osobowych do przetwarzania;  
Zgłaszanie Organowi Nadzorcemu naruszeń ochrony  
danych; Odpowiedzialność prawna; Kontrola

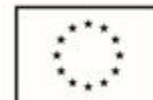
Monitorowanie stanu ochrony danych osobowych;  
Sprawdzenie nabytej wiedzy; Pytania, uwagi, wnioski



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne

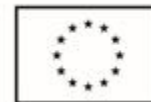


Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Agenda – sesja nr 1

- Sprawy organizacyjne
- Podsumowanie aktualnie obowiązujących regulacji UODO, RTO, KRI
- Wprowadzenie do RODO, nowej UODO i zmian w przepisach krajowych
- Podstawowe terminy oraz zasady przetwarzania danych osobowych i ochrony prywatności podmiotów danych
- Różnice i podobieństwa pomiędzy ABI i IOD





# Źródła wymagań dotyczących bezpieczeństwa informacji

## Konstytucja RP

art. 47

art. 51

## Ustawa o ochronie danych osobowych

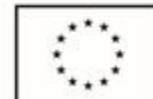
art. 1



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Źródła wymagań dotyczących bezpieczeństwa informacji

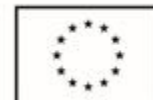
- Ustawa o ochronie danych osobowych
- Rozporządzenie w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych
- Rozporządzenia wykonawcze MAiC



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# 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 wydane na podstawie art. 18 ustawy o informatyzacji działalności podmiotów realizujących zadania publiczne

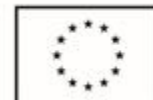
System Zarządzania Bezpieczeństwem Informacji w KRI



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Inne przepisy i regulacje cz.1

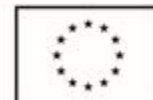
- Ustawy samorządowe (województwo, gmina, powiat)
- Przepisy szczególne w administracji publicznej (np. Centra Usług Wspólnych)
- Ustawa Prawo Pracy (art. 22<sup>1</sup>)
- Ustawa o ochronie informacji niejawnych
- Ustawa Prawo zamówień publicznych
- Ustawa o dostępie do informacji publicznej {o *jawności życia publicznego*}
- Ustawa o świadczeniu usług drogą elektroniczną (art.9-10, 16-22) {*ePrivacy*}



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





## Inne przepisy i regulacje cz.2

- 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, ...
- Wytyczne Grupy artykułu 29





# Źródła wymagań dotyczących bezpieczeństwa informacji - Normy ISO

grupa norm z serii 27000 - Bezpieczeństwo Informacji

PN-ISO/IEC 20000-1,-2 - zarządzanie usługami

PN-ISO/IEC 29100 - ramy prywatności, ochrona danych identyfikujących osobę (PII)

ISO/IEC 29134:2017 - „Guidelines for privacy impact assessment” – ocena skutków

PN-ISO/IEC 24762 - odtwarzanie w ramach ciągłości działania

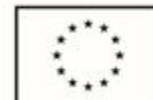
PN-ISO 31000 - wytyczne dotyczące zarządzania ryzykiem i techniki oceny ryzyka



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Źródła wymagań dotyczących bezpieczeństwa informacji

## Informacje prawnie chronione

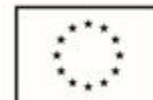
- Tajemnice zawodowe,
- Tajemnice przedsiębiorstwa, pracodawcy,
- Tajemnica pracownika samorządowego,
- Tajemnica skarbową,
- Informacje niejawne



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



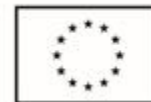
Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Źródła wymagań dotyczących bezpieczeństwa informacji

## Regulacje wewnętrzne

- Polityka Bezpieczeństwa Danych Osobowych
- Instrukcja zarządzania systemem informatycznym służącym do przetwarzania danych osobowych
- Instrukcja postępowania 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

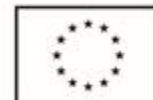
RODO Rozporządzenie o Ochronie Danych Osobowych  
GDPR General Data Protection Regulation



