odoekspert

# Zarządzanie procesem dostosowawczym do unijnej reformy ochrony danych osobowych (GDPR / RODO)

mec. Jakub Wezgraj

**Warszawa, 10 maja 2017 r.**

# Czym będzie ta prezentacja?

- **Zestawem wskazówek, na co warto zwrócić uwagę przy dostosowywaniu organizacji do wymagań ogólnego rozporządzenia o ochronie danych (GDPR / RODO)**
- **Listą kluczowych zasad (przedstawionych w formie tez) z perspektywy osoby wdrażającej dedykowane rozwiązania z zakresu ochrony danych osobowych**
- **Propozycją podejścia do tej tematyki jako procesu, którym należy zarządzać z perspektywy całej organizacji (a nie wybranych działów/komórek organizacyjnych)**
- **Zachętą do podejścia racjonalnego, w oparciu o plan działania, a nie na fali doniesień medialnych i rynkowych**

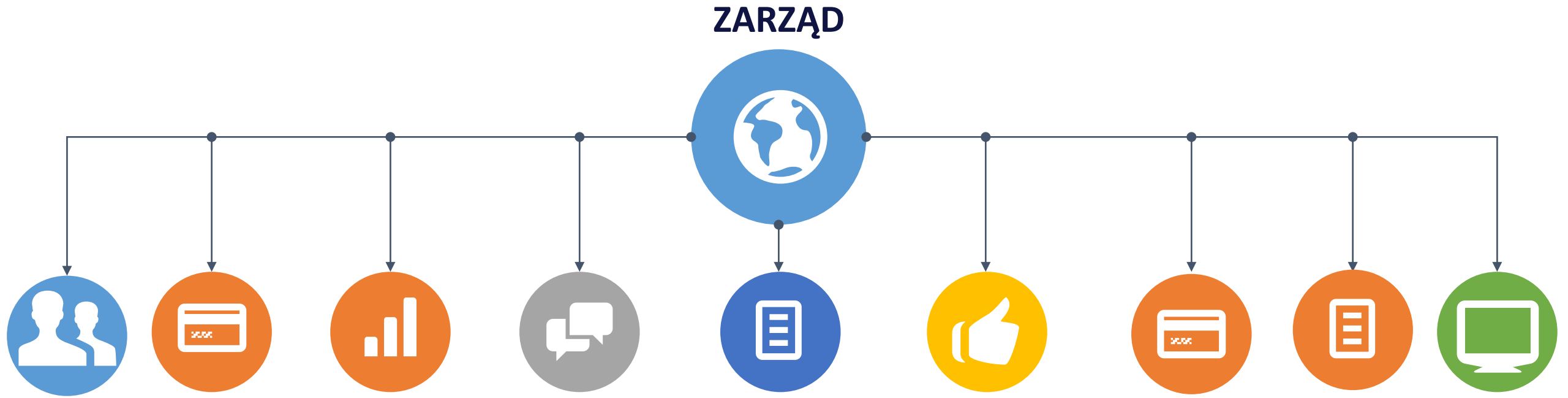
# Proces prawny
# – gdzie jesteśmy i dokąd zmierzamy?

# RODO TEZA #1

## Tylko i wyłącznie indywidualne podejście

- charakter, zakres, kontekst i cele przetwarzania danych oraz ryzyko naruszenia praw i wolności osób fizycznych w wyniku przetwarzania danych przez konkretną organizację

# Wyobraźmy sobie przykładową strukturę organizacyjną przykładowej firmy




DZIAŁ HR | FINANSE | KONTROLING | DZIAŁ HANDLU | BIURO ZARZĄDU | MARKETING | WINDYKACJA | DZIAŁ PRAWNY | DZIAŁ IT

odoekspert

## Moje pytanie brzmi:

- **Czy przedstawiony przykład struktury organizacji pokrywa się w 100% ze strukturą Państwa organizacji?**
- **Oczywiście, że nie bo nie ma czegoś takiego jak „przykładowa organizacja”**
- **I takie podejście widać również w RODO:**

***„W szczególności administrator powinien mieć obowiązek wdrożenia odpowiednich i skutecznych środków oraz powinien być w stanie wykazać, że czynności przetwarzania są zgodne z niniejszym rozporządzeniem oraz, że są skuteczne. Środki te powinny uwzględniać charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych”***

