

Zmiany w prawie o ochronie danych osobowych

informacje ważne dla kadrowych

Wejście w życie i obowiązywanie RODO

- 4 maja 2016 r. – publikacja w Dzienniku Urzędowym UE
- 24 maja 2016 r. – wejście w życie (20 dni od daty publikacji)
- 25 maja 2018 r. – stosowanie przepisów RODO w państwach Unii Europejskiej (tj. w terminie 2 lat licząc od 24 maja 2016 r.)
- Nowe przepisy będą stosowane także wobec przetwarzania danych osobowych zebranych przed wejściem w życie RODO

Motyw nr 171

„Przetwarzanie, które w dniu rozpoczęcia stosowania niniejszego rozporządzenia już się toczy, powinno w terminie dwóch lat od wejścia niniejszego rozporządzenia w życie zostać dostosowane do jego przepisów.”

Zakres podmiotowy

- Zakres podmiotowy obejmuje jedynie **dane osobowe dotyczących osób fizycznych**.
- Obowiązek ochrony danych nałożony jest na **wszystkie podmioty, które przetwarzają dane osobowe**, a w szczególności:
 - a) Podmioty publiczne (np. organy państwowe czy samorządowe),
 - b) Podmioty prywatne (spółki, spółdzielnie czy fundacje),
 - c) Podmioty niepubliczne realizujące zadania publiczne (prywatne przedszkola),
 - d) Osoby fizyczne.

Zakres terytorialny

- Zakres terytorialny RODO obejmuje przetwarzanie danych osobowych przez administratora lub procesora w związku z jego działalnością w Unii Europejskiej, **bez względu na to czy przetwarzanie ma miejsce w Unii Europejskiej**.
- Obejmuje również - przetwarzanie danych osobowych **osób będących w Unii Europejskiej** przez podmioty, które nie posiadają na terenie Unii Europejskiej jednostek organizacyjnych, ale przetwarzanie związane jest z:
 - a) **Oferowaniem** dóbr i usług osobom z Unii Europejskiej, niezależnie od tego, czy wymaga się od tych osób zapłaty,
 - b) **Monitorowaniem** ich zachowania, o ile do zachowania dochodzi w Unii Europejskiej.

RODO – skutki prawne

- **Uchylenie** dyrektywy 95/46/WE oraz ustawy o ochronie danych osobowych.
- **Bezpośrednie stosowanie** przepisów Rozporządzenia w państwach członkowskich UE.
- **Niezbędne** wprowadzenie dodatkowych przepisów krajowych o charakterze uzupełniającym.

RODO – skutki prawne

Przepisy krajowe towarzyszące wdrożeniu RODO mogą być:

- a) obligatoryjne – „państwa członkowskie przyjmują przepisy...”
- b) fakultatywne – „państwa członkowskie mogą zachować lub wprowadzić bardziej szczegółowe przepisy”

Fakultatywne przepisy krajowe odnoszące się do danych pracowniczych

•art. 88

a)ust.1 Państwa członkowskie **mogą** zawrzeć w swoich przepisach lub w porozumieniach zbiorowych bardziej **szczegółowe** przepisy mające zapewnić ochronę praw i wolności **w przypadku przetwarzania danych osobowych pracowników w związku z zatrudnieniem**, w szczególności do celów rekrutacji, wykonania umowy o pracę, w tym wykonania obowiązków określonych przepisami lub porozumieniami zbiorowymi, zarządzania, planowania i organizacji pracy, równości i różnorodności w miejscu pracy, bezpieczeństwa i higieny pracy, ochrony własności pracodawcy lub klienta oraz do celów indywidualnego lub zbiorowego wykonywania praw i korzystania ze świadczeń związanych z zatrudnieniem, a także do celów zakończenia stosunku pracy.

