Nowe zasady przetwarzania danych wynikające z RODO

Wytyczne dla Agentów Ubezpieczeniowych

RODO w ubezpieczeniach

czyli wpływ rozporządzenia o ochronie danych osobowych na działalność ubezpieczycieli i pośredników

Zasady przetwarzania danych osobowych

- Zgodność z prawem, rzetelność, przejrzystość.
- Ograniczenie celu.
- Minimalizacja danych.
- Prawidłowość.
- Ograniczenie przechowywania.
- Integralność i poufność.
- Rozliczalność.

Zgodność z prawem, rzetelność i przejrzystość

Dane osobowe muszą być przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą:

- konieczna podstawa prawna przetwarzania (zgoda, wykonanie umowy, wypełnienie obowiązku prawnego ciążącego na administratorze),
- wszelkie informacje i komunikaty związane z przetwarzaniem danych osobowych muszą być **łatwo dostępne i zrozumiałe** oraz sformułowane **jasnym i prostym językiem** istnieje możliwość dodatkowej wizualizacji,
- zasada ta dotyczy w szczególności informowania osób, których dane dotyczą, o **tożsamości administratora i celach przetwarzania,**
- osobom fizycznym należy uświadomić **ryzyka, zasady, zabezpieczenia i prawa związane z przetwarzaniem danych osobowych oraz sposoby wykonywania praw przysługujących im w związku z takim przetwarzaniem** pełna informacja o celach przetwarzania.

Zasada przejrzystości – realizacja

Dystrybutorzy ubezpieczeń będący administratorami danych mają obowiązek:

- umożliwić klientom **składanie zapytań i żądań** związanych z przetwarzaniem danych (np. pisemnie, drogą elektroniczną poprzez formularz na stronie internetowej, przez e-mail, telefonicznie, w placówce),
- **odpowiadać na żądania udzielenia informacji** o przetwarzaniu, żądania usunięcia danych, sprzeciwy wobec przetwarzania danych itp. w terminie miesiąca (przedłużenie terminu możliwe tylko z uwagi na skomplikowany charakter żądania lub liczbę żądań),
- wykazać fakt, że przestrzegana jest zasada przejrzystości informacji wobec klientów oraz w polityce wewnętrznej firmy (ciężar dowodu po stronie administratora).

Ograniczenie celu

Dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami:

- konkretne cele przetwarzania danych osobowych powinny być **wyraźne, uzasadnione i określone w momencie zbierania danych,**
- dane powinny być **adekwatne, ograniczone do tego co niezbędne w kontekście celów przetwarzania,**
- aby zapobiec przechowywaniu danych osobowych przez okres dłuższy, niż jest to niezbędne, administrator powinien ustalić termin ich usuwania lub okresowego przeglądu,
- przetwarzanie danych do celów innych niż te, dla których dane zostały zebrane, jest dozwolone, gdy jest zgodne z celami pierwotnymi.

Minimalizacja danych

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

- kluczowe w przypadku przetwarzania szczególnych kategorii danych,
- ograniczenie zakresu zbieranych danych,
- wyeliminowanie praktyki zbierania danych „na zapas".

Minimalizacja danych w praktyce

- Nie jest dopuszczalne przetrzymywanie całości wrażliwych danych klienta zakładu ubezpieczeń w oparciu o podstawę prawną bezpodstawnie wydłużającą okres przechowywania danych.
- Liczenie okresu przechowywania danych osobowych dla każdej polisy powinno następować odrębnie.

Zasada prawidłowości

Dane osobowe muszą być prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

- Zapewnienie odpowiednich praw osobom, których dane dotyczą:
  - prawo do sprostowania danych,
  - prawo do ograniczenia przetwarzania .
- Problem pozyskiwania danych z nieznanych źródeł pochodzenia.
- Zestawianie danych na podstawie różnych źródeł (w tym profilowanie).

Zasada ograniczenia przechowywania w praktyce

Konieczność usunięcia danych osobowych przez dystrybutora ubezpieczeń może zależeć od:

- cofnięcia zgody przez osobę, której dane dotyczą,
- wyrażenia sprzeciwu przez osobę, której dane dotyczą,
- przedawnienia roszczeń,
- upływu terminów przechowywania z przepisów szczególnych.

