Nowe zasady ochrony danych osobowych - RODO

r.pr. dr Paweł Biały

dr Agnieszka Stępień

INSTYTUT OCHRONY DANYCH OSOBOWYCH

Podstawowe przepisy prawa UE i PL dotyczące ochrony danych osobowych oraz prawa do prywatności

- Dyrektywa 95/46/WE podstawowy akt dot. ochrony danych osobowych z 1995 roku. Implementowany do prawa polskiego poprzez przepis art. 51 i 47 Konstytucji RP i ustawę o ochronie danych osobowych ale także szereg przepisów ustaw odrębnych.
- Konwencja 108 z 1981 r. dot. o ochronie osób w związku z automatycznym przetwarzaniem danych.
- Traktat o funkcjonowaniu Unii Europejskiej Art. 15 (dawny artykuł 286 TWE) „Każda osoba ma prawo do ochrony danych osobowych jej dotyczących."
- Karta Praw Podstawowych Unii Europejskiej - Art. 8 „Każdy ma prawo do ochrony danych osobowych, które go dotyczą. Dane te muszą być przetwarzane rzetelnie w określanych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie"

Podstawowe przepisy prawa UE i PL dotyczące ochrony danych osobowych oraz prawa do prywatności

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 -> jest to tzw. ogólne rozporządzenie o ochronie danych tj. RODO.