b)ust. 2 Przepisy te muszą obejmować odpowiednie i szczegółowe środki zapewniające osobie, której dane dotyczą, poszanowanie jej godności, prawnie uzasadnionych interesów i praw podstawowych, **w szczególności pod względem przejrzystości przetwarzania, przekazywania danych osobowych w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą oraz systemów monitorujących w miejscu pracy.**

Zakres niezmienny przez RODO

- Definicja danych osobowych,
- Warunki uznania podmiotów za administratorów danych i podmioty przetwarzające dane,
- Rozdział obowiązków informacyjnych uzależniony od tego, czy dane są zbierane od osoby, której dotyczą czy też w inny sposób,
- Reguły i mechanizmy dot. transferu danych osobowych do państw trzecich,
- Regulacje dot. statusu i zadań ABl (Inspektor Ochrony Danych Osobowych),
- Zasady szczególnej staranności związane z przetwarzaniem danych osobowych,
- Wykaz podstaw prawnych regulujących przetwarzanie danych (**pewne zmiany co do przesłanki zgody i usprawiedliwionego celu**).

Dane pracownicze – najważniejsze zmiany

- W zakresie **podstaw prawnych** przetwarzania danych – konstrukcja prawna zgody i przesłanka usprawiedliwionego celu
- **Obowiązek pseudonimizacji danych**
- Rozszerzenie zakresu **obowiązków informacyjnych**
- Poszerzenie **prawa dostępu do danych**
- **Nowe prawa** podmiotów danych osobowych
- Modyfikacja zasad **profilowania danych**
- Doprecyzowanie relacji **administrator – procesor**
- Obowiązek powiadomienia o **naruszeniach ochrony danych osobowych**
- **Nowe sankcje** administracyjne i cywilnoprawne

Podstawy prawne przetwarzania danych „zwykłych”

• Musi być spełniony **co najmniej jeden** z poniższych warunków

a) **osoba**, której dane dotyczą **wyraziła zgodę** na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) przetwarzanie jest **niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze**;

d) przetwarzanie jest **niezbędne do ochrony żywotnych interesów osoby**, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest **niezbędne do wykonania zadania realizowanego w interesie publicznym** lub w ramach sprawowania władzy publicznej powierzonej administratorowi;

f) przetwarzanie jest **niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią**, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Podstawy prawne przetwarzania danych „zwykłych”

- Co się zmienia?
- nowa konstrukcja prawna i ogólne warunki wyrażenia zgody
- doprecyzowana przesłanka usprawiedliwionego celu

Zgoda podmiotu danych

art. 4 pkt. 11 RODO

- „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”
- Jeśli przetwarzanie odbywa się na podstawie zgody osoby, której dane dotyczą, administrator powinien **być w stanie wykazać**, że osoba, której dane dotyczą, wyraziła zgodę na operację przetwarzania.

Zgoda podmiotu danych

- Wystąpienie przez administratora o udzielenie przez podmiot danych zgody na przetwarzanie danych w określonym celu powinno następować wyłącznie w przypadkach, gdy zgoda ma być jedyną podstawą prawną przetwarzania. Jeżeli **przetwarzanie danych jest ustawowym obowiązkiem albo uprawnieniem administratora** lub jest niezbędne do wykonania umowy (tj. nastąpi na innej podstawie prawnej niż zgoda podmiotu danych), to nie należy podmiotowi danych sugerować prawa odmowy wyrażenia zgody.
- Możliwość **wyrażenia zgody musi towarzyszyć faktyczna**, a nie iluzoryczna możliwość odmowy.

Zgoda podmiotu danych

Sposób wyrażenia zgody:

1.oświadczenie woli,

2.zgoda konkludentna – wyrażana poprzez działanie dostatecznie ujawniające zamiar udzielenia zgody (okoliczności udzielenia zgody, zwyczaje w danej branży)

–przykładem jest samodzielne umieszczenie przez pracowników zdjęć w bazie kontaktów w intranecie, po otrzymaniu id pracodawcy informacji, że jest taka możliwość; zaznaczenie okienka wyboru podczas przeglądania strony internetowej.