***Motyw 74 Preambuły***

# RODO TEZA #2

## Dział Prawny / Compliance oraz IT /Security to za mało

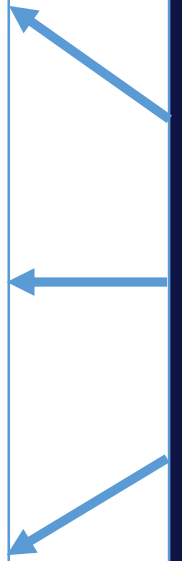
- potrzebne jest zaangażowanie praktycznie wszystkich komórek organizacyjnych (oczywiście na różnym poziomie)

# Perspektywa Działu IT

odoekspert

# Jak Dział IT postrzega inne komórki (na przykładzie Działu HR):

- Krytyczne systemy (np. Kadrowo – Płacowy) -> *BCM*
- Polityka backupow'a (archiwizacja i przechowywanie danych)
- Sprzęt informatyczny i zasoby (np. zasoby sieciowe)
- Dostępy (uprawnienia w systemach i zasobach,
- Stosowane środki bezpieczeństwa
- Help Desk
- Licencje
- Incydenty



**DZIAŁ HR**

**widziany**

**„oczami"**

**DZIAŁU IT**

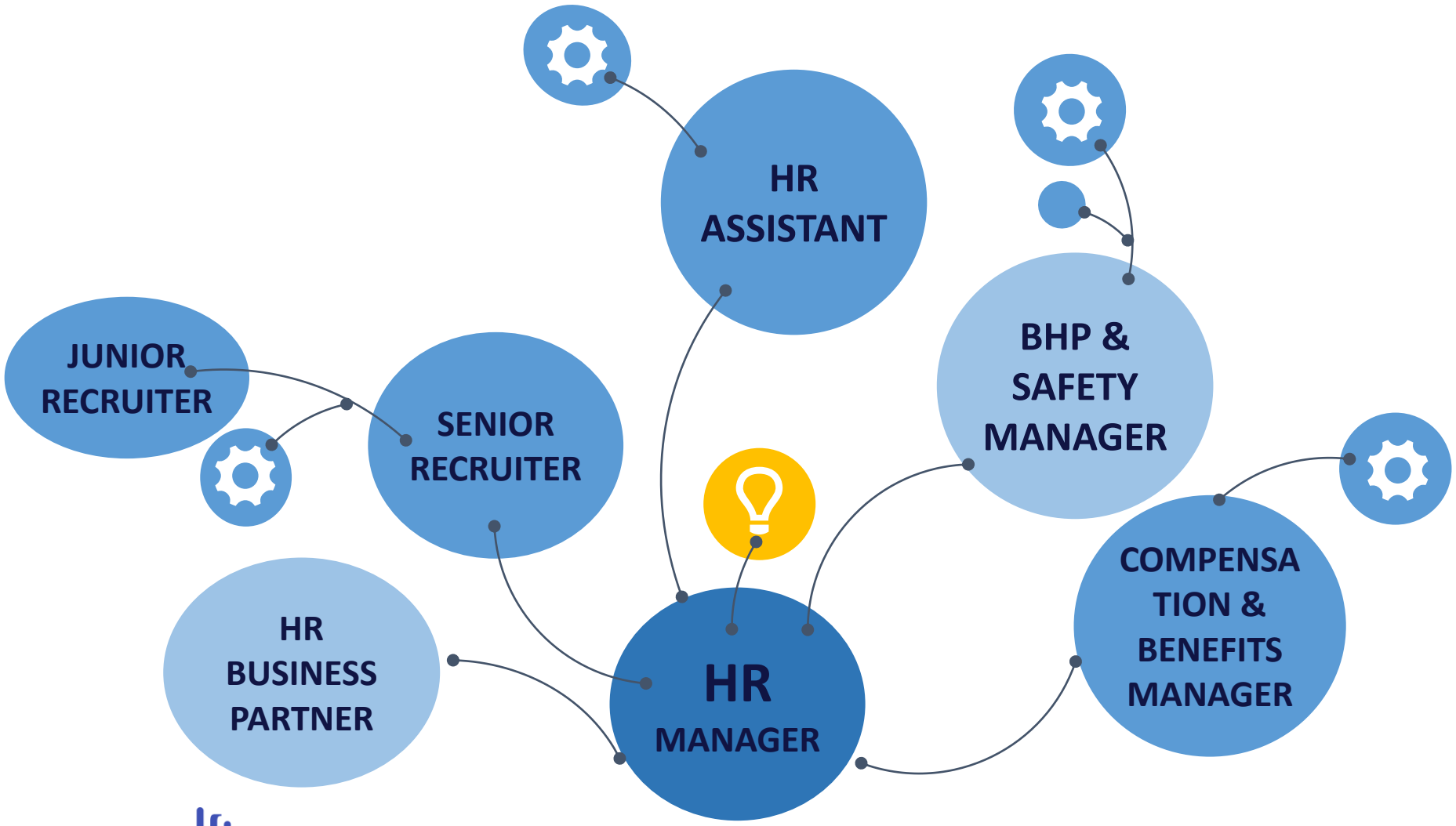
# Perspektywa Działu Prawnego

odoekspert

# Jak Dział Prawny postrzega inne komórki (na przykładzie Działu HR):

- Regulacje wewnętrzne (Regulaminy Pracy, Wynagrodzeń, ZFŚS)
- Wzory dokumentów (umowy o pracę, cywilnoprawne, zakazy konkurencji etc.)
- Współpraca z organami państwa (ZUS, US, organy ścigania)
- Postępowania sądowe (np. sprawy pracownicze)
- Uprawnienia pracownicze

# A JAK SAM DZIAŁ HR POSTRZEGA SIEBIE?




## WŁAŚCICIELE PROCESÓW

- Każdy odpowiada za określone procesy
- Jasno ustalone role i zakresy zadań w tych procesach

odoekspert

# RODO TEZA #3

## Potrzebne badanie w ujęciu „procesowym”

- procesy biznesowe i administracyjne związane z tematyką przetwarzania danych osobowych lub mające na nie wpływ
- „cykl życia danych” w organizacji

# Przykładowe procesy obsługiwane przez Dział HR

## Rekrutacja

- Decyzja o naborze
- Źródła poszukiwań i sposób wyboru
- Zewnętrzni dostawcy usług
- Co z dokumentami aplikacyjnymi niewybranych kandydatów?

