# Ubezpieczeniowy Fundusz Gwarancyjny

## Znaczenie Rozporządzenia o Ochronie Danych Osobowych dla funkcjonowania zakładów ubezpieczeń

Warszawa, wrzesień 2017

## Agenda

1. **Rozporządzenie 2016/679** – Informacje podstawowe
2. **Nowe zasady przetwarzania danych osobowych –** Aspekty istotne dla zakładów ubezpieczeń
3. **Kontrola przetwarzania danych osobowych –** Nadzór, naruszenia, sankcje
4. **Zmiany w polskim porządku prawnym –** Dostosowanie przepisów, ograniczenia

# Rozporządzenie 2016/679

Informacje podstawowe

# RODO – Informacje podstawowe

- Podstawą wprowadzenia nowych regulacji jest **Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679** z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych (ogólne rozporządzenie o ochronie danych) **(RODO).**
- RODO jest aktem prawnym **stosowanym bezpośrednio** w prawie krajowym, jednak istnieje konieczność dostosowania polskich przepisów do nowych regulacji unijnych.
- RODO zostało przyjęte 27 kwietnia 2016 roku, weszło w życie 17 maja 2016 roku, jednakże zacznie obowiązywać od **25 maja 2018 roku.**
- **krajowe przepisy obligatoryjne** dotyczą m.in. wprowadzenia i zasad funkcjonowania organu nadzoru (odpowiednik obecnego GIODO)
- **krajowe przepisy fakultatywne** dotyczą ograniczeń stosowania RODO (art. 23) oraz podstaw prawnych dotyczących przetwarzania danych (art. 6 ust. 2-3 i art. 9 ust. 4 RODO)

# RODO – Informacje podstawowe

## Podstawowe cele RODO:

- zapewnienie przejrzystości i pewności prawa ochrony danych osobowych
- wyważenie prawa do ochrony danych osobowych względem innych praw podstawowych oraz respektowanie fundamentalnych praw i wolności ludzkości
- wprowadzenie jednolitych regulacji i zapewnienie równego poziomu ochrony danych osobowych w państwach członkowskich Unii Europejskiej
- zapewnienie swobody przepływu danych osobowych na terenie UE
- współpraca i wzrost wymiany danych osobowych między podmiotami publicznymi i prywatnymi
- dostosowanie przepisów do szybkiego postępu technicznego i globalizacji – postępujący rozwój technologii i informatyzacja podmiotów przetwarzających dane

# Nowe zasady przetwarzania danych osobowych

Aspekty istotne dla zakładów ubezpieczeń

# Najważniejsze zmiany zasad ochrony danych osobowych

## Zasady dotyczące przetwarzania danych (art. 5) (1):

- zgodność z prawem, rzetelność i przejrzystość
- ograniczenie celu przetwarzania danych
- minimalizacja danych
- prawidłowość przetwarzania danych osobowych
- ograniczenie przechowywania danych
- integralność i poufność danych
- rozliczalność

# Najważniejsze zmiany zasad ochrony danych osobowych

## Warunki zgodności przetwarzania danych z prawem (art. 6):

- **zgoda** podmiotu danych na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów

lub, gdy przetwarzanie jest niezbędne do:

- **wykonania umowy**, której stroną jest osoba, której dane dotyczą, lub do **podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy**
- **wypełnienia obowiązku prawnego** ciążącego na administratorze
- **ochrony żywotnych interesów** osoby, której dane dotyczą, lub innej osoby fizycznej

# Najważniejsze zmiany zasad ochrony danych osobowych

## Warunki wyrażenia zgody (art. 7):

- **administrator musi być w stanie wykazać, że osoba, której dane przetwarza wyraziła zgodę** na przetwarzanie jej danych osobowych (jeżeli wymagana)
- zapytanie o zgodę musi zostać przedstawione **w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem**
- **w dowolnym momencie można wycofać zgodę**, o czym osoba, której dane dotyczą, musi zostać poinformowana, zanim wyrazi zgodę
- **Wycofanie zgody musi być równie łatwe jak jej wyrażenie**
- Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy m.in. **od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy**, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy

# Najważniejsze zmiany zasad ochrony danych osobowych

## Warunki przetwarzania danych sensytywnych (art. 9):

- **wyraźna zgoda** na przetwarzanie danych osobowych,
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody,
- przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą,
- **przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy,**
- przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

## Przetwarzanie danych dotyczących wyroków skazujących i naruszeń prawa (art. 10):

Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub **prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą**. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

# Najważniejsze zmiany zasad ochrony danych osobowych

## Obowiązki informacyjne (art. 12-15):

- Zasada przejrzystości - wszelkie informacje i komunikacja dotyczące przetwarzania danych osobowych powinny być przekazywane w sposób zrozumiały i niebudzący wątpliwości
- RODO rozszerzyło obowiązki informacyjne o:
  - dane kontaktowe inspektora danych osobowych (dawny ABI),
  - podstawę prawną przetwarzania danych,
  - wyjaśnienie usprawiedliwionego celu,
  - zamiar przekazania danych do państwa trzeciego,
  - okres przechowywania danych (okoliczności wskazujące na okres przetwarzania danych),
  - prawo cofnięcia zgody,
  - prawo wniesienia skargi do organu nadzorczego,
  - informację o profilowaniu i automatycznych decyzjach.
- Obowiązek informowania o przetwarzanych danych na każdy wniosek osoby, której dane dotyczą i w każdym czasie