Integralność i poufność

Dane osobowe muszą być przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych:

- kluczowa rola zabezpieczeń informatycznych,
- zapewnienie bezpieczeństwa i poufności danych,
- ochrona przed nieuprawnionym dostępem do danych i sprzętu służącego do przetwarzania (system haseł, szyfrowanie, kontrola dostępu, monitoring),
- zabezpieczenie przed nieuprawnionym korzystaniem.

Zasada rozliczalności

Administrator jest odpowiedzialny za przestrzeganie zasad przetwarzania danych osobowych i musi być w stanie wykazać ich przestrzeganie:

- odpowiednie udokumentowanie,
  - spełnienia obowiązków wynikających z RODO (np. odebranie zgód),
  - czynności z zakresu przetwarzania danych,
  - stosowanych środków technicznych i organizacyjnych,
- przeprowadzenie i udokumentowanie oceny skutków dla ochrony danych,
- wdrożenie odpowiednich procedur/polityk bezpieczeństwa,
- stosowanie zatwierdzonych kodeksów postępowania,
- stosowanie wytycznych ERODO i norm ISO,
- utrzymanie polityki prywatności/bezpieczeństwa.

Prawa klientów, których dane osobowe dotyczą

Dystrybutor ubezpieczeń musi zapewnić klientowi:

- prawo dostępu do danych,
- prawo do przeniesienia danych osobowych,
- prawo do usunięcia danych (bycia zapomnianym),
- prawo do sprostowania,
- prawo do ograniczenia przetwarzania,
- prawo do sprzeciwu,
- prawo niepodlegania decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu danych (profilowanie).

Agent jako procesor

- **„Administrator"** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;** jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.

Administratorem jest Zakład Ubezpieczeń lub multiagent

- **„Podmiot przetwarzający"-** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który **przetwarza dane osobowe w imieniu administratora.**

Podmiotem Przetwarzającym jest Agent ubezpieczeniowy

Podwójna rola multiagenta

- W odniesieniu do klientów ZU, a więc osób, które zawarły już umowę ubezpieczenia, multiagent, co do zasady będzie **procesorem**.
- W odniesieniu do danych osobowych potencjalnych Klientów, multiagent może tworzyć własne bazy danych i działać jako **administrator** tych danych.

Odpowiednie obowiązki wynikają z zależności od roli w której agent występuje!

Współadministratorzy – nowe pojęcie w RODO

- Jeżeli co najmniej dwóch administratorów wspólnie **ustala cele i sposoby przetwarzania**, są oni współadministratorami.
- W drodze wspólnych uzgodnień współadministratorzy w przejrzysty sposób określają **odpowiednie zakresy swojej odpowiedzialności** dotyczącej wypełniania obowiązków wynikających z niniejszego rozporządzenia (w szczególności obowiązki informacyjne).
- W uzgodnieniach można wskazać punkt kontaktowy dla osób, których dane dotyczą.
- Uzgodnienia powinny należycie odzwierciedlać odpowiednie **zakresy obowiązków** współadministratorów oraz **relacje pomiędzy nimi a podmiotami, których dane dotyczą**.
- Zasadnicza treść uzgodnień jest **udostępniana** podmiotom, których dane dotyczą.

Współadministratorzy

- Niezależnie od tych uzgodnień osoba, której dane dotyczą, może wykonywać przysługujące jej prawa wynikające z niniejszego rozporządzenia **wobec każdego z administratorów**.
- **Solidarna odpowiedzialność współadministratorów.**

- ✓ **ZU (administrator) i Agent (procesor).**
- ✓ **ZU majątek (współadministrator) i ZU życie (współadministrator).**

Rejestr czynności przetwarzania danych

Zastępuje obowiązek zgłaszania zbiorów danych osobowych.

Powstaje obowiązek prowadzenia dwóch rejestrów:

- przez administratora,
- przez podmiot przetwarzający.