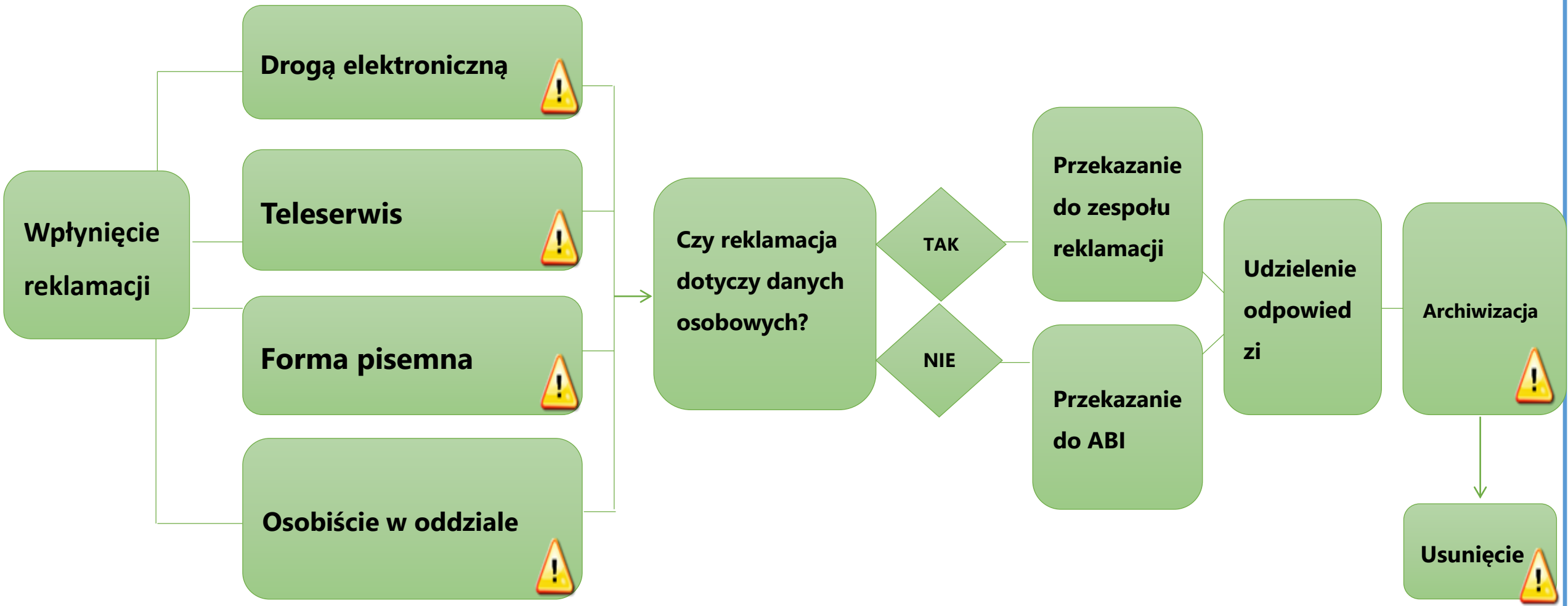
## Zatrudnienie

- Zakres dokumentów, które wypełnia nowy pracownik
- Przygotowanie do pracy na danym stanowisku
- Szkolenia wstępne

## Wsparcie etapu zatrudnienia

- Rozliczenia pracownicze
- Dodatkowe benefity / ubezpieczenia etc.
- ZFŚS
- Oceny okresowe i rozwój kompetencji
- Przypadki „szczególne” (np. monitoring, sygnaliści, badanie trzeźwości etc.)
- Udostępnianie danych pracowników (np. do innych podmiotów z Grupy kapitałowej)
- Wsparcie administracyjne (hotele, bilety lotnicze etc.)

# I jeszcze przykład „cyklu życia danych” z zupełnie innego obszaru - reklamacje



# RODO TEZA #4

## Potrzebny lider

- osoba zarządzająca procesem dostosowania organizacji do wymagań RODO

## Potrzebny lider, który:

- Zbierze „punkty widzenia” poszczególnych komórek organizacyjnych oraz posiadaną przez nie wiedzę
- Stworzy mapę procesów mających wpływ na ochronę danych osobowych na poziomie całej organizacji (a nie wyłącznie poszczególnych komórek organizacyjnych)
