Fundusze Europejskie Program Regionalny

Rzeczpospolita Polska

promuje łódzkie

Unia Europejska Europejski Fundusz Społeczny

Ochrona danych osobowych po zmianach unijnego Rozporządzenia o Ochronie Danych Osobowych (RODO)

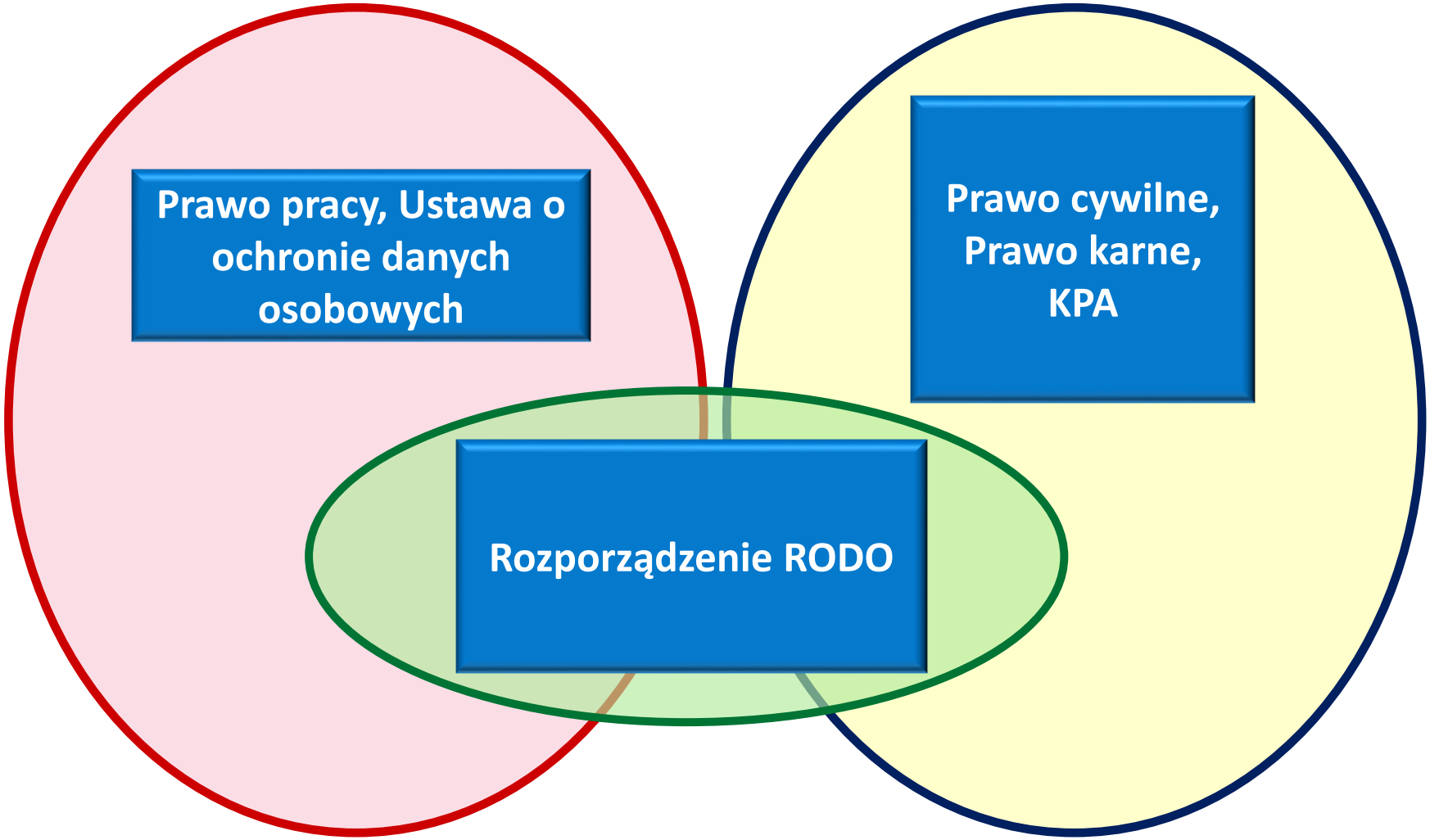
Opracowanie: Maciej Kasperowicz

Łódź, 25.07.2018 r.