Wyjątek od tego obowiązku przewidziany jest w art. 30 ust 5 RODO (co do zasady obowiązek prowadzenia rejestru nie odnosi się do przedsiębiorcy lub podmiotu zatrudniającego mniej niż 250 osób), **jednak nie odnoszą się one do zakładów ubezpieczeń i podmiotów przetwarzających z uwagi na przetwarzanie szczególnej kategorii danych (dane dotyczące zdrowia).**

Rejestr czynności przetwarzania danych

Administrator lub podmiot przetwarzający może powierzyć IOD prowadzenie, w imieniu administratora albo podmiotu przetwarzającego, rejestru czynności przetwarzania danych. Taki rejestr powinien być uznany za jedno z narzędzi umożliwiających IOD realizację jego zadań w zakresie monitorowania przestrzegania przepisów, informowania administratora lub podmiotu przetwarzającego i doradzania im.

Artykuł 39(1) RODO określa minimalną listę zakresu obowiązków IOD (Inspektor Ochrony Danych).

Rejestr czynności – administrator (art. 30 RODO) zawiera:

- Imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie przedstawiciela administratora oraz inspektora danych osobowych.
- Cele przetwarzania.
- Opis kategorii osób których dane dotyczą oraz kategorii danych osobowych.
- Kategorie odbiorców, którym dane osobowe zostały ujawnione (w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych).
- Gdy ma to zastosowanie , przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej.
- Jeżeli jest to jest to możliwe, planowane terminy przesunięcia poszczególnych kategorii danych.
- Jeśli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust 1.

Rejestr czynności - podmiot przetwarzający (art. 30 RODO) zawiera:

- Imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora w imieniu którego działa podmiot przetwarzający, a gdy ma to zastosowanie- przedstawiciela administratora lub podmiotu przetwarzającego oraz inspektora ochrony danych.
- Kategorie przetwarzań dokonywanych w imieniu poszczególnych administratorów.
- Gdy ma to zastosowanie , przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwa tego państwa trzeciego lub organizacji, a w przypadku przekazań, o których mowa w art. 49 ust 1 akapit drugi, dokumentacja odpowiednich zabezpieczeń.
- Jeśli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust 1.

Bezpieczeństwo przetwarzania – art. 32 (zasady wspólne i dla administratora i dla procesora)

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 techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

- pseudonimizację i szyfrowanie danych osobowych,
- zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
- zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
- regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Bezpieczeństwo przetwarzania – kodeksy i certyfikacja

- Wywiązywanie się z obowiązków, w zakresie bezpieczeństwa przetwarzania, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji.
- Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Bezpieczeństwo przetwarzania – dostęp osób upoważnionych

Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

Naruszenie danych a obowiązki administratora

- Dokumentowanie naruszeń do weryfikacji przez organ nadzorczy.
- Zgłoszenie naruszeń do organu nadzorczego (chyba że jest mało prawdopodobne, że naruszenie będzie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych).

Dokumentowanie okoliczności naruszenia ochrony danych, skutków oraz podjętych działań zaradczych może być prowadzone w formie rejestru naruszeń, a w przypadku opóźnionego zgłoszenia wyjaśnienie przyczyn. Wyjaśnienie również w przypadku braku zgłoszenia lub zawiadomienia osób których dane dotyczą.

Naruszenie danych a obowiązki administratora

Zawiadomienie o naruszeniu:

- Ma umożliwić osobom, których dane dotyczą podjęcie środków zaradczych.
- Ma zostać wysłane bez zbędnej zwłoki (w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia).
- Zawiadomienie musi być wysłane w odrębnej wiadomości.
- W razie gdy zawiadomienie wymaga od administratora niewspółmiernie dużego wysiłku możliwość wydania publicznego komunikatu, który zapewni poinformowanie osób których dane zostały naruszone o naruszeniu.

Naruszenie danych a obowiązki procesora

Procesor zgłasza naruszenia administratorowi:

- po stwierdzeniu naruszenia bez zbędnej zwłoki,
- procesor nie ma obowiązku dokumentowania naruszeń (może zostać on nałożony umownie),
- procesor może zgłosić naruszenie w imieniu administratora danych o ile posiada stosowne upoważnienie. **Mimo tego odpowiedzialność za brak zgłoszenia ciąży na administratorze.**

Naruszenie danych - zawiadomienie osoby

- 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.
- Zawiadomienie nie jest wymagane w następujących przypadkach:
  - administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych,
  - administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
  - wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Zawiadomienie – również na żądanie **PUODO.**

Okresy retencji danych- umowa ubezpieczenia

Usunięcie danych osobowych przez zakład następuje na skutek:

- **w przypadku przetwarzania danych w celach marketingowych- cofnięcia zgody przez osobę, której dane dotyczą (podstawa prawna- art. 6 ust 1 lit. a) RODO,**
- **w przypadku przetwarzania danych których podstawą jest niezbędność przetwarzania danych celem realizacji uzasadnionego interesu administratora (marketing bezpośredni) - zależy od wyrażenia sprzeciwu przez osobę, której dane dotyczą,**
- **w przypadku przetwarzania w celu realizacji umowy ubezpieczenia- zależy od przedawnienia roszczeń,**
- **w przypadku gdy dane dotyczą dowodów księgowych z umowy ubezpieczenia- terminy wynikające z przepisów o rachunkowości.**

Okresy retencji danych - umowa ubezpieczenia

Dane osobowe powinny zostać zanonimizowane / usunięte po najdłuższym okresie przedawnienia roszczeń:

- 3 lata wynikają z umowy ubezpieczenia,
- 10 lat – roszczenia z innych tytułów niż umowa ubezpieczenia,
- 10/20 lat w przypadku czynów niedozwolonych w zależności co jest przedmiotem ubezpieczenia OC.

Nowy przepis w art. 41 UoDUiR

3. Przetwarzanie danych o którym mowa w ust. 1 i 1a podlega zabezpieczeniom zapobiegającym nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu i są przechowywane **wyłącznie przez okres niezbędny do oceny ryzyka ubezpieczeniowego i wykonywania umowy ubezpieczenia**.

Przetwarzanie danych wrażliwych - nowe zasady

Dane wrażliwe - dane szczególnej kategorii.

Poszerzony zakres przedmiotowy:

- zabrania się przetwarzania danych osobowych ujawniających: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania **danych genetycznych, danych biometrycznych** w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby.
- przetwarzania danych osobowych dotyczących wyroków **skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa** na podstawie art. 6 ust. 1 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.

Kliknij na podkreślony tekst.

„**Dane biometryczne**" oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech **fizycznych, fizjologicznych lub behawioralnych** osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak **wizerunek twarzy lub dane daktyloskopijne.**

„**Dane genetyczne**" oznaczają dane osobowe dotyczące **odziedziczonych lub nabytych cech genetycznych osoby fizycznej**, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej (pojęcie szersze niż kod genetyczny).

Przetwarzanie szczególnej kategorii danych osobowych

- Wyraźna zgoda osoby, której dane dotyczą.
- Niezbędne do wykonania obowiązków przez administratora i osobę, której dane dotyczą (prawo pracy, zabezpieczenie społeczne, ochrona socjalna).
- Niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej, niezdolnej do wyrażenia zgody osoby.
- Dane członków i byłych członków fundacji, stowarzyszeń i innych niezarobkowych podmiotów w ramach ich uprawnionej działalności.
- Dane upublicznione przez osobę, której dotyczą.
- Niezbędne do ustalenia, dochodzenia lub obrony roszczeń w ramach sprawowania wymiaru sprawiedliwości przez sądy.
- Ważny interes publiczny (wymóg proporcjonalności).
- Niezbędne do profilaktyki zdrowotnej lub medycyny pracy – tajemnica zawodowa.
- Niezbędne ze względu na interes publiczny w dziedzinie zdrowia publicznego. Przetwarzanie danych dotyczących zdrowia z uwagi na względy interesu publicznego

Zgoda jako podstawa przetwarzania danych osobowych

Zgoda osoby, której dane dotyczą oznacza:

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

Zgoda nie może być:

- warunkowa,
- niejednoznaczna,
- „zaszyta" w innych oświadczeniach klienta.

Zgoda jako podstawa przetwarzania danych osobowych

Zgoda osoby, której dane dotyczą oznacza:

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

Zgoda nie może być:

- warunkowa,
- niejednoznaczna,
- „zaszyta" w innych oświadczeniach klienta.

Warunki wyrażenia zgody na przetwarzanie danych

- Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych – kwestie dowodowe!
- Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
- **Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca!**
- Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę.

Wycofanie zgody musi być równie łatwe jak jej wyrażenie.

- Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi 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.