- Przypisze wymagania RODO do poszczególnych procesów
- Ustali, które wymagania RODO oraz w jakich przypadkach i na jakim poziomie mają zastosowanie wobec danej organizacji
- Zaproponuje konkretne rozwiązania
- Będzie koordynował ich implementację

odoekspert

# Inspektor Ochrony Danych

(art. 37 – 39 RODO)

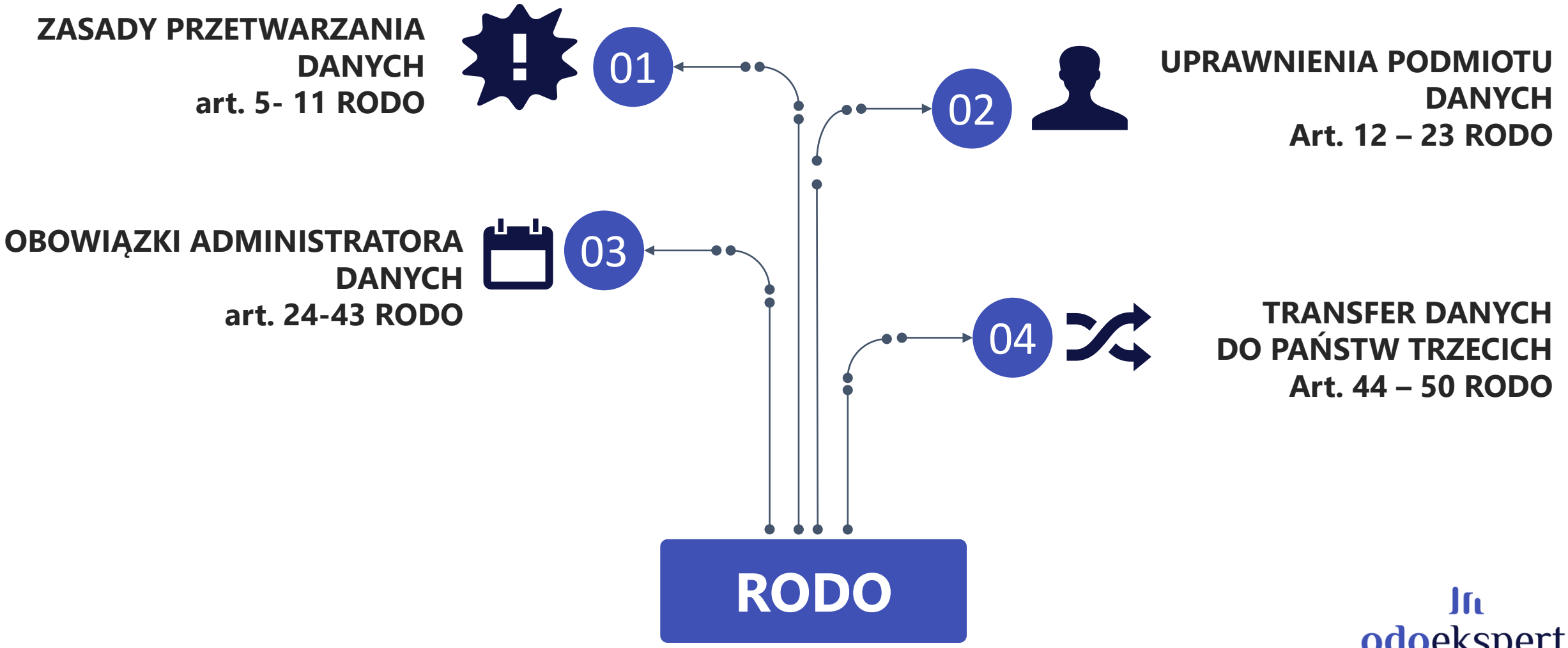
- **informowanie** administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, **o obowiązkach spoczywających na nich na mocy RODO** oraz innych przepisów Unii lub państw członkowskich o ochronie danych i **doradzanie im** w tej sprawie;
- **monitorowanie przestrzegania RODO** oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- udzielanie na żądanie **zaleceń co do oceny skutków dla ochrony danych** oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;
- współpraca z organem nadzorczym;
- pełnienie funkcji **punktu kontaktowego** dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