–Milczenie, okienka domyślnie zaznaczone lub niepodjęcie działania **nie** powinny zatem oznaczać zgody.

Zgoda podmiotu danych

Charakter dobrowolnej zgody

- a) Aby wyrażenie zgody było świadome, osoba, której dane dotyczą, powinna znać przynajmniej tożsamość administratora oraz zamierzone cele przetwarzania danych osobowych.
- b) Wyrażenia zgody nie należy uznawać za dobrowolne, jeżeli osoba, której dane dotyczą, nie ma rzeczywistego lub wolnego wyboru oraz nie może odmówić ani wycofać zgody bez niekorzystnych konsekwencji.
- c) Aby zapewnić dobrowolność, zgoda nie powinna stanowić ważnej podstawy prawnej przetwarzania danych osobowych w szczególnej sytuacji, w której istnieje wyraźny brak równowagi między osobą, której dane dotyczą, a administratorem.

Zgoda podmiotu danych

Zdaniem Grupy Roboczej 29

•*"(...) pracodawca popełnia błąd, jeśli próbuje zalegalizować przetwarzanie danych pochodzących od pracownika za pomocą uzyskanej od pracownika zgody. Można posłużyć się zgodą, jeśli odnosi się ona do przypadku, w którym pracownik ma całkowitą swobodę jej udzielenia i może odmówić udzielenia takiej zgody bez poniesienia szkody".*

Zgoda podmiotu danych

Zgoda musi być **jednoznaczna oraz świadoma**, co oznacza, że:

- osoba wyraziła zgodę na przetwarzanie swoich danych osobowych **w jednym lub większej liczbie określonych celów** (art. 6 ust. 1),
- osoba jest **świadoma wyrażenia zgody oraz jej zakresu** (motyw nr 42),
- oświadczenie o wyrażeniu zgody przygotowane przez administratora powinno mieć zrozumiałą i łatwo dostępną formę, być sformułowane **jasnym i prostym językiem i nie powinno zawierać nieuczciwych warunków** (motyw nr 42).

Wycofanie zgody podmiotu danych

- Podmiot danych ma **prawo w dowolnym momencie wycofać** udzieloną wcześniej zgodę na przetwarzanie danych;
- Wycofanie zgody **nie wpływa na dotychczasową zgodność z prawem przetwarzania** prowadzonego na podstawie zgody przed jej wycofaniem (*skutek ex nunc*);
- Wycofanie zgody musi być równie **łatwe**, jak jej wyrażenie – niedopuszczalne jest stawianie sztucznych nieuzasadnionych barier dla odwołania zgody.

Wycofanie zgody podmiotu danych

Możliwość odwołania zgody powoduje, że oparcie na zgodzie systemu przetwarzania danych, np. **systematycznych transferów danych w ramach grup spółek korzystających ze wspólnych baz** jest ryzykowne – gdy administrator nie dysponuje inną podstawą prawną przetwarzania danych, odwołanie zgody choćby przez jedną osobę, której dane są przetwarzane, może podważyć wdrożony system.

Przesłanka usprawiedliwionego celu

Trzy warunki posłużenia się tą przesłanką:

- a) Cel musi być prawnie **usprawiedliwiony**;
- b) Dane muszą być **niezbędne** do spełnienia tego celu (zasada „adekwatności”);
- c) Usprawiedliwiony interes **nie jest podrzędny** wobec interesów lub podstawowych praw i wolności podmiotu danych.

Przesłanka usprawiedliwionego celu

- Usprawiedliwiony cel występuje w przypadku:
 - a) Przesyłania danych osobowych w ramach grupy przedsiębiorstw do wewnętrznych celów administracyjnych, co dotyczy też przetwarzania danych pracowników (!!!);
 - b) Gdy dane są niezbędne do zapobiegania oszustwom;
 - c) „Własnego” marketingu bezpośredniego;
 - d) Gdy jest to niezbędne dla zapewnienia bezpieczeństwa sieci i informacji.
- Jest to otwarty katalog definiowany przez administratora danych.