Zgoda „wyraźna" zamiast pisemnej

art. 39 ust. 1 UDUiR

Zakład ubezpieczeń może, za ~~**pisemną**~~ zgodą osoby, której dane dotyczą, albo jej przedstawiciela ustawowego, na ~~**pisemne**~~ żądanie innego zakładu ubezpieczeń, udostępnić temu zakładowi ubezpieczeń przetwarzane przez siebie dane osobowe w zakresie potrzebnym do oceny ryzyka ubezpieczeniowego i weryfikacji danych podanych przez ubezpieczającego, ubezpieczonego lub osobę, na rachunek której ma zostać zawarta umowa ubezpieczenia, ustalenia prawa ubezpieczonego do świadczenia z zawartej umowy ubezpieczenia i wysokości tego świadczenia, a także do udzielenia posiadanych przez siebie informacji o przyczynie śmierci ubezpieczonego lub informacji niezbędnych do ustalenia prawa uprawnionego z umowy ubezpieczenia do świadczenia i jego wysokości.


Zgoda na przetwarzanie danych wrażliwych

- Art. 7 zasady ogólne – administrator musi wykazać, że udzielono zgodę (**kwestie dowodowe**), oddzielne oświadczenie w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, poinformowanie (**przed wyrażeniem zgody**) o możliwości cofnięcia zgody i jego konsekwencjach.

„Wyrażam zgodę na przetwarzanie przez ABC Towarzystwo Ubezpieczeń S.A. z siedzibą w Warszawie (dalej: Administrator danych) danych osobowych dotyczących mojego stanu zdrowia, zawartych we wniosku o ubezpieczenie oraz w innych dokumentach i materiałach przekazanych Administratorowi danych."

„Oświadczam, że zostałem poinformowany, że mogę w dowolnym momencie wycofać zgodę na przetwarzanie moich danych oraz, że wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem."

  - Zgoda udzielona **przez telefon.**
  - Zgoda udzielona **na piśmie.**
  - Zgoda **zeskanowana do TU.**
  - Zgoda udzielona **przez Internet (odhaczenie zgody).**
- Wymogi informacyjne z art. 13 i art. 14 RODO.

Powierzanie danych osobowych - zmiany

Od 25 maja 2018 roku (a więc od momentu rozpoczęcia bezpośredniego stosowania RODO), administrator danych będzie mógł korzystać **wyłącznie z usług takich podmiotów** przetwarzających, które zapewniają **wystarczające gwarancje** wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. W praktyce więc administrator danych na żądanie organu nadzorczego będzie musiał **udowodnić**, że podmiot przetwarzający z którego usług korzysta, spełnia te wymagania.

Ciężar **odpowiedzialności** za wybranie właściwego procesora spoczywa **na administratorze.**

NA DZIEŃ **25.05.2018** WSZYSTKIE UMOWY POWIERZENIA
(W TYM JUŻ OBOWIĄZUJĄCE)
MUSZĄ BYĆ DOSTOSOWANE DO NOWYCH WYMOGÓW

Powierzanie danych osobowych - art. 28 RODO

Zmianie ulegnie zakres szczegółowych elementów jakie będą **musiały się znaleźć w umowie** powierzenia przetwarzania danych. W umowie powierzenia muszą znaleźć się zobowiązania **podmiotu przetwarzającego**, zgodnie z którymi:

- przetwarza on dane osobowe wyłącznie na **udokumentowane polecenie administratora danych** (co dotyczy też ewentualnego przekazywania danych osobowych do państwa trzeciego, chyba że obowiązek taki nakłada na niego prawo Unii lub prawo państwa członkowskiego, któremu podlega podmiot przetwarzający - w takim przypadku przed rozpoczęciem przetwarzania podmiot przetwarzający informuje administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny),
- zapewnia, by **osoby upoważnione** do przetwarzania danych osobowych zobowiązały się do **zachowania tajemnicy** lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy,
- podejmuje wszelkie środki wymagane na mocy **art. 32 RODO**,
- przestrzega warunków korzystania z usług **innego podmiotu przetwarzającego** podwykonawcy.

Powierzanie danych osobowych - art. 28 RODO

- Uwzględniając charakter przetwarzania oraz dostępne mu informacje, pomaga administratorowi danych wywiązać się z obowiązków określonych w art. 32–36 RODO,
- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora danych usuwa lub zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują dalsze przechowywanie tych danych osobowych,
- udostępnia Administratorowi danych wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w niniejszym artykule oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora danych przeprowadzanie audytów, w tym inspekcji, i przyczynia się do nich.