# RODO TEZA #5

## Nie wszystkie wymagania RODO będą musieli stosować wszyscy i na takim samym poziomie

- charakter, zakres, kontekst i cele przetwarzania danych oraz ocena ryzyka naruszenia praw i wolności osób fizycznych ma wpływ na zakres obowiązków jakie trzeba będzie realizować

# Kluczowe obszary wymogów RODO z perspektywy obowiązków Administratora danych (ADO)




odoekspert

# Fakultatywność lub obligatoryjność stosowania pewnych wymagań

## PRAWO DO „BYCIA ZAPOMNIANYM” – art. 17 RODO

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:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;

b) osoba, której dane dotyczą, **cofnęła zgodę**, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a), i nie ma innej podstawy prawnej przetwarzania;

c) osoba, której dane dotyczą, **wnosi sprzeciw** na mocy art. 21 ust. 1 wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania;

d) dane osobowe były przetwarzane **niezgodnie z prawem**;

e) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1

## Fakultatywność lub obligatoryjność stosowania pewnych wymagań

### ZGŁASZANIE NARUSZENIA OCHRONY DANYCH – art. 33 RODO

W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, **chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych**.

**ALE:**

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.

# Fakultatywność lub obligatoryjność stosowania pewnych wymagań

## OCENA SKUTKÓW DLA OCHRONY DANYCH – art. 35 RODO

Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować **wysokie ryzyko naruszenia praw lub wolności osób fizycznych**, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

Ocena skutków dla ochrony danych jest wymagana **w szczególności** w przypadku:

a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na **zautomatyzowanym przetwarzaniu**, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na **dużą skalę** szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub

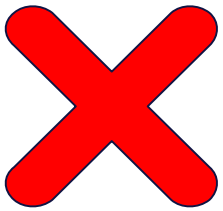
c) systematycznego monitorowania na **dużą skalę** miejsc dostępnych publicznie.

# Fakultatywność lub obligatoryjność stosowania pewnych wymagań

## OCENA SKUTKÓW DLA OCHRONY DANYCH – art. 35 RODO

**ALE DODATKOWO:**

Organ nadzorczy **ustanawia i podaje do publicznej wiadomości** wykaz rodzajów operacji przetwarzania **podlegających wymogowi dokonania oceny skutków** dla ochrony danych na mocy ust. 1.



Organ nadzorczy **może** także ustanowić i podać do wiadomości publicznej wykaz rodzajów operacji przetwarzania **niepodlegających** wymogowi dokonania oceny skutków dla ochrony danych.

# RODO TEZA #6

## Bez audytu nie mamy szans na dostosowanie do RODO

- na nowo poznaj swoją organizację i zdefiniuj ją językiem RODO

# Klucz do sukcesu: zdefiniuj aktywa podlegające ochronie prawnej – zbiory danych i systemy informatyczne

„Ochrona osób fizycznych powinna mieć zastosowanie do **zautomatyzowanego przetwarzania danych osobowych** oraz do **przetwarzania ręcznego, jeżeli dane osobowe znajdują się lub mają się znaleźć w zbiorze danych.** Zbiory lub zestawy zbiorów oraz ich strony tytułowe, które nie są uporządkowane według określonych kryteriów nie powinny być objęte zakresem niniejszego rozporządzenia.”