Podstawy prawne przetwarzania danych wrażliwych

- Przetwarzanie danych wrażliwych jest co do zasady zabronione, chyba że zostanie spełniony jeden z warunków określonych w art. 9. ust. 2 (brak otwartej przesłanki uzasadnionego celu).
- **Dane o niekaralności** nie należą do kategorii danych wrażliwych, ale również są danymi szczególnie chronionymi, których przetwarzania jest **dopuszczalne 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 (art. 10).

Podstawy prawne przetwarzania danych wrażliwych

art. 9 ust. 2 pkt. B)

„przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej (...)”

Czy można posłużyć się zgodą?

Podstawy prawne przetwarzania danych wrażliwych

Art. 9 ust. 2 pkt. A)

• „osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1”

• Wyraźna zgoda (opt-in)

- a) wyrażona może być na piśmie lub ustnie;
- b) tzw. zgoda konkludentna (dorozumiana) nie jest wystarczająca.

Obowiązek pseudonimizacji danych

- Zgodnie z art. 4 pkt 5 RODO „pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, **bez użycia dodatkowych informacji**, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
- Pseudonimizacja polega na **zakryciu lub zastąpieniu informacjami niezrozumiałymi dla odbiorcy**, na przykład inicjały imion osób lub pierwsze litery nazw miast.

Zastosowanie przy przejściu zakładu pracy.

Rozszerzenie zakresu obowiązków informacyjnych

- Informacje mają być przekazywane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, na piśmie lub w inny sposób np. elektronicznie, ustnie na żądanie osoby, której dane dotyczą.
- Co do zasady **nieodpłatnie**.

Rozszerzenie zakresu obowiązków informacyjnych

Zakres informacji, które mają być podane przy zbieraniu danych (art. 13 i 14) **znacznie rozszerzony**:

- Nie tylko oznaczenie administratora danych, ale także **dane kontaktowe ABl/inspektora ochrony danych**.
- Nie tylko cel przetwarzania, ale także **podstawa prawna przetwarzania**.
- **Wskazanie uzasadnionych interesów** jeżeli są one podstawą przetwarzania.
- Nie tylko pouczenie o prawie dostępu do danych, korekty i sprzeciwu, ale również o **prawie do cofnięcia zgody**, jeżeli jest ona podstawą przetwarzania oraz o **prawie wniesienia skargi do organu nadzorczego**.
- Informacja o **zamiarze przekazania danych do państwa trzeciego** oraz o gwarancjach odpowiedniego poziomu ochrony danych w tym państwie.
- O **okresie przechowywania danych** lub kryteriach jego ustalania.
- O **profilowaniu**.

Rozszerzenie zakresu obowiązków informacyjnych

W przypadku pozyskiwania danych nie od osoby, której dotyczą należy poinformować o **kategoriach** pozyskanych danych i tak jak dotychczas o **źródle pochodzenia danych** (w tym czy pochodzą ze źródeł publicznie dostępnych).

ALE zmienił się termin przekazania tych danych co może mieć znaczenie dla wewnętrznych postępowań wyjaśniających (*whistleblowing*):

- Poprzednio: „*bezpośrednio po utrwaleniu zebranych danych*”
- Obecnie: „*w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych*”

Poszerzenie prawa dostępu do danych

- Przekazanie podmiotowi danych **na jego żądanie** określonych informacji, których zakres został rozszerzony analogicznie do katalogu informacji przekazywanych przy zbieraniu danych (art. 13 i 14)
- Sposób realizacji prawa dostępu do danych (art. 15 ust.3)
 - a) Dostarczenie przez Administratora osobie, której dane dotyczą, jedną kopię danych osobowych podlegających przetwarzaniu.
 - b) Za wszelkie kolejne kopie administrator **może pobrać opłatę** w rozsądnej wysokości wynikającej z kosztów administracyjnych.
 - c) Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, **informacji udziela się powszechnie stosowaną drogą elektroniczną.**