Podpowierzanie danych osobowych - art. 28 RODO
Nowa odpowiedzialność procesora (pośrednika ubezpieczeniowego)

SZERSZA ODPOWIEDZIALNOSĆ PODMIOTU PRZETWARZAJĄCEGO - NOWOŚĆ

Jeżeli podmiot przetwarzający będzie korzystał ze wsparcia swoich podwykonawców (podpowierzał) za zgodą "szczegółową" lub "ogólną", to podwykonawca będzie zobligowany do spełnienia analogicznych wymagań prawnych jak podmiot przetwarzający (art. 28 ust. 4 RODO) . W razie naruszenia swoich obowiązków, pełną odpowiedzialność względem Administratora danych za jego działania lub zaniechania będzie ponosić podmiot przetwarzający. **Podmiot przetwarzający z mocy prawa będzie ponosić pełną odpowiedzialność względem Administratora danych za swoich podwykonawców. Innymi słowy, ścisła kontrola administratora ograniczona zostaje do pierwszego ogniwa łańcucha powierzenia.**

Podpowierzanie danych osobowych - art. 28 RODO

„Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian„

Przepis ten opisuje tzw. podpowierzenie (dalsze powierzenie) tj. sytuację w której podmiot przetwarzający korzysta z usług swoich podwykonawców, w ramach których podwykonawcy również muszą uzyskiwać dostęp do danych osobowych.

Podpowierzanie danych osobowych - art. 28 RODO

O ile podmiot przetwarzający zamierza korzystać z pomocy podwykonawców przy przetwarzaniu powierzonych danych osobowych – istnieją dwie opcje:

- za każdym razem gdy zamierza skorzystać z usług konkretnego podwykonawcy - poinformować o swoim zamiarze administratora danych i poprosić go o zgodę (wówczas będzie to "szczegółowa" zgoda w rozumieniu RODO bo będzie dotyczyła konkretnego podwykonawcy) lub
- ustalić umownie z administratorem danych, że ten co do zasady wyraża zgodę na to by podmiot przetwarzający korzystał ze wsparcia innych podmiotów (podwykonawców), ale pod warunkiem, że Administrator danych o takim zamierzeniu będzie informowany z wyprzedzeniem tak żeby miał możliwość ewentualnie sprzeciwić się na skorzystanie z pomocy konkretnego podwykonawcy ("ogólna" zgoda z RODO). Jeżeli tego sprzeciwu nie zgłosi, a był informowany przez podmiot przetwarzający o zamiarze skorzystania z pomocy podwykonawcy, wówczas taki podwykonawca będzie mógł podjąć współpracę z podmiotem przetwarzającym w zakresie przetwarzania powierzonych danych osobowych.

Podpowierzanie danych osobowych - art. 28 RODO
Nowa odpowiedzialność procesora (pośrednika ubezpieczeniowego)

SZERSZA ODPOWIEDZIALNOSĆ PODMIOTU PRZETWARZAJĄCEGO - NOWOŚĆ

Jeżeli podmiot przetwarzający będzie korzystał ze wsparcia swoich podwykonawców (podpowierzał) za zgodą "szczegółową" lub "ogólną", to podwykonawca będzie zobligowany do spełnienia analogicznych wymagań prawnych jak podmiot przetwarzający (art. 28 ust. 4 RODO) . W razie naruszenia swoich obowiązków, pełną odpowiedzialność względem Administratora danych za jego działania lub zaniechania będzie ponosić podmiot przetwarzający. **Podmiot przetwarzający z mocy prawa będzie ponosić pełną odpowiedzialność względem Administratora danych za swoich podwykonawców. Innymi słowy, ścisła kontrola administratora ograniczona zostaje do pierwszego ogniwa łańcucha powierzenia.**