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Proces ochrony danych osobowych

prawa osób których dane przetwarzamy  
przykłady z RODO cz.1

- Prawo do dostępu do zebranych danych osobowych
- Prawo do wiedzy i informacji o założeniach ewentualnego zautomatyzowanego przetwarzania danych
- Prawo do wiedzy i informacji o profilowaniu
- Prawo do wiedzy i informacji o konsekwencjach profilowania
- Prawo do wiedzy i informacji





# Proces ochrony danych osobowych

prawa osób których dane przetwarzamy  
przykłady z RODO cz.2

- 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
- Prawo do usunięcia danych (wewnątrz struktur administratora danych)





## Dane osobowe

### UODO:

**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**

### RODO:

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







# Administrator Danych Osobowych w UODO

Administrator Danych

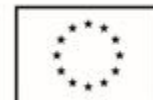
(organ, jednostka organizacyjna, podmiot lub osoba, ..., decydujące o celach i środkach przetwarzania danych osobowych)



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Administrator i inni w RODO

„Administrator” ustala cele i sposoby przetwarzania danych osobowych;

„Współadministrator” Jeżeli co najmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania,

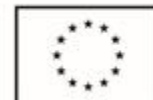
„Podmiot przetwarzający” (potocznie „procesor”) przetwarza dane osobowe w imieniu administratora;



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Przetwarzanie danych osobowych

UODO:

jakiegokolwiek 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:

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych





# Jak przetwarzać dane osobowe ?

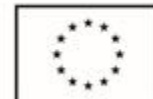
- Zasada legalności
- Zasada celowości
- Zasada merytorycznej poprawności
- Zasada adekwatności
- Zasada ograniczenia czasowego



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Podstawy przetwarzania danych osobowych

## UODO

- Art. 23 1. osoba, wyrazi na to zgodę,
- 2. dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa;**
  3. konieczne do realizacji umowy
  - 4. niezbędne do wykonania określonych prawem zadań realizowanych dla dobra publicznego;**
  5. niezbędne dla prawnie usprawiedliwionych celów realizowanych przez administratorów danych





# Podstawy przetwarzania danych osobowych

## RODO

- Art. 6 1. a) osoba, wyraziła zgodę
- b) niezbędne do wykonania umowy,
- c) niezbędne do wypełnienia obowiązku prawnego;**
- d) niezbędne do ochrony żywotnych interesów osoby**
- e) niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej**
- f) niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora





# Usuwanie danych osobowych

UODO:

„anonimizacja” zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

RODO:

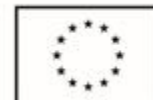
„pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie,



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Obowiązek informacyjny - UODO

Art. 24. 1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, administrator danych jest obowiązany poinformować tę osobę o:

- a) Adresie i nazwie,
- b) celu zbierania danych, o odbiorcach lub ich kategoriach
- c) prawie dostępu do treści danych oraz ich poprawiania;
- d) dobrowolności albo obowiązku podania danych, o jego podstawie prawnej.







# 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):





# Obowiązek informacyjny - RODO

Art. 13-14

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

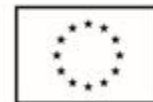
- podstawie prawnej przetwarzania,
- informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony
- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Administrator Bezpieczeństwa Informacji

*Ustawa o Ochronie Danych Osobowych (od 1.1.2015)*

- Powołanie ABI (art. 36a ust. 1)
- Zakres zadań ABI (art. 36a ust. 2)
- Wymagane kwalifikacje do pełnienia funkcji ABI (art. 36a ust. 5)
- Zapewnienie niezależności stanowiska ABI (art. 36a ust. 7 i 8)
- Rejestracja ABI przez GIODO (art. 46b)
- Rola ABI w kontroli GIODO (art. 19b)





# Powołanie ABI

Art. 36a ust. 1:

Administrator Danych Osobowych **może powołać** Administratora Bezpieczeństwa Informacji.

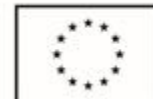
Administrator Danych może powołać zastępców Administratora Bezpieczeństwa Informacji (art. 36a ust. 6).