# Najważniejsze zmiany zasad ochrony danych osobowych

## Uprawnienia podmiotów danych:

- **Prawo do sprostowania danych (art. 16):**

prawo żądania od administratora **niezwłocznego sprostowania danych osobowych, które są nieprawidłowe lub niekompletne**

- **Prawo do bycia zapomnianym (art. 17):**

prawo żądania od administratora, **niezwłocznego usunięcia danych i informacji**, w określonych sytuacjach i pod pewnymi zastrzeżeniami

- **Prawo do przenoszenia danych (art. 20):**

prawo otrzymania danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego, celem przeniesienia ich do innego administratora

- **Prawo sprzeciwu (art. 21):**

prawo wniesienia sprzeciwu przetwarzania danych, w tym profilowania, skutkujące brakiem możliwości ich dalszego przetwarzania w zakresie marketingu bezpośredniego oraz w innych celach, chyba że administrator wykaże **istnienie** ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub **podstaw do ustalenia, dochodzenia lub obrony roszczeń**

# Najważniejsze zmiany zasad ochrony danych osobowych

## Profilowanie i podejmowanie zautomatyzowanych decyzji (art. 22):

- **Profilowanie** to dowolna forma zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu tych danych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się
- Prawo do niepodlegania decyzji, opartej wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, wywołującej skutki prawne lub w podobny sposób istotnie na nią wpływające. Niniejszego uprawnienia, nie stosuje się, gdy przetwarzanie:
  - jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem
  - jest dozwolona prawem Unii lub prawem krajowym, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i uzasadnionych interesów osoby, której dane dotyczą; lub
  - opiera się na wyraźnej zgodzie osoby, której dane dotyczą

## Privacy by Design / Privacy by Default (art. 25):

- administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania – wdraża odpowiednie środki techniczne i organizacyjne, takie jak **pseudonimizacja**, zaprojektowane w celu skutecznej ochrony danych, takich jak **minimalizacja danych**, oraz w celu nadania przetwarzaniu **niezbędnych zabezpieczeń**, tak by spełnić wymogi RODO oraz chronić prawa osób, których dane dotyczą
- administrator wdraża odpowiednie środki techniczne i organizacyjne, aby **domyślnie** przetwarzane były **wyłącznie** te dane osobowe, które są **niezbędne** dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek zapewnienia aby dane osobowe nie były domyślnie udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych

# Najważniejsze zmiany zasad ochrony danych osobowych

## Data protection impact assessment (art. 35):

- Jeżeli dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele może nieść duże zagrożenie dla praw i wolności osób fizycznych, administrator przed przetworzeniem dokonuje **oceny skutków planowanych operacji przetwarzania** dla ochrony danych osobowych. Dla zbioru podobnych operacji przetwarzania wiążących się z podobnymi dużymi zagrożeniami można przeprowadzić pojedynczą ocenę
- Ocena skutków jest wymagana, w szczególności w przypadku:
  - oceny osobowych czynników, opierających się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, będących podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób na nią wpływających;
  - przetwarzania na dużą skalę np. danych sensytywnych lub danych o wyrokach skazujących i o przestępstwach; lub
  - systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie

# Kontrola przetwarzania danych osobowych

Nadzór, naruszenia, sankcje

# Kontrola przetwarzania danych osobowych

## Organ ochrony danych:

- Obowiązek ustanowienia.
- Właściwy jeżeli przetwarzania danych dokonują organa publiczne lub **podmioty prywatne, w zakresie określonym przepisami**
- Zadania:
  - nadzór, kontrola realizacji przepisów, rozpatrywanie skarg, prowadzenie postępowań
  - prowadzenie rejestru naruszeń
  - **zatwierdzanie wiążących reguł korporacyjnych, przyjmowanie standardowych klauzul umownych, udzielanie zaleceń i zezwalania na transfer danych**
- Kompetencje:
  - wprowadzanie czasowego lub całkowitego ograniczenia przetwarzania danych
  - prowadzenie postępowań w formie audytów ochrony danych
  - wydawanie ostrzeżeń o możliwości naruszenia RODO poprzez planowane operacje przetwarzania
  - udzielanie upomnień w przypadku naruszenia RODO
  - nakazanie spełnienia żądania osoby, w zakresie uprawnień, wynikających z RODO