Nowe prawa podmiotów danych

- Prawo do bycia zapomnianym (art. 17)
- Prawo do ograniczenia przetwarzania (art. 18)
- Prawo do przenoszenia danych (art. 20)

Prawo do bycia zapomnianym (art. 17)

- Prawo żądania od administratora danych usunięcia danych, w sytuacji gdy:
 - a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
 - b) osoba, której dotyczą dane cofnęła zgodę i nie ma już innej podstawy przetwarzania;
 - c) osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 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.
- W przypadku „upublicznienia” danych przez administratora, obowiązek poinformowania innych administratorów o żądaniu usunięcia danych.
- Prawo do bycia zapomnianym nie jest bezwzględne i w pewnych sytuacjach nie znajduje zastosowania (przypadki wymienione w art. 17 ust. 3).

Prawo do przenoszenia danych (art. 20)

- Podmiot danych jest uprawniony do otrzymania od administratora w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące oraz do przesłania ich innemu administratorowi bez przeszkód ze strony obecnego administratora.
- Również prawo do żądania transferu przenoszonych danych osobowych wprost przez administratora bezpośrednio kolejnemu administratorowi, jeżeli jest to technicznie możliwe.
- Dotyczy tylko przetwarzania prowadzonego w sposób zautomatyzowany.
- Obejmuje tylko dane, które zostały dostarczone administratorowi przez podmiot danych, natomiast nie są to dane zebrane przez administratora z innego źródła.

Relacja Administrator - Processor

- Administrator ma obowiązek korzystania tylko 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.
- Podstawą przetwarzania jest umowa (art. 28 ust. 3) – jej treść została istotnie zmodyfikowana (konieczność weryfikacji umów!!!!).
- KE oraz GIODO otrzymały kompetencje do wydawania **standardowych klauzul umownych** dotyczących relacji administrator-processor (podmioty przetwarzające mogą, ale nie muszą z nich korzystać).

Relacja Processor - Subprocessor

- Podpowierzenie danych (subprocessing) jest dopuszczalne wyłącznie za zgodą (ogólną lub szczegółową) administratora
- Na subprocessora zostają nałożone takie same obowiązki ochrony danych jak w umowie między administratorem a processorem.
- Jeżeli subprocessor nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec administratora za wypełnienie obowiązków subprocessora spoczywa na procesorze.

Nowe sankcje administracyjne i cywilnoprawne

- RODO przewiduje sankcje administracyjne i cywilnoprawne (każda osoba ma prawo uzyskać odszkodowanie).
- Regulacje prawa krajowego przewidują również sankcje karne.

Nowe sankcje administracyjne i cywilnoprawne

- Dwa rodzaje stosowanych kar pieniężnych:
 - a) Administracyjna kara pieniężna 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.
 - b) Administracyjna kara pieniężna 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.

Naruszenie warunków zgody i podstawowych zasad, praw osób, których dane dotyczą, przekazywania danych do państw trzecich

Edyta Jagiełło

radca prawny

Zajmuje się bieżącą obsługą spółek w zakresie prawa pracy oraz doradza Klientom w obszarach ochrony danych osobowych pracowników, w tym przetwarzania danych osobowych w grupach kapitałowych, włącznie z transferem danych za granicę. Obszar jej specjalizacji obejmuje także pracowniczoprawne zagadnienia związane z międzynarodowymi transferami przedsiębiorstw. Jej Klientami są między innymi wiodące spółki z branży IT, farmaceutycznej i turystycznej.



RACZKOWSKI PARUCH | Ius Laboris
Poland | Global HR Lawyers
ul. Bonifraterska 17, 00-203 Warszawa

M +48 668 806 152 | **T** +48 22 380 42 50 |
F +48 22 380 42 51
edyta.jagiello@raczkowski.eu