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Główne zadania ABI

### Zapewnianie przestrzegania przepisów o ochronie danych osobowych,

w szczególności przez: UODO art. 36a. 2. 1)

**a) sprawdzanie zgodności przetwarzania danych osobowych oraz opracowanie w tym zakresie sprawozdania dla administratora danych,**

**b) nadzorowanie opracowania i aktualizowania dokumentacji, oraz jej przestrzegania**

**c) zapewnianie zapoznania osób upoważnionych z przepisami o ochronie danych osobowych;**

**art. 36a 2. 2) prowadzenie rejestru zbiorów danych**





# Rozszerzenie zakresu zadań ABI

Art. 36a ust. 4 – zadania dodatkowe:

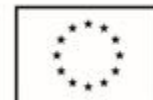
Administrator Danych Osobowych może powierzyć Administratorowi Bezpieczeństwa Informacji wykonywanie innych obowiązków, jeżeli nie naruszy to prawidłowego wykonywania zadań, o których mowa w art. 36a ust. 2.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Inspektor ochrony danych w RODO

Rozdział 4 – Administrator (danych osobowych) i podmiot przetwarzający (procesor)

Sekcja 4: IOD - Inspektor Ochrony Danych  
(DPO - Data Protection Officer):

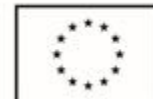
- Wyznaczenie Inspektora art. 37
- Status Inspektora art. 38
- Zadania Inspektora art. 39



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Wyznaczenie Inspektora

*sekcja IV artykuł 37*

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

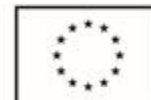
1.a) przez podmiot lub organ publiczny, z wyłączeniem sądów w ramach prowadzonych przez nie postępowań



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Wyznaczenie Inspektora

sekcja IV artykuł 37

**UWAGA:**

Należy dokonać analizy w kontekście obowiązkowego powołania IOD w sytuacji gdy przedsiębiorca wykonuje usługi związane z przetwarzaniem danych jako podmiot przetwarzający dla podmiotów lub organów publicznych.

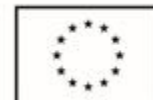
Grupa art. 29 w wytycznych 16/EN WP243 dotyczących IOD rekomenduje, aby w spółkach publicznych (transport, media, drogi itp.) inspektor nie był obowiązkowy, a jedynie zalecany.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Wyznaczenie Inspektora

sekcja IV artykuł 37

## 3. Możliwość wyznaczenia jednego Inspektora dla kilku podmiotów:

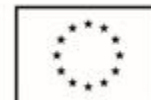
- Kilka organów lub podmiotów publicznych może wyznaczyć jednego Inspektora, uwzględniając przy tym ich wielkość i strukturę organizacyjną.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Status Inspektora

sekcja IV artykuł 38

3. Inspektor musi podlegać bezpośrednio pod najwyższe kierownictwo Administratora lub procesora i muszą zapewnić aby Inspektor był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

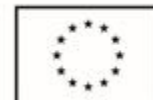
2. Administrator oraz procesor muszą wspierać Inspektora w wypełnianiu przez niego zadań,, zapewniając mu zasoby niezbędne do ich realizacji oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Status Inspektora

*sekcja IV artykuł 38*

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

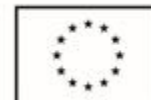
3. Inspektor nie będzie mógł być odwoływany ani karany za wypełnianie swoich zadań.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zadania Inspektora Ochrony Danych

sekcja IV artykuł 39

Zgodnie z art. 39 RODO Inspektor ma następujące zadania:

1.a) Informowanie o obowiązkach o ochronie danych i doradzanie

1.b) Monitorowanie przestrzegania RODO, innych przepisów UE oraz polityk, w dziedzinie ochrony danych, szkolenia oraz audyty.

1.c) Udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania

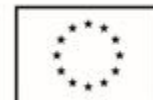
1.d) Współpraca i 1.e) Pełnienie punktu kontaktowego dla DPA



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zadania Inspektora Ochrony Danych

*sekcja IV artykuł 38*

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.