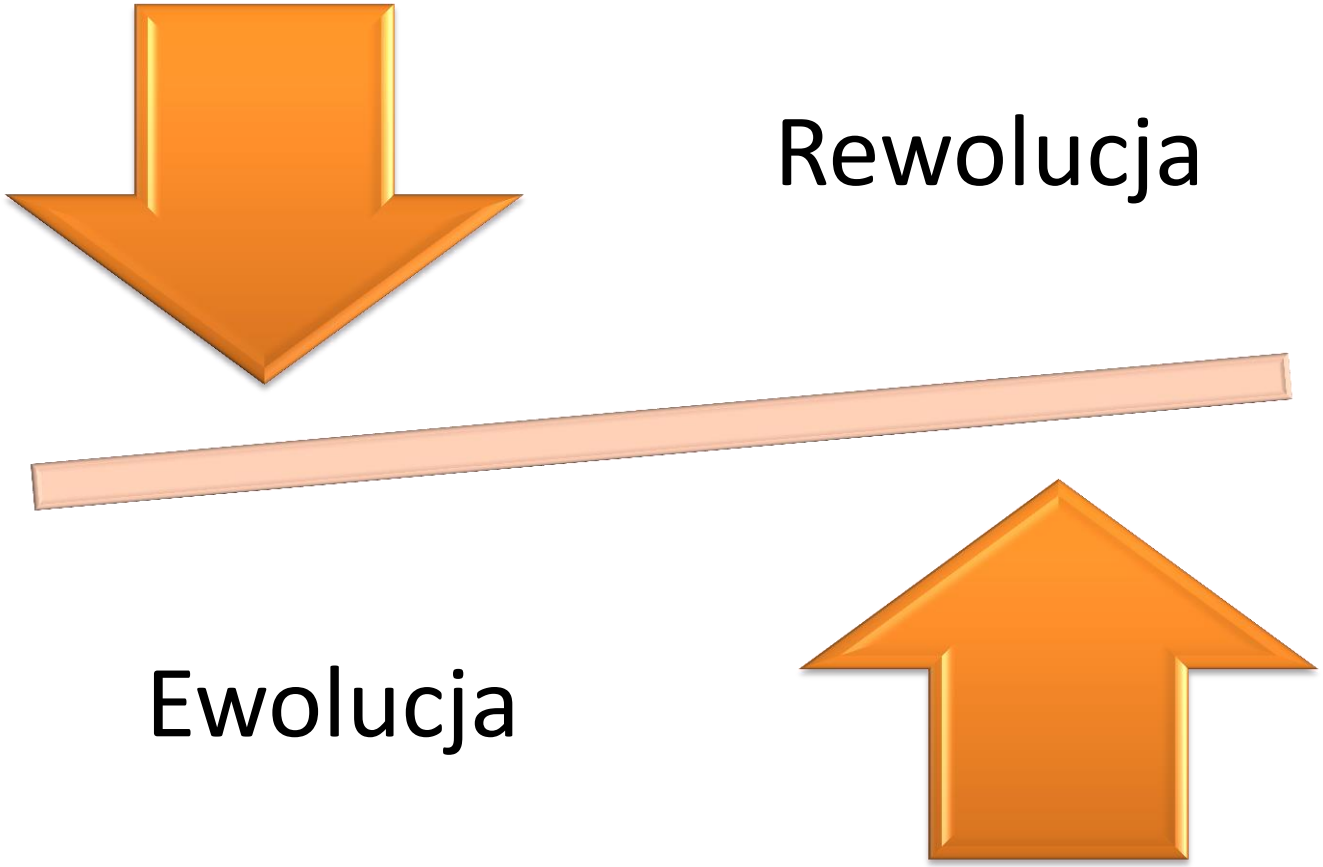
Dane osobowe – przykłady z praktyki

- Imię i nazwisko
- Wzór podpisu
- Adres mailowy i tradycyjny
- Numer telefonu
- Numer i seria dowodu osobistego
- Numer PESEL
- Wizerunek
- Dane z monitoringu
- Numer rejestracyjny
- Dane o rodzinie
- Dane o partnerce/partnerze życiowym
- Dane o dzieciach

Administrator Danych Osobowych – czyli kto w praktyce?

- Administrator danych osobowych to podmiot, który decyduje o środkach i celach przetwarzania danych osobowych
- Obowiązki ADO reguluje k.p. oraz uodo
- Praktyka:
- jednoosobowa działalność gospodarcza
- spółki
- każdy pracodawca
- fundacje, stowarzyszenia, Izby, etc.

RODO w Twojej firmie



Motyw Rozporządzenia

Szybki rozwój technologiczny i globalizacja przyniosły nowe wyzwania w zakresie ochrony danych osobowych. Niezwykle wzrosła skala wymiany i zbierania danych.

Technologia umożliwia zarówno przedsiębiorcom prywatnym, jak i organom publicznym wykorzystywanie danych osobowych do wykonywania powierzonych im zadań na niespotykaną dotąd skalę.

Technologia całkowicie zmieniła zarówno **gospodarkę, jak i życie społeczne**, i wymaga dalszego ułatwienia swobodnego przepływu danych w Unii oraz przekazywania ich do państw trzecich i organizacji międzynarodowych, przy równoczesnym zagwarantowaniu wysokiego poziomu ochrony danych osobowych.

Nowe wyzwania

- **Big Data**, która uświadamia nam, jak lawina informacji dogłębnie zmienia nasz sposób myślenia, pojmowania świata a którym żyjemy. Zjawisko Big Data jest **rewolucją** którą niesie nam przyszłość.
- Big data kusi i nabiera rozpędu jej stosowanie i wdrażanie ale przewidywania stworzone na jej podstawie mogą być wykorzystywane do karania ludzi za ich skłonności a nie działania.
- **Internet przedmiotów** (ang. *Internet of Things, IoT*) jest od dawna oczekiwanym rozszerzeniem Internetu, które obejmuje przedmioty codziennego użytku (np. inteligentne czytniki zużycia energii elektrycznej, lampę, telewizor, wagę) wyposażone w możliwość łączenia się z Internetem.

Nowe wyzwania

Jesteśmy pod stałą obserwacją od najprostszych czynności codziennego życia jak np. używanie światła czy bardziej złożone jak korzystanie z Internetu czy korzystanie z numeru PESEL.

- **Kradzież tożsamości** jako określona kategoria karno - prawna jest identyfikowana dopiero przy jej użyciu dla przetwarzania tych informacji o osobie w celu uzyskania określonych korzyści, a dla osoby której dane dotyczą spowodowanie określonej szkody materialnej lub osobistej.