# Kontrola przetwarzania danych osobowych

## Zgłaszanie incydentów organowi (art. 33) i podmiotowi danych (art. 34)

- Obowiązek administratora do poinformowania organu o każdym incydencie bezpieczeństwa danych osobowych, np.:
  - przypadkowym lub niezgodnym z prawem zniszczeniem, utraceniem, zmodyfikowaniem danych
  - nieuprawnionym ujawnieniem lub udostępnieniem danych osobowych
- Zgłoszenie musi:
  - zostać dokonane niezwłocznie, nie później niż w ciągu 72 godzin od naruszenia
  - opisywać charakter naruszenia
  - opisywać możliwe konsekwencje naruszenia i zastosowane środki zaradcze
- Administrator danych prowadzi rejestr naruszeń
- W razie wysokiego ryzyka naruszenia praw lub wolności osoby fizycznej – obowiązek jej zawiadomienia (jasnym i prostym językiem), o takim naruszeniu. Nie stosuje się, gdy:
  - wdrożone zostały odpowiednie techniczne i organizacyjne środki ochrony
  - administrator podjął środki eliminujące zagrożenie dla praw i wolności osoby
  - wymagałoby niewspółmiernie dużego wysiłku

# Kontrola przetwarzania danych osobowych

## Administracyjne kary pieniężne (art. 83 i n.):

- Nakładane przez organ również z innymi sankcjami (ostrzeżenia, nakazy, zakazy, obowiązki zaprzestania przetwarzania danych)
- Kary finansowe mają być skuteczne, proporcjonalne i odstraszające
- Nałożenie kary i jej wysokości zależne od okoliczności, w tym m.in. od:
  - charakteru, wagi, czasu trwania naruszenia, liczby poszkodowanych, rozmiaru szkody
  - charakteru naruszenia (umyślny lub lekkomyślny)
  - działań podjętych w celu zminimalizowania szkody
- Wysokość kar:
  - **do 10 mln euro lub do 2% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota **wyższa**, w przypadku naruszeń mniejszej wagi
  - **do 20 mln euro lub do 4% całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota **wyższa**, w przypadku znaczących naruszeń

# Zmiany w polskim porządku prawnym

Dostosowanie przepisów, ograniczenia

# Zmiany w polskim porządku prawnym

## Grupa robocza ds. ochrony danych osobowych UFG

- UFG w listopadzie 2016r. powołał **Grupę roboczą ds. ochrony danych osobowych,** która wypracowała propozycję sektorowych przepisów fakultatywnych (ograniczenia lub wyłączenia stosowania RODO)
- członkami grupy byli przedstawiciele zakładów ubezpieczeń działu I i II (**26 zakładów**), **PIU oraz PBUK,**
- propozycje zmian przepisów**, 23 lutego 2017r. UFG przekazało do MF, w zakresie**:
  - ustawy z 11 września 2015 roku o działalności ubezpieczeniowej i reasekuracyjnej
  - ustawy z 22 maja 2003 roku o ubezpieczeniach obowiązkowych, UFG i PBUK

# Zmiany w polskim porządku prawnym

## Projekt ustawy o ochronie danych osobowych z 28 marca 2017 roku

- Utworzenie Urzędu Ochrony Danych Osobowych pod przewodnictwem Prezesa Urzędu
- Kompetencje Prezesa:
  - wydawanie **niewiążących** dobrych praktyk przetwarzania danych – wskazówki, zalecenia
  - prowadzenie kontroli przestrzegania przepisów o ochronie danych osobowych
  - prawo autokontroli Prezesa (uchylenie lub zmiana wydanej)
  - wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych osobowych lub zakazu przetwarzania
  - udzielanie upomnień, w sprawie naruszeń niskiej wagi
  - sprostowanie lub usunięcie danych
  - nakładanie administracyjnych kar finansowych
- Nowe zasady prowadzenia postępowania w sprawie naruszenia ochrony danych osobowych:
  - jednoinstancyjność
  - możliwość wszczęcia lub udziału w postępowaniach przez organizacje społeczne,

# Zmiany w polskim porządku prawnym

## Harmonogram dalszych prac

- Propozycja dostosowania regulacji sektorowych (bankowość, ubezpieczenia)
- Propozycje zmian wypracowane przez rynek ubezpieczeniowy (grupa robocza) zostały przekazane przez Ministerstwo Finansów do Ministerstwa Cyfryzacji – resort odpowiedzialny za dostosowanie przepisów do zmiany regulacji dotyczących ochrony danych osobowych
- Proces opiniowania przygotowanych zmian do ustaw sektorowych
- Po zakończeniu procesu legislacyjnego na poziomie krajowym prace legislacyjnej zostaną skierowane do Komisji Europejskiej
- Od 25 maja 2018 roku obowiązywać będą przepisy RODO i przyjęte do tego czasu przepisy krajowe

# Dziękuję za uwagę.

**Wojciech Majewski**

Ośrodek Informacji

wmajewski@ufg.pl

Tel. +48 22 53 96 229| Kom. +48 691 362 338

**Ubezpieczeniowy Fundusz Gwarancyjny**

ul. Płocka 9/11, 01-231 Warszawa

Tel. +48 22 53 96 100|Fax +48 22 53 96 261

ufg.@ufg.pl