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Agenda – sesja nr 2

- Zbiory danych osobowych, ewidencja, zgłaszanie i nadzór w UODO oraz nowe obowiązki w RODO
- Proces ochrony danych z perspektywy:  
ADO, ABI/IOD, Operatorów i Podmiotów danych
- Szkolenia organizowane na zlecenie ADO.
- Rola ABI oraz IOD w procedurach szkoleniowych



# Rejestry zbiorów danych osobowych

Ustawa o ochronie danych osobowych

Ustawa definiuje dwa rodzaje rejestrów zbiorów danych:

1. **Ogólnokrajowy jawny rejestr zbiorów danych osobowych**, prowadzony w Biurze GIODO (art. 42 ust.1);

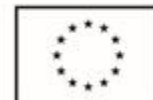
2. **Rejestry zbiorów danych prowadzone przez Administratorów Bezpieczeństwa Informatycznego** zgłoszonych do GIODO.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Obowiązki

Rejestracja zbiorów danych osobowych od 1.01.2015

Zbiory danych podzielone zostały dodatkowo według kryterium sposobu przetwarzania

- przetwarzane z użyciem systemów informatycznych,
- przetwarzane bez użycia systemów informatycznych.

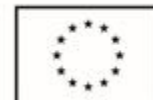
błędnie określane nazwą „zbiory papierowe”, ponieważ może to być też np. zbiory fotografii lub nagrań.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zadania ADO Rejestr czynności przetwarzania

*RODO sekcja IV artykuł 30*

1. Każdy administrator oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą rejestr czynności przetwarzania danych osobowych, za które odpowiadają.

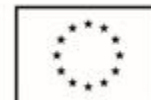
2. Każdy podmiot przetwarzający oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje:



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zadania Administratora (Danych)

RODO sekcja IV artykuł 30

## Rejestrowanie czynności przetwarzania

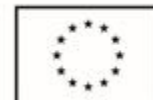
5. Obowiązki, o których mowa w ust. 1 i 2, nie mają zastosowania do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób, chyba że przetwarzanie, którego dokonują, może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategorie danych osobowych, o których mowa w art. 9 ust. 1, lub dane osobowe dotyczące wyroków skazujących i naruszeń prawa, o czym mowa w art. 10.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zapoznanie, uświadamianie, szkolenia

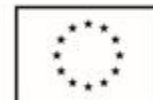
- RODO art. 39 1.a)
- UODO Art. 36a 2. 1) c)
- KRI § 20. 2. 6) a) b) c)
- ISO 27001 7.2.2



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Agenda – sesja nr 3

- Wymagania techniczno-organizacyjne
- Określenie wymogów formalnych
- Analiza ryzyka i odpowiedzialność Administratora w świetle RODO
- Wdrażanie zabezpieczeń technicznych i organizacyjnych
- Przetwarzanie danych kadrowych, podwykonawców i klientów (np. uczestników projektów)





# Wykaz zbiorów danych osobowych

Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r

ADO wdraża **Politykę bezpieczeństwa** (§ 4.):

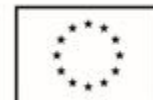
- 1) wykaz budynków,
- 2) **wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych;**
- 3) opis struktury zbiorów
- 4) sposób przepływu danych
- 5) wskazanie środków techniczno-organizacyjnych



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Dokumentacja systemu przetwarzania danych osobowych

- RODO Art. 24.2, Art. 30, Art. 33.5
- UODO Art. 36 2. Art. 36a 2. 1) b)
- KRI § 20. 2. 1)
- ISO 27001 pkt. 7.5

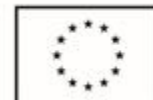
Realizacja: RTO § 4 i § 5 + kontrola wersji, integralność PBDO i IZSI (uprawnienia do edycji), a wgląd wewnątrz organizacji



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zadania Administratora

## Prowadzenie dokumentacji w RODO

Rozdział IV sekcja I artykuł 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,*

2. wdrożenie przez administratora odpowiednich polityk ochrony danych.