Nowe wyzwania

- Przeprowadzone przez „Washington Post” śledztwo przeprowadzone w 2010 roku wykazało, ze amerykańska NSA (National Security Agency) każdego dnia przechwytuje i archiwizuje **1,7 mld. e-maili, rozmów telefonicznych i innych wiadomości**.

- Były pracownik NSA, William Binney oszacował że rząd Stanów Zjednoczonych zgromadził informacje o **20 bilionach operacji** przeprowadzonych między amerykanami a obywatelami innych krajów - kto do kogo dzwonił , kto do kogo pisał, kto komu przekazywał pieniądze itp.

Najważniejsze definicje

- ograniczenie przetwarzania”,
- „profilowanie”,
- „pseudonimizacja”,
- „odbiorca”,
- „strona trzecia”,
- „zgoda”,
- „naruszenie ochrony danych osobowych”,
- „dane genetyczne”,
- „dane biometryczne”,
- „dane dotyczące zdrowia”,

Najważniejsze definicje

- główna jednostka organizacyjna”,
- „przedsiębiorca”,
- „grupa przedsiębiorstw”,
- „organ nadzorczy, którego sprawa dotyczy”,
- „transgraniczne przetwarzanie”,
- „mający znaczenie dla sprawy i uzasadniony sprzeciw”,
- „usługa społeczeństwa informacyjnego”,
- „organizacja międzynarodowa”

PROFILOWANIE

- Oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy **aspektów dotyczących efektów pracy** tej osoby fizycznej, jej **sytuacji ekonomicznej**, **zdrowia**, **osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się,**
- Osoba, której dane dotyczą, **ma prawo do tego, by nie podlegać decyzji**, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, **w tym profilowaniu**, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa,
- Jeżeli dane osobowe są przetwarzane **na potrzeby marketingu bezpośredniego**, osoba, której dane dotyczą, **ma prawo w dowolnym momencie wnieść sprzeciw.**

Aktorzy procesu przetwarzania danych

- **GIODO** – Generalny Inspektor Ochrony Danych Osobowych **/ Organ nadzorczy,**
- Grupa Robocza Art. 29 **- Europejska Rada Ochronny Danych**,
- **Administrator Danych,**
- **Współadministrator,**
- **Procesor (podmiot przetwarzający),**
- **Data Protection Officer/Inspektor Ochrony Danych**
- **Administrator Systemu Informatycznego,**
- Użytkownicy danych osobowych,
- Personel wspierający,
- (Komisja, podmioty certyfikujące),

ABI czy DPO ?

Wyznaczenie Inspektora Ochrony Danych (IOD) – ART. 37 RODO

Administrator i **podmiot przetwarzający** wyznaczają inspektora ochrony danych, **zawsze gdy:**

- przetwarzania dokonują **organ lub podmiot publiczny**, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
- **główna działalność** administratora lub podmiotu przetwarzającego polega na operacjach przetwarzania, które ze względu na swój charakter, zakres lub cele **wymagają regularnego i systematycznego monitorowania** osób, których dane dotyczą, na dużą skalę; lub
- główna działalność administratora lub podmiotu przetwarzającego polega na przetwarzaniu na **dużą skalę szczególnych kategorii danych osobowych**, o których mowa w **art. 9** ust. 1, oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w **art. 10**;

Prawa osób których dane dotyczą

- Prawo do zachowania prywatności,
- Prawo do decydowania o swoich danych,
- Prawo do ochrony dotyczących mnie danych osobowych,
- Prawo do bycia poinformowanym,
- Prawo do zgłoszenia sprzeciwu,
- Prawo do żądania zaprzestania przetwarzania danych osobowych,
- Prawo do bycia przejrzyście poinformowanym i do przejrzystej komunikacji oraz trybu wykonywania praw,