Podstawy prawne

- 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
- Ustawy:
- O ochronie danych osobowych
- Kodeks pracy
- O dostępie do informacji publicznej
- KPA
- Kodeks karny
- Kodeks cywilny
- O rehabilitacji społecznej i zawodowej oraz zatrudnianiu osób niepełnosprawnych
- Orzecznictwo NSA i SN

Prawo


Prawo pracy, Ustawa o ochronie danych osobowych
Prawo cywilne, Prawo karne, KPA
Rozporządzenie RODO

Najważniejsze zmiany w ochronie danych osobowych

RODO wprowadza obowiązek:

- Stosowania identycznego prawa w całej UE
- Konieczności stosowania przystępnego, jasnego i zrozumiałego języka przez administratorów danych
- Pośrednio, poprzez Rozporządzenie, zmieni się organ ODO w Polsce – zniknie GIODO, a w jego miejsce powstanie UODO z Prezesem UODO na czele
- Stosowania nowych sankcji za naruszenie danych osobowych
- Możliwości ubiegania się o odszkodowanie za naruszenie danych osobowych

Najważniejsze zmiany w ochronie danych osobowych

RODO wprowadza obowiązek:

- Wprowadzenia nowej dokumentacji ODO, tzw. rejestru czynności przetwarzania danych osobowych
- Powołania Inspektora Ochrony Danych
- Obowiązek dokonania oceny wpływu przetwarzania danych osobowych i oszacowania związanego z tym ryzyka
- Usuwania danych osobowych – w konkretnych sytuacjach
- Stosowania szerszego katalogu „danych szczególnej kategorii”

Najważniejsze zmiany w ochronie danych osobowych

RODO wprowadza obowiązek:

- Stosowania nowego trybu obowiązku informacyjnego
- Stosowania nowych procedur dot. wyrażenia zgody na przetwarzanie danych osobowych

Dane osobowe

Czy imię i nazwisko to dane osobowe?

- 410 000 ludzi nosi nazwisko Kowalski albo Nowak

Czym są dane osobowe wg. ustawy z 1997 r.

- Za dane osobowe uważa się :
- wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej

Dane osobowe

- Numery identyfikacyjne:
- **PESEL, NIP, paszport, dowód osobisty**
- Cechy fizyczne:
- **wygląd zewnętrzny, siatkówka oka, linie papilarne,**
- Cechy fizjologiczne:
- **grupa krwi, kod genetyczny**
- Cechy ekonomiczne:
- **status majątkowy, lista zaległości finansowych**
- Cechy umysłowe, kulturowe lub społeczne
- **poglądy, wyznanie, pochodzenie lub przynależność związkowa**

Ustawa z 1997 r. dzieli dane osobowe na dane zwykłe i wrażliwe

- Dane osobowe dzielą się na zwykłe i wrażliwe, do których zalicza się zgodnie z art. 27 ust. 1 u.o.d.o. informacje dotyczące:
- pochodzenia rasowego lub etnicznego,
- poglądów politycznych,
- przekonań religijnych lub filozoficznych,
- przynależności wyznaniowej, partyjnej lub związkowej,
- stanu zdrowia,
- kodu genetycznego,
- nałogów,
- życia seksualnego,
- skazań,
- orzeczeń o ukaraniu w postępowaniu sądowym lub administracyjnym.

- Przepisy nie zawierają natomiast katalogu „zwykłych” (czyli innych niż wrażliwe) danych osobowych.

Dane osobowe wg. RODO

- dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
- możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak
- imię i nazwisko,
- numer identyfikacyjny,
- dane o lokalizacji,
- identyfikator internetowy lub
- jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;

Osoba możliwa do zidentyfikowania

- Informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu (podobnie kwestię tą rozpatrywano w art. 6 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych)

Kogo dotyczy ochrona danych osobowych

- Ochrona danych osobowych dotyczy wyłącznie osób fizycznych
- Nie dotyczy zatem przedsiębiorców, zarówno tych prowadzących jednoosobową działalność gospod. jak i spółek
- **Gdy osoba fizyczna prowadzi działalność gospodarczą pod firmą swojego nazwiska (staje się tym samym przedsiębiorcą czyli podmiotem gospodarczym) w pierwszym rzędzie korzysta z ochrony jaką ustawodawca zapewnia przedsiębiorcy.** (I SA/Wa 1584/09 – Wyrok WSA z 24.11.2009).
- Zgodnie z motywem 18 przedsiębiorca" oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeszenia prowadzące regularną działalność gospodarczą

Kogo dotyczy ochrona danych osobowych

- Ochrona danych osobowych dotyczy wyłącznie osób żywych.
- Ochrona informacji dotyczących osób zmarłych odbywa się natomiast na podstawie przepisów Kodeksu cywilnego – dotyczących ochrony dóbr osobistych (art. 23 k.c.)