*3. Stosowanie zatwierdzonych kodeksów postępowania,*



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Analiza ryzyka

Art. 25 RODO **Uwzględnianie ochrony danych w fazie projektowania oraz domyślna ochrona danych.**

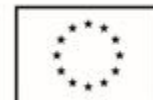
1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, **administrator** wdraża odpowiednie środki techniczne i organizacyjne,



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



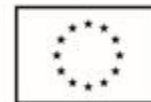
Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Analiza ryzyka w RODO wymagania

Sytuacje wskazane w RODO, gdy trzeba dokonać analizy ryzyka:

- Przy wdrażaniu przez ADO (procesora) „odpowiednich środków technicznych i organizacyjnych” (art. 25 i 32)
- Po wystąpieniu naruszenia (art. 33 i 34; motyw 85 i 86)
- Ocena skutków dla ochrony danych (art. 35) planowanych szczególnych operacji przetwarzania (motyw 84 i 90)





# Analiza ryzyka w RODO wymagania

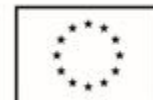
Art. 32 ust. 1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz **ryzyko naruszenia praw lub wolności osób fizycznych** o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki technicznej organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Analiza ryzyka w RODO

## Jak wykorzystać doświadczenia w kontekście RODO?

- Ustalenie kontekstu (RODO: ochrona praw i wolności osób)
- Identyfikowanie ryzyka, aktywów, zagrożeń, podatności, zabezpieczeń, następstw
- Analiza ryzyka, szacowanie następstw, prawdopodobieństwa naruszeń, ocena ryzyka
- Postępowanie z ryzykiem
- Monitorowanie ryzyka





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

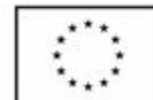
Administrator danych powinien określić wykaz stosowanych w organizacji środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzania danych. odpowiednie rozwiązania techniczne i organizacyjne



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne

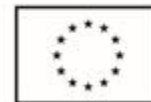


Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# 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





# Kopie zapasowe

- RT/O A. IV 3. 4. a) b)
- KRI § 20. 2. 9)
- ISO 27002 pkt. 12.3

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





# Kontrola dostępu

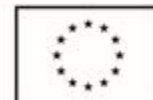
- Art. 39. 1. 1) 2) 3)
- RT/O zał. część A. II, IV ust. 1. i 2, część B. VIII
- KRI § 20. 2. 4)
- ISO 27002 pkt. 9.4



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Poczta elektroniczna

dobre praktyki

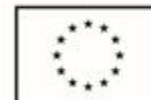
- Zasada działania poczty elektronicznej, przekazywanie informacji,
- Zabezpieczanie treści przesyłek,
- Zasady dotyczące obsługi załączników,
- Korzystanie z treści aktywnych i odsyłaczy do zasobów



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Gdzie i u kogo przechowywać dane ?

miejsca i sposób przetwarzania danych

Własna serwerownia

VS

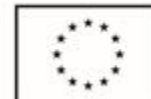
kolokacja, hoteling, hosting, hosting aplikacyjny,  
chmura obliczeniowa



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Bezpieczeństwo sprzętu i aktywów poza siedzibą

- RT/O A. VI
- KRI § 20. 2. 11)
- ISO 27002 pkt. 11.2.6, 11.2.7

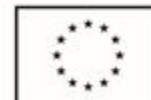
Realizacja – np. autoryzacja wyniesienia sprzętu poza siedzibę; dziennik



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



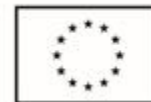
Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Urządzenia mobilne

- RT/O A. V
- KRI § 20. 2. 8)
- KRI § 20. 2. 11)
- ISO 27002 pkt. 6.2.1

Realizacja – wykaz urządzeń mobilnych;  
szyfrowanie dysków; zasady zdalnego dostępu do  
zasobów





# Ochrona przed szkodliwym oprogramowaniem

- RT/O A. III
- KRI – brak
- ISO 27002 pkt. 12.2



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Rozliczalność

- RODO
- UODO Art. 38.
- RT/O § 7
- KRI § 21. ust. 1. – 5.
- ISO 27002 pkt. 12.4



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# 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,