Prawa osób których dane dotyczą

- Prawo dostępu do danych,
- Prawo do sprostowania danych,
- Prawo do usuwania danych,
- Prawo do bycia zapomnianym,
- Prawo do ograniczenia przetwarzania,
- Prawo do przenoszenia danych,
- Prawo do kopiowania danych,
- Prawo do odszkodowania i odpowiedzialność,
- Prawo do wniesienia skargi do organu nadzorczego,

Prawa osób których dane dotyczą

- **Artykuł 82 Rozporządzenie UE**
- **Prawo do odszkodowania i odpowiedzialność**

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

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

Powierzenie przetwarzania danych osobowych uodo/rodo

- Administrator danych może **powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych**. Procesor może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie. Procesor jest obowiązany przed rozpoczęciem przetwarzania danych podjąć środki zabezpieczające zbiór danych, o których mowa w art. 36-39, oraz spełnić wymagania określone w przepisach, o których mowa w art. 39a.
- Przetwarzanie **przez podmiot przetwarzający** podlegają odbywa się na podstawie umowy lub innego instrumentu prawnego, które prawu Unii lub prawu państwa członkowskiego i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora.

Nowe rozwiązania

Nowe rozwiązania to przede wszystkim dwa rewolucyjnie pojmowane rozwiązania:

- **przesunięcie odpowiedzialności** za zapewnienie zgodności przetwarzania danych na administratora danych osobowych,
- **zwiększona ochrona** praw i wolności osób, których dane dotyczą.

Nowe rozwiązania

Do pierwszej grupy należą rozwiązania dotyczące:

- uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych (art. 25 rodo),
- Zgłaszanie naruszenia ochrony danych:
  - organowi ochrony danych w terminie 72 godzin - art.33 rodo
  - zawiadomienie osoby, której dane dotyczą - art. 34 rodo

Wskazane obowiązki nakładają na ADO konieczność przewidywania skutków wynikającego z przetwarzania danych osobowych.

Obowiązek informacyjny

- Zgodnie z art. 12 rodo *„administrator danych powinien realizować obowiązek informacyjny w łatwo dostępnej formie, przejrzystej i zrozumiałej, jasnym i prostym językiem”.*
- Wszystko to po to, by osoba, której dotyczą nie miała żadnych wątpliwości na co wyraża zgodę.
- Doprecyzowana został także forma realizacji obowiązku wskazując za właściwą formę pisemną. Na żądanie uprawnionego w formie ustnej.

Obowiązek informacyjny

Zakres informacji podawany w treści obowiązku informacyjnego:

- **swoją tożsamość** i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego **przedstawiciela**;
- gdy ma to zastosowanie – dane **kontaktowe inspektora ochrony danych**;
- **cele** przetwarzania danych osobowych, oraz **podstawę prawną przetwarzania**;
- jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) – **prawnie uzasadnione** interesy realizowane przez administratora lub przez stronę trzecią;
- **informacje o odbiorcach** danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

Obowiązek informacyjny

- gdy ma to zastosowanie – informacje o **zamiarze przekazania danych osobowych do państwa trzeciego** lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych

- **okres**, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
- informacje o **prawie do żądania** od administratora **dostępu** do danych osobowych dotyczących osoby, której dane dotyczą, ich **sprostowania, usunięcia** lub **ograniczenia** przetwarzania lub o **prawie do wniesienia sprzeciwu wobec przetwarzania**, a także o **prawie do przenoszenia danych**;

Obowiązek informacyjny

- jeżeli przetwarzanie odbywa się na **podstawie zgody** – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- informacje o **prawie wniesienia skargi do organu nadzorczego**;
- informację, czy podanie danych osobowych jest **wymogiem ustawowym** lub **umownym** lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- informacje o **zautomatyzowanym podejmowaniu** decyzji, w **tym o profilowaniu**, o którym mowa w art. 22 ust. 1 i 4, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i **przewidywanych konsekwencjach** takiego przetwarzania dla osoby, której dane dotyczą.