Dane osobowe szczególnej kategorii

- Dane wrażliwe w ustawie nie miały własnej nazwy, za to w RODO zostały określone jako **dane szczególnej kategorii**.
- Zgodnie z art. 9 ust. 1 Rozporządzenia RODO zabrania się przetwarzania danych osobowych ujawniających:
- pochodzenie rasowe lub etniczne,
- poglądy polityczne,
- przekonania religijne lub światopoglądowe,
- przynależność do związków zawodowych,

- a także przetwarzania:
- danych genetycznych,
- danych biometrycznych, w celu jednoznacznego zidentyfikowania osoby albo:
- danych dotyczących zdrowia,
- seksualności oraz orientacji seksualnej.

Czym są dane biometryczne

- owal twarzy,
- oczy, usta, uszy
- sposób chodzenia,
- sposób mówienia
- gesty
- podpis odręczny,
- sposób pisania na klawiaturze,

Przetwarzanie danych

Pod pojęciem przetwarzania danych rozumie się: jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych

W konsekwencji powyższych definicji uznać należy, iż każda czynność wykonywana na przekazanych danych osobowych, powinna podlegać zasadom określonym w Ustawie.

Zasady przetwarzania danych osobowych

- Główne zasady postępowania przy przetwarzaniu danych osobowych.
- Instytucja ma przestrzegać m.in. zasad:
- legalności
- celowości
- merytorycznej poprawności
- adekwatności danych
- ograniczenia czasowego

Zasada celowości

- Zasada ta oznacza, iż zbieranie danych osobowych powinno być dokonywane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami. Oznacza to, iż:
- nie można określać celu przetwarzania danych w sposób ogólnikowy,
- cel ten powinien być zakomunikowany zainteresowanemu przed tym zebraniem danych osobowych,
- niedopuszczalne jest uzależnianie zawarcia umowy od wyrażenia zgody na przetwarzanie danych w zupełnie innych celach (np.marketingu produktów i usług podmiotów trzecich).

Zasada merytorycznej poprawności (prawdziwości)

- Administrator danych jest obowiązany zapewnić poprawność danych osobowych, tj. aby dane były zgodne z prawdą, pełne (kompletne) i aktualne.
- W celu zapewnienia merytorycznej poprawności danych konieczne jest aby w procesie przetwarzania danych procesor:
- każdorazowo oceniał wiarygodność źródła pozyskania danych,
- wypracował tryb weryfikowania prawdziwości danych oraz ustalił zasady postępowania w przypadku stwierdzenia nieprawdziwości danych.
- Naruszeniem tej zasady jest zbieranie danych ze źródeł niewiadomego pochodzenia, które nie gwarantują poprawności danych osobowych.

- Ważne : miejsce zamieszkania!!!!

Zasada ograniczenia czasowego

- Rozporządzenie RODO nakłada na administratora danych obowiązek przechowywania danych w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż to jest niezbędne do osiągnięcia celu przetwarzania.
- Po osiągnięciu celu (np.wykonaniu zawartej umowy, upływie wskazanego w przepisach prawa okresu przechowywania danych) dane powinny zostać usunięte.
- Przykładowo, w kontekście przetwarzania danych osobowych przez Biuro Informacji Kredytowej Sąd wskazał, iż „(…) z chwilą całkowitej spłaty kredytu (zamknięcia rachunku bankowego) kończy się prawne zezwolenie na przetwarzanie danych osobowych tych osób, których rachunki zostały zamknięte.

Informowanie osób, których dane dotyczą

Zgodnie z RODO podczas zbierania danych należy poinformować osobę o:

- inspektorze ochrony danych, jeżeli istnieje
- podstawie prawnej przetwarzania,
- prawnie uzasadnionym interesie administratora, jeżeli na tej podstawie odbywa się przetwarzanie,
- informacji o zamiarze przekazywania danych do państwa trzeciego,
- okresie, przez który dane osobowe będą przechowywane, bądź kryteria ustalania tego okresu,
- profilowaniu,
- o prawie wniesienia skargi do organu nadzorczego,
- w przypadku istnienia obowiązku podania danych osobowych: wskazaniu ewentualnych konsekwencji niepodania danych,

Informowanie osób, których dane dotyczą

Zgodnie z RODO podczas zbierania danych należy poinformować osobę o:

- prawach osoby, której dane dotyczą, tj. prawie do:
- usunięcia danych,
- ograniczenia przetwarzania,
- prawie przenoszenia danych,
- prawie do cofnięcia zgody (gdy osoba, której dane dotyczą wyraża zgodę na przetwarzanie danych).