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Szyfrowanie danych

- RT/O C. XIII
- KRI § 20. 2. 12) d)
- ISO 27002 pkt. 10.1.1

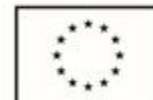
Realizacja: ujednoczenie zasad w organizacji;  
badanie wpływu szyfrowania na inne  
zabezpieczenia; HTTPS



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Sieci, usługi sieciowych, dostęp do zasobów

- RT/O C. XII 1. 2. a) b)
- KRI § 20. 2. 7) c)
- ISO 27002 pkt. 9.1.2

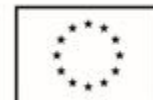
Realizacja: autoryzacja i monitorowanie dostępu do sieci (w tym bezprzewodowych) i usług; usługi VPN



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Bezpieczeństwo zasobów ludzkich

- UODO Art. 37.
- Art. 39. 2.
- ISO 27001 pkt. 7.1.2

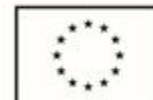
Realizacja – np. powiązanie zakresu upoważnienia z zakresem obowiązków pracownika lub opisem stanowiska, na którym został zatrudniony



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Bezpieczeństwo zasobów ludzkich Kadry/HR

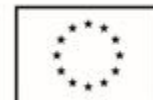
- Przed zatrudnieniem
- Podczas zatrudnienia
- Zakończenie lub zmiana zatrudnienia



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Umowa z pracownikiem/współpracownikiem

„Cykl życia” pracownika !

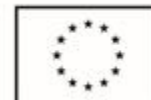
Podpisanie odpowiedniej wersji umowy  
Przygotowanie zasobów dla nowego stanowiska pracy  
Założenie kont np. w AD, systemach i aplikacjach  
Konfiguracja uprawnień  
Obiegówka przyjęcia pracownika  
Zmiany  
Obiegówka odejścia



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Rozwiązanie umowy

„Cykl życia” danych Użytkownika

Usunięcie konta ≠ usunięcie danych

Okresy przechowywania informacji

Odmowa usunięcia danych

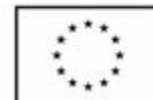
Odmowa udostępnienia informacji



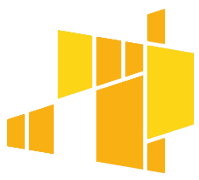
Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)

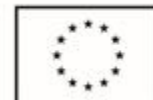


## Agenda – sesja nr 4

- Nowe zasady powierzania danych osobowych do przetwarzania. Wymagania stawiane przed Procesorem i Podprocesorami. Procedury kontrolne
- Nowy obowiązek zgłaszania przypadków naruszenia ochrony danych osobowych
- Odpowiedzialność i penalizacja w przepisach administracyjnych, karnych i cywilnych.
- Jak przygotować się na kontrolę

# Powierzenie przetwarzania danych osobowych

**Art. 31. 1. Administrator danych może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych.**





# Administrator i inni w RODO

## Relacja Administrator-Processor

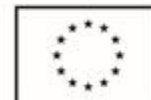
Administrator ma obowiązek korzystania wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi niniejszego rozporządzenia i chroniło prawa osób, których dane dotyczą (art.28 ust.1)



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Administrator i inni w RODO

## Relacja Administrator-Processor

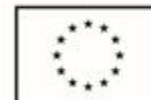
Podstawą przetwarzania ma być umowa, której treść została istotnie zmodyfikowana (art.28 ust.3 RODO) w stosunku do dotychczasowego stanu prawnego wynikającego z UODO, lub inny instrument prawny



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Administrator i inni w RODO

## Relacja Administrator-Processor

Komisja Europejska oraz Organ Nadzoru otrzymały kompetencje do wydawania standardowych klauzul umownych dotyczących relacji ADO – procesor

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

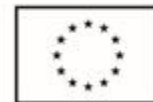
W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających (subprocesorów),



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Administrator i inni w RODO

## Relacja Processor-Subprocessor

Podpowierzenie danych – obowiązki i odpowiedzialność *procesora* (art.28 ust.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,





# Umowa powierzenia danych osobowych

## Obowiązki procesora (podprocesora) zależne od charakteru przetwarzania

Procesor powinien wdrożyć środki techniczne i organizacyjne mające na celu realizację obowiązku informacyjnego oraz praw osób:

- dostęp
- sprostowanie danych
- bycie zapomnianym
- ograniczenie przetwarzania
- przenoszenie danych
- sprzeciw

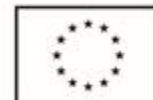




# Umowa powierzenia danych osobowych

**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
- b) zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
- c) podejmuje wszelkie środki wymagane na mocy art. 32
- d) przestrzega warunków korzystania z usług innego podmiotu przetwarzającego,





# 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.):

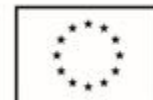
- e) f) pomaga administratorowi
- g) po zakończeniu świadczenia usług usuwa lub zwraca mu wszelkie dane osobowe;
- h) udostępnia administratorowi wszelkie informacje oraz umożliwia administratorowi przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# 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



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

*RODO sekcja II artykuł 33*

## Zadanie Administratora

Art.4 pkt 12

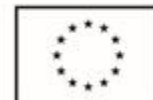
„naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych”



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)





# Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorcemu

*RODO sekcja II artykuł 33/34*

## Zgłaszanie naruszenia organowi nadzorcemu:

- W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza (art. 33 ust. 1)

## Zawiadomienia osób, których dane dotyczą:

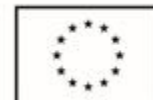
- Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. (art. 34 ust. 1)



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



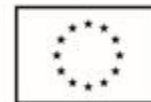
Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Penalizacja w UODO

## Naruszenie ustawy zagrożone karą:

- do 3 lat pozbawienia wolności
- do 2 lat pozbawienia wolności, ograniczenia wolności lub grzywny za:
- do roku pozbawienia wolności, ograniczenia wolności lub grzywny za:





# Penalizacja w RODO

## Odpowiedzialność za naruszenie przepisów o ochronie danych osobowych

Art.58 ust.2 Uprawnienia naprawcze Organu Nadzorczego:

- **wydawanie ostrzeżeń**
- **udzielanie upomnień**
- **nakazanie spełnienia żądania osoby**
- **nakazanie dostosowania operacji przetwarzania do przepisów**





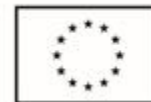
# Penalizacja w RODO

## Art.82 Prawo do odszkodowania i odpowiedzialność

1. Każda osoba która poniosła szkodę ma prawo uzyskać odszkodowanie

## Art.83 Kary pieniężne

nUODO Art. 83. 1. Na podmioty publiczne, o których mowa w art. 9 pkt 1 – 12 i 14 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych Prezes Urzędu może nałożyć, w drodze decyzji, administracyjne kary pieniężne w wysokości do 100tyś zł. Nałożenie kary spowoduje odpowiedzialność urzędnika za dyscyplinę finansów publ.





# Sprawdzanie zgodności, audyt wewnętrzny

- Art. 36a 2. 1) a) b)
- RT/O zał. część A. VII.
- KRI § 20. 2. 14).
- ISO 27001 pkt. 9.2

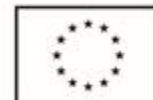
Realizacja: program audytów realizowany przez odpowiednich audytorów i odpowiednio dokumentowany, a wyniki sprawozdawane kierownictwu



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Wytyczne dla kontroli działania systemów teleinformatycznych używanych do realizacji zadań publicznych

Ministerstwo Cyfryzacji, z dnia 15 grudnia 2015 r.

## Zasady prowadzenia kontroli:

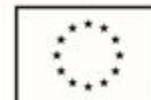
- 1. Cel kontroli**
- 2. Tryb kontroli**
- 3. Zespół kontrolny**



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Agenda – sesja nr 5

- Monitorowanie stanu ochrony danych osobowych u beneficjenta Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020  
zasady ogólne, dyskusja z uczestnikami szkolenia
- Sprawdzenie nabytej przez uczestników szkolenia wiedzy
- Pytania, uwagi, wnioski