Obowiązek informacyjny

- Jeżeli administrator planuje dalej przetwarzać dane osobowe w **celu innym niż cel**, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w ust. 2.
- **źródło pochodzenia** danych osobowych.

Zgoda na przetwarzanie danych osobowych

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

- **Praktyczny problem interpretacyjny:**

  a. jednoznaczne – czyli jakie?

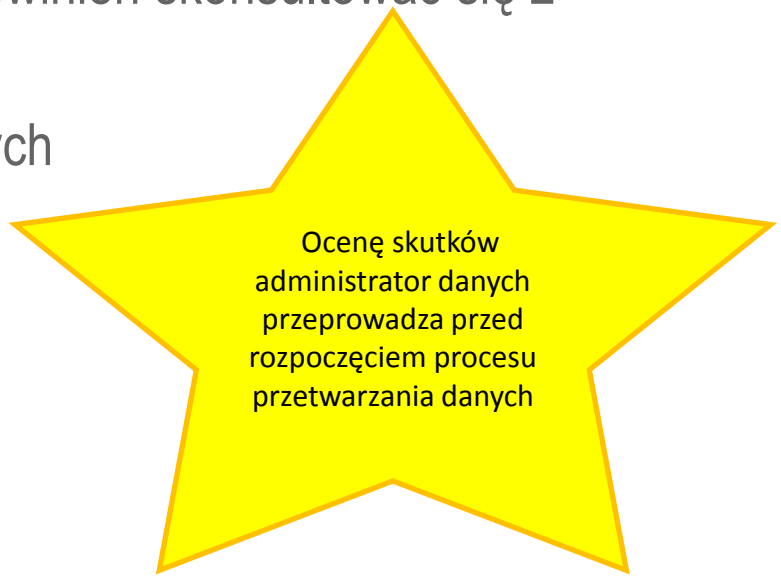
  b. okazanie woli – nie oświadczenie woli art. 60 k.c. (pojęcie węższe)

  c. działanie – zachowanie prawne: działanie/zaniechanie, wymóg aktywnego podjęcia czynności, nie bierne.

Ocena skutków dla ochrony danych

:

- Powinna zostać przeprowadzona w sytuacji, gdy przewidziany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych
- W takiej sytuacji administrator danych powinien skonsultować się z organem nadzorczym
- **Cel** – zapewnienie bezpieczeństwa danych



Ocena skutków dla ochrony danych

Kiedy więc DPIA nie będzie konieczna?

- przetwarzanie z dużym prawdopodobieństwem nie spowoduje wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (art. 35 ust. 1 rodo)
- - charakter, zakres, kontekst i cel przetwarzania są bardzo podobne do przetwarzania dla którego dokonano DPIA (art. 35 ust. 1 rodo)
- - gdy operacja przetwarzania ma podstawę prawną w prawie UE lub państwa członkowskiego i wstępna DPIA nie musi być przeprowadzona, gdy prawo reguluje określoną operację przetwarzania danych oraz gdy DPIA zgodnie ze standardami RODO już została dokonana w ramach ustanowienia podstawy prawnej (art. 35 ust.10 rodo)
- - gdy przetwarzanie uwzględnione jest w wykazie organu nadzorczego niepodlegających DPIA (art. 35 ust. 5 rodo)

Ocena skutków dla ochrony danych

- Organy nadzorcze zostały zobowiązane do podania do wiadomości publicznej wykazu rodzajów operacji, w których trzeba przeprowadzić DPIA lub tych gdzie nie jest to wymagane
- Jeżeli okaże się, że istnieje wysokie ryzyko naruszenia praw lub wolności osób fizycznych wynikających z przetwarzania danych osobowych administrator danych zobowiązany jest przeprowadzić ocenę skutków dla ochrony danych oraz skonsultować się z inspektorem ochrony danych.

Ocena skutków dla ochrony danych

Kiedy przeprowadzenie DPIA jest obligatoryjne?