Zgoda na przetwarzanie danych
Jak było do tej pory

W polskim prawie dotychczasowa definicja brzmiała następująco:

- to oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie;
- zgoda nie może być domniemana lub dorozumiana.

- Dopuszczalne były sytuacje w których np.: domyślnie zaznaczone już było przez system okienko wyrażenia zgody

Zgoda na przetwarzanie danych Zmiany w RODO

W art. 4 pkt 11 RODO wskazano, że zgodą jest:

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

- domyślnie zaznaczone przez system okienko wyrażenia zgody **odchodzi**

Techniczne środki zabezpieczenia danych osobowych

- dane na dyskach przenośnych (CD/DVD, pendrive) muszą być zabezpieczone hasłem a po ich wykorzystaniu kasowane,
- zabronione jest kopiowanie danych osobowych na dowolnego typu przenośne nośniki zewnętrzne (pamięci flash, przenośne dyski, płyty CD/DVD, taśmy, urządzenia mobilne); dopuszcza się jedynie służbowe nośniki zewnętrzne, zaszyfrowane,
- pliki zawierające dane osobowe zabezpieczone są hasłem znanym tylko osobie upoważnionej do przetwarzania danych
- „polityka czystego ekranu” -pracownik opuszcza stanowisko pracy, na którym przetwarzane były dane osobowe, dopiero po zablokowaniu stacji roboczej (CTRL+ALT+DELATE),
- hasła wymagane do uwierzytelniania się w systemie przetwarzającym dane osobowe i na stacji roboczej są hasłami mocnymi – adekwatne do zagrożeń, niesłownikowe, które nie nawiązują do informacji o danym użytkowniku, jego bliskich, miejscu zatrudnienia itp.

Hasła mocne

- HASŁA MOCNE są to hasła, które ciężko jest złamać.
- Hasło mocne jest hasłem nie słownikowym (nie zawiera słów);
- **nie nawiązuje:** do imienia, pseudonimów użytkowników i jego bliskich (np. dzieci), nazw pupili, dat urodzenia, tablic rejestracyjnych, numerów telefonów, miesięcy i roku (np. LUTY2017!), miejsca pracy (np. Lubelskie1!);
- nie zawiera więcej niż 2 takich samych znaków; nie zawiera ciągów cyfr (np. 123456…) czy liter (np. abc…, xyz…);
- kolejne hasła nie przypominają poprzedniego (np. Lubelskie1!, Lubelskie2!, Lubelskie3!); w celu wzmocnienia hasła można stosować: cyfry i znaki specjalne zamiast liter np. o=0, 1=!,a=@, B=3, S=$ itd.;

Przykład

- @n!@
- K@$!@

Techniczne środki zabezpieczenia danych osobowych

- ekrany komputerów ustawione są w sposób uniemożliwiający osobom postronnym oglądanie ich zawartości,
- pracownik kończy pracę lub opuszcza stanowisko pracy, na którym przetwarzane były dane, dopiero po wylogowaniu się z aplikacji i z systemu operacyjnego,
- przetwarzanie danych osobowych odbywa się tylko w wyznaczonych do tego celu pomieszczeniach służbowych
- zbiory danych osobowych oraz wszelkie ich wypisy nie są wynoszone z Urzędu na jakichkolwiek nośnikach ani w postaci papierowej, bez uprzedniej zgody,
- wydruki zawierające dane po zakończeniu pracy niszczone są w sposób uniemożliwiający ich odczytanie (w niszczarce),
- kopie zapasowe danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco,

Kontrola i sankcje

Uprawnienia kontrolne Biura GIODO

Wstęp do pomieszczeń w których przechowywany jest zbiór danych osobowych w godz. **6.00 – 22.00**;

Żądanie złożenia wyjaśnień pisemnych lub ustnych w celu ustalenia stanu faktycznego;

Wgląd do wszelkich dokumentów;

Przeprowadzenia oględzin urządzeń, nośników etc.

Zlecanie sporządzania ekspertyz i opinii.

Odpowiedzialność

Art. 49.

1. Kto przetwarza w zbiorze dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do których przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
2. Jeżeli czyn określony w ust. 1 dotyczy danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia **wolności do lat 3.**