# Przetwarzanie danych osobowych w urzędach

Nowa perspektywa finansowa 2014-2020

## Ustawa z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-20

**Art. 2. 1) beneficjent**

8) instytucja audytowa

9) instytucja pośrednicząca

10) instytucja wdrażająca

11) instytucja zarządzająca







# Kolejne kroki procesu zmian przepisów ODO

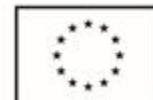
- Wytyczne Grupy Roboczej Art. 29
- Akty delegowane Komisji Europejskiej doprecyzowujące RODO
- Nowa polska ustawa dotycząca ochrony danych osobowych
- Zmiany sektorowe w krajowych przepisach szczególnych
- Interpretacje dotyczące nowych przepisów
- Kodeksy Dobrych Praktyk
- Certyfikacje



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Podsumowanie istotnych obowiązków z RODO

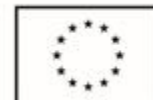
1. Organy i podmioty publiczne (zgodne z definicją formalną) mają obowiązek wyznaczenia Inspektora Ochrony Danych
2. Administracja musi działać ściśle według obowiązków i nakazów wynikających z przepisów prawa, w szczególności z zakresie techniczno-organizacyjnym obowiązuje ustawa o informatyzacji, rozporządzenie KRI i przepisy szczególne



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



## Podsumowanie istotnych obowiązków z RODO

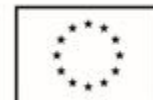
3. Podstawą przetwarzania DO, co do zasady jest przepis prawa, nie ma dobrowolności typu "może coś przetwarzać", skupia się tylko na "musi"
4. Nie ma możliwości korzystania z prawnie uzasadnionego interesu
5. Administracja może korzystać ze zgody, w przypadku niestandardowych aktywności o charakterze publicznym (np. konkursy dla mieszkańców)



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Podsumowanie istotnych obowiązków z RODO

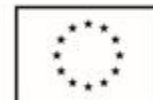
6. Brak jest swobody w określaniu celu i zakresu danych osobowych do przetwarzania (z wyj. inicjatyw specjalnych jw. 5.)
7. Kara pieniężna została ograniczona do ustalonej w przepisach granicy, co jednak nie wyklucza roszczeń cywilnych ze strony poszkodowanych podmiotów



Fundusze  
Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Podsumowanie istotnych obowiązków z RODO

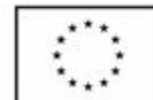
8. Obowiązują zasady należytej staranności przy wyborze podwykonawców, procesorów, w szczególności w zakresie oceny ryzyka oraz obowiązku wyznaczenia u nich IOD
9. Przy konstruowaniu SIWZ publiczny zamawiający powinien wziąć pod uwagę powierzenie przetwarzania, określić, jakie warunki ma spełniać, żeby wykazać zgodność z art. 28 ust. 1



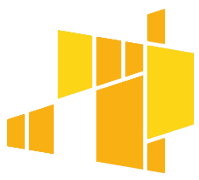
Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Bibliografia - wykaz najważniejszych źródeł

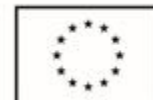
- „Ochrona danych osobowych w ramach funduszy europejskich dot. nowej perspektywy finansowej 2014-20”, M.Kołodziej, Urząd Marszałkowski, CE Compendium, Kraków, 11.2014
- „Bezpieczeństwo teleinformatyczne w jednostce samorządowej”, M.Kołodziej, SNTSW, Pabianice, 09.2016r.
- „Audyty ochrony danych osobowych”, 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
- Zestaw materiałów konferencyjnych z cyklu Forum Ochrony Danych Osobowych, Zarząd Stowarzyszenia ABI, SABI/Ariergarda, 2016-2017
- Materiały własne z ponad 50 szkoleń, warsztatów forów i konferencji, M.Kołodziej, lata 2015-2017



Fundusze Europejskie  
Program Regionalny



Unia Europejska  
Europejskie Fundusze  
Strukturalne i Inwestycyjne



Zmieniamy Łódzkie  
z Funduszami Europejskimi  
[www.rpo.lodzkie.pl](http://www.rpo.lodzkie.pl)



# Bibliografia - wykaz najważniejszych źródeł

- „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