*Motyw 15 Preambuły*

„Niniejsze rozporządzenie ma zastosowanie do przetwarzania danych osobowych w sposób **całkowicie lub częściowo zautomatyzowany** oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych **stanowiących część zbioru danych lub mających stanowić część zbioru danych.”**

*Art. 2 ust. 1 RODO*

# CEL AUDYTU:

- **ustalenie aktywów podlegających ochronie prawnej z zakresu ochrony danych osobowych (zbiory danych + systemy),**
- **ustalenie zasad przetwarzania danych w poszczególnych zbiorach i systemach,**
- **analiza modelu biznesowego oraz procesów biznesowych związanych z czynnościami przetwarzania danych osobowych lub mających na nie wpływ,**
- **weryfikacja poszczególnych wymagań RODO pod kątem ustalenia, które z nich i w jakich przypadkach mogą mieć zastosowanie w danej organizacji,**
- **wskazanie aktualnego poziomu spełnienia wymagań oraz obszarów niezgodności,**
- **przedstawienie rekomendacji naprawczych z omówieniem możliwego sposobu ich realizacji w praktyce,**
- **ocena ryzyka.**

# RODO TEZA #7

## Wprowadzanie rozwiązań dostosowujących do wymagań RODO to proces, a nie jednorazowa czynność

- to rodzaj zarządzania zmianą w organizacji

## Wdrażanie wymagań RODO to zarządzanie zmianą w organizacji

1. **ustalenie celu wprowadzanej zmiany;**
2. **określenie wielkości i poziomu ważności zmiany (wyniki audytu);**
3. **uwzględnienie charakteru organizacji, jej kultury organizacyjnej;**
4. **określenie ograniczeń krytycznych;**
5. **aktywne włączenie pracowników w proces zmian.**

# RODO – które wymagania są kluczowe?

- **Analiza ryzyka np. przy doborze środków bezpieczeństwa**
- ***Privacy by design i privacy by default,* zasada niezbędności**
- **Współpraca z podmiotami przetwarzającymi, zasady doboru**
- **Polityki informacyjne wobec podmiotu danych**

- **Zasadniczy podział na wymogi prawne obarczone:**
  - administracyjną karą finansową do 10 mln Euro lub 2% światowego rocznego obrotu lub
  - do 20 mln Euro lub 4% światowego rocznego obrotu

- **Powołanie inspektora ochrony danych**
- **„Prawo do bycia zapomnianym”**
- **Ocena skutków dla ochrony danych**
- **Zgłaszanie naruszenia ochrony danych organowi nadzorczemu**

**KRYTERIUM**

**Złożoność, poziom skomplikowania, koszt i czas wdrożenia**

**Wysokość sankcji**

**Fakultatywność lub obligatoryjność stosowania wymogu**

# RODO – które wymagania są kluczowe?

## TO ZALEŻY:

- od charakterystyki aktywów podlegających ochronie
- od sposobu wykorzystywania tych aktywów
- od charakteru i kultury organizacyjnej
- od dostępnych zasobów organizacji
- od wyników oceny ryzyka
- od możliwości implementacyjnych w danej organizacji

# RODO TEZA #8

## Działaj racjonalnie i w oparciu o plan

- step by step

# STEP BY STEP

*Wszystko zaczyna się od ludzi ...*

01 LIDER + ZESPÓŁ

PLAN AUDYTU + HARMONOGRAMY CZYNNOŚCI + KOMUNIKACJA O PLANOWANYCH DZIAŁANIACH 02

03 ANALIZA WYNIKÓW AUDYTU + OCENA + PLAN NAPRAWCZY

PLAN WDROŻENIA Z UWZGLĘDNIENIEM CHARAKTERU ORGANIZACJI, OCENY RYZYKA, MOŻLIWOŚCI 04

05 STOPNIOWY PROCES IMPLEMENTACJI NA POZIOMIE CAŁEJ ORGANIZACJI

*... i kończy na ludziach*

odoekspert

odoekspert

**DZIĘKUJĘ ZA UWAGĘ !**

**Jakub Wezgraj**
**Radca prawny**
+48 600 677 026
j.wezgraj@odoekspert.pl
www.odoekspert.pl