Podstawowe obowiązki agenta jako podmiotu przetwarzającego dane osobowe

- Agent może przetwarzać powierzone dane wyłącznie na udokumentowane polecenie ZU (administratora tych danych). W przypadku, gdy agent zmieni cel przetwarzania to automatycznie stanie się administratorem powierzonych danych w tym zakresie – ponosi odpowiedzialność jak administrator.
- Agent musi uzyskać pisemną zgodę na podpowierzenie danych.
- Agent musi zapewnić odpowiedni poziom bezpieczeństwa przez podmiot, któremu podpowierzył przetwarzanie danych osobowych - odpowiedzialność za jego uchybienia poniesie agent nie ZU.
- Agent musi zadbać o to by osoby, które zostały upoważnione do przetwarzania powierzonych danych osobowych zachowały je w tajemnicy.
- Agent musi– w miarę możliwości – pomagać ZU wywiązać się z obowiązku odpowiadania na żądania osób, których dane dotyczą.
- Agent po zakończeniu przetwarzania powierzonych danych będzie obowiązany usunąć je lub zwrócić ZU w zależności od jego woli.
- Agent jest zobowiązany do udostępnia ZU wszelkich informacji niezbędnych do wykazania spełnienia obowiązków określonych w RODO oraz umożliwienia ZU lub upoważnionym audytorom przeprowadzenia audytów.

Uprawnienia Prezesa przy stwierdzeniu naruszenia przepisów

- nakazuje uwzględnienie żądań zawartych w skardze osoby, której dane dotyczą,
- nakazuje dostosowanie operacji przetwarzania danych osobowych do przepisów RODO ze wskazaniem, gdzie to właściwe, sposobu i terminu dostosowania,
- nakazuje zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych,
- nakazuje wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych osobowych lub zakazu przetwarzania,
- nakazuje sprostowanie lub usunięcie danych osobowych,
- nakazuje powiadomienie odbiorców, którym dane osobowe zostały ujawnione o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych,
- nakazuje zawieszenie przepływu danych do odbiorców w państwie trzecim lub do organizacji międzynarodowej,
- może udzielić upomnienia, gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia.

Prezes Urzędu Ochrony Danych Osobowych

- Zastąpi Generalnego Inspektora Ochrony Danych Osobowych.
- Przysługuje mu znaczny katalog zadań i uprawnień, w szczególności w zakresie nakładania wysokich kar pieniężnych i przeprowadzania niezapowiedzianych kontroli.
- Szeroki zakres zadań dot. podnoszenia świadomości i wiedzy w zakresie poszanowania prawa do ochrony danych osobowych, wymóg podjęcia szeregu działań edukacyjnych dla osób fizycznych i administratorów.
- Wymóg niezależności organu nadzorczego (aktualnie GIODO jest powoływany przez Sejm za zgodą Senatu).

Uprawnienia Prezesa UODO (II)

W toku postępowania w sprawie naruszenia przepisów o ochronie danych osobowych

- prowadzi postępowanie,
- może **wyznaczyć stronie termin do przedstawienia dowodu będącego w jej posiadaniu, b. wysokie kary w przypadku niezastosowania się!**
- może żądać od strony przedstawienia tłumaczenia na j. polski dokumentacji przedłożonej przez stronę, sporządzonej w j. obcym,
- może **zobowiązać podmiot**, któremu jest zarzucane naruszenie przepisów o ochronie danych osobowych, **do ograniczania przetwarzania danych** w określonym zakresie (forma **niezaskarżalnego** postanowienia; może obowiązywać nawet do zakończenia postępowania głównego).

Uprawnienia Prezesa przy stwierdzeniu naruszenia przepisów

- nakazuje uwzględnienie żądań zawartych w skardze osoby, której dane dotyczą,
- nakazuje dostosowanie operacji przetwarzania danych osobowych do przepisów RODO ze wskazaniem, gdzie to właściwe, sposobu i terminu dostosowania,
- nakazuje zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych,
- nakazuje wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania danych osobowych lub zakazu przetwarzania,
- nakazuje sprostowanie lub usunięcie danych osobowych,
- nakazuje powiadomienie odbiorców, którym dane osobowe zostały ujawnione o sprostowaniu, usunięciu lub ograniczeniu przetwarzania danych,
- nakazuje zawieszenie przepływu danych do odbiorców w państwie trzecim lub do organizacji międzynarodowej,
- może udzielić upomnienia, gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia.

- może udzielić upomnienia, gdy waga naruszenia przepisów o ochronie danych osobowych jest znikoma, a strona zaprzestała naruszenia.

Niezależnie od w/w rozstrzygnięć:

- może nałożyć karę pieniężną.