- Ze względu na rodzaj przetwarzania danych w szczególności przy wykorzystaniu nowoczesnych rozwiązań technologicznych
- Przetwarzanie polega na ocenie 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 w podobny sposób znacząco wpływających na osobę fizyczną
- Planowane jest przetwarzanie na dużą skalę szczególnych kategorii danych
- Planowane jest przetwarzanie polegające na systematycznym monitorowaniu na dużą skalę miejsc dostępnych publicznie

Analiza ryzyka

- Administrator danych będzie zobowiązany do oceny ryzyka naruszenia praw i wolności podmiotów danych w związku z realizowanym procesem przetwarzania danych
- Kategorie:

- Niskie ryzyko
- Ryzyko
- Wysokie ryzyko

- *W każdej sytuacji gdy zbieramy lub korzystamy z danych musimy analizować ryzyko.*

Rejestr czynności przetwarzania danych

- **Art. 30 rodo: Każdy administrator** oraz – gdy ma to zastosowanie – przedstawiciel administratora prowadzą **rejestr czynności przetwarzania** danych osobowych, za które odpowiadają. W rejestrze tym zamieszcza się wszystkie następujące informacje …..
- **Art. 30 rodo: Każdy podmiot przetwarzający** oraz – gdy ma to zastosowanie – przedstawiciel podmiotu przetwarzającego prowadzą rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, zawierający następujące informacje ….

Rejestr czynności przetwarzania danych

- 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.

Odpowiedzialność w zakresie przetwarzania danych

- **Odpowiedzialność administracyjna** – wydanie decyzji przez GIODO (zakaz przetwarzania danych lub nakaz zastosowania dodatkowych zabezpieczeń),
- **Odpowiedzialność karna** – kara grzywny/pozbawienie wolności 1-3 lat,
- **Odpowiedzialność cywilnoprawna** - dane osobowe jako dobro osobiste, roszczenia sądowe zadośćuczynienia za doznaną krzywdę wyrządzoną wskutek nieuprawnionego przetwarzania danych,
- **Odpowiedzialność według prawa pracy** - postępowanie w celu nałożenia kary porządkowej, postępowanie zmierzające do rozwiązania stosunku pracy,
- **Odpowiedzialność finansowa** - nałożenie kary w egzekucyjnym postępowaniu administracyjnym do 200 tys. PLN (obecnie), do 4% obrotu rocznego światowego lub 20 mln EUR (RODO),
- Zgłoszenie do Prokuratury zawiadomienia o **prawdopodobieństwie popełnienia przestępstwa**,

MUST HAVE

Co może zrobić ADO by już dziś spać spokojnie ?

- Diagnoza ochrony procesu przetwarzania danych osobowych,
- Identyfikacja rodzaju i zakresu wykorzystywanych danych osobowych
- Raport + wnioski -> wiem co zmienić w związku z RODO

MUST HAVE

- Przygotowanie nowej dokumentacji i jej wdrożenie:
- Upoważnienia,
- Ewidencje,
- Umowy powierzenia danych wg nowych zasad
- Umowy udostępniające dane wg nowych zasad
- Zasady i reguły przetwarzania danych
- Plany sprawdzeń
- Polityka i instrukcja zarządzania wg nowych zasad, etc.

MUST HAVE

- Cykl szkoleń dla wyznaczonych pracowników
- Zabezpieczenie pasywne spółki (tzw. bezpieczeństwo fizyczne)
- Zabezpieczenie teleinformatyczne
- Outsourcing pomocowy dla ABI/Inspektora Ochrony Danych

Podsumowanie

Wiceprzewodnicząca KE Viviane Reding, Komisarz UE ds. Sprawiedliwości powiedziała:

"Wiadomość, jaką przekazuje Parlament Europejski, jest jednoznaczna: Ta reforma to konieczność i teraz jest już nieodwracalna."

"Ochrona danych powstaje w Europie. Solidne zasady ochrony danych muszą być znakiem towarowym Europy. Po mających miejsce skandalach związanych ze szpiegostwem informacyjnym USA, ochrona danych jest tak konkurencyjną zaletą jak nigdy dotąd."