Postępowanie kontrolne

- Prezes Urzędu może prowadzić kontrolę przestrzegania przepisów o ochronie danych osobowych,
- kontrola może być zaplanowana lub odbyć się **bez uprzedzenia** kontrolowanego,
- nie może trwać dłużej niż miesiąc,
- **kontrolujący ma prawo**:
  - wstępu na grunt oraz do budynków, lokali lub innych pomieszczeń,
  - wglądu do **wszelkich dokumentów i wszelkich informacji** mających bezpośredni związek z przedmiotem kontroli,
  - przeprowadzania oględzin urządzeń, nośników oraz systemów informatycznych lub teleinformatycznych służących do przetwarzania danych,
  - żądać złożenia pisemnych lub ustnych wyjaśnień oraz **wzywać i przesłuchiwać w charakterze świadka** osoby w zakresie niezbędnym do ustalenia stanu faktycznego.

W razie stwierdzenia w toku postępowania kontrolnego naruszenia przepisów o ochronie danych osobowych Prezes Urzędu niezwłocznie wszczyna postępowanie.

Wysokość administracyjnych kar pieniężnych

Skuteczne, proporcjonalne, odstraszające w każdym indywidualnym przypadku.

- Kara w wysokości **do 10 000 000 EUR**, a w przypadku przedsiębiorstwa – w wysokości **do 2 % jego całkowitego rocznego światowego obrotu** z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa:
  - naruszenie obowiązków administratora i podmiotu przetwarzającego, o których mowa w art. 8, 11, 25 –39 oraz 42 i 43,
  - naruszenie obowiązków podmiotu certyfikującego, o których mowa w art. 42 oraz 43,
  - naruszenie obowiązków podmiotu monitorującego, o których mowa w art. 41 ust. 4.
- Kara w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, za naruszenie:
  - podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9,
  - praw osób, których dane dotyczą, o których mowa w art. 12–22,

- Kara w wysokości do 20 000 000 EUR, a w przypadku przedsiębiorstwa – w wysokości do 4 % jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, przy czym zastosowanie ma kwota wyższa, za naruszenie:
  - podstawowych zasad przetwarzania, w tym warunków zgody, o których to zasadach i warunkach mowa w art. 5, 6, 7 oraz 9,
  - praw osób, których dane dotyczą, o których mowa w art. 12–22,
  - przekazywania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej, o którym to przekazywaniu mowa w art. 44–49,
  - wszelkich obowiązków wynikających z prawa państwa członkowskiego przyjętego na podstawie rozdziału IX,
  - nieprzestrzegania nakazu, tymczasowego lub ostatecznego ograniczenia przetwarzania lub zawieszenia przepływu danych orzeczonego przez organ nadzorczy na podstawie art. 58 ust. 2 lub niezapewnienia dostępu skutkującego naruszeniem art. 58 ust. 1.

Prawo wniesienia skargi do Prezesa UODO i sądu administracyjnego

- Wynika bezpośrednio z RODO (art. 77 i 78).
- **Każda osoba, której dane dotyczą, ma prawo wnieść skargę do organu nadzorczego**, w szczególności w państwie członkowskim swojego zwykłego pobytu, swojego miejsca pracy lub miejsca popełnienia domniemanego naruszenia, jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczące narusza RODO.
- Prezes UODO informuje skarżącego o postępach i efektach rozpatrywania skargi, w tym o możliwości skorzystania z sądowego środka ochrony prawnej na mocy art. 78 (skarga do sądu administracyjnego na wydaną w sprawie wiążącą decyzję, gdy strona jest niezadowolona z rozstrzygnięcia).
- Skarga do sądu administracyjnego przysługuje także, gdy organ nie rozpatrzył skargi lub nie poinformował osoby, której dane dotyczą w terminie 3 miesięcy o postępach lub efektach rozpatrywania skargi.

Rozporządzenie o ochronie danych osobowych - RODO

- 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 (ogólne rozporządzenie o ochronie danych).
- Ma zastosowanie od dnia **25 maja 2018 r.** – od tej daty wszystkie Państwa Członkowskie mają obowiązek stosować bezpośrednio przepisy RODO.
- Projekt ustawy o ochronie danych osobowych z dnia 12 września 2017 r. i Projekt przepisów wprowadzających (trwa etap uzgodnień i konsultacji publicznych).