Szanowni Państwo,

W polskim porządku prawnym od 25 maja 2018 r., będzie bezpośrednio stosowane 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, zwane w dalszej części poradnika **Rozporządzeniem** lub **RODO**.

Głęboka reforma systemu ochrony danych osobowych ma niewątpliwie wpływ na postrzeganie całej problematyki ochrony danych osobowych, a zwłaszcza legalności ich przetwarzania.
Wraz z rozpoczęciem stosowania RODO wchodzimy w zupełnie inny reżim prawny ochrony danych osobowych, co przełoży się na daleko idące konsekwencje prawne i biznesowe.

Niniejszy poradnik przygotowaliśmy z myślą o Państwu, jako materiał edukacyjny, który omawia wybrane i ważniejsze aspekty Rozporządzenia.

Mamy nadzieję, że przystępny język poradnika pozwoli Państwu w łatwy sposób zapoznać się z poniższymi informacjami. Poradnik ma również na celu wskazanie, w jaki sposób zarządzać zgodami na przetwarzanie danych osobowych na prowadzonych przez Państwa stronach internetowych oraz jak spełniać obowiązek informacyjny wynikający z RODO.

Zespół Rzetelna Grupa

Autorzy
Anna Stępniewska, Katarzyna Sawczuk

Projekt i skład
Manowce Zuzanna Mann

Redakcja i korekta
Dorota Kraskowska, Małgorzata Jodłowska

Spis treści

*Dodatek specjalny

1.
Kto podlega RODO? Kto powinien wdrożyć RODO?

Każdy kto prowadzi działalność w Unii Europejskiej, czy jest to jednoosobowa działalność gospodarcza czy spółka prawa handlowego, czy nawet oddział w Unii Europejskiej przedsiębiorcy mającego siedzibę poza Unią, podlega pod regulację RODO, niezależenie od tego czy samo przetwarzanie danych odbywa się w Unii, czyli gdzie np. znajdują się serwery.

Przykład:

W praktyce oznacza to, że oddział w Polsce przedsiębiorcy z USA podlega pod przepisy RODO, tak samo gdy polski podmiot oferuje usługi obywatelom Ukrainy.

RODO znajduje również zastosowanie do przetwarzania danych osobowych osób, których dane dotyczą, przebywających w Unii, przez administratora lub podmiot przetwarzający niemających siedziby czy też oddziałów w Unii, jeżeli czynności przetwarzania wiążą się z:

a) oferowaniem towarów lub usług takim osobom, których dane dotyczą, w Unii, niezależnie od tego czy wymaga się od tych osób zapłaty; lub

b) monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii.

Podstawa prawna art. 3 RODO.

RODO nie ma natomiast zastosowania do przetwarzania danych osobowych:

a) w ramach działalności nieobjętej zakresem prawa Unii;

b) przez państwa członkowskie w ramach wykonywania działań wchodzących w zakres tytułu V rozdział 2 TUE;

c) przez osobę fizyczną w ramach czynności o czysto osobistym lub domowym charakterze;

d) przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych lub wykonywania kar, w tym ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Podstawa prawna art. 2 RODO.

2.
Co to są dane osobowe?

Dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą").

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.

Natomiast osoba zidentyfikowana to taka, której tożsamość już znamy, którą możemy wskazać.

Przykład:

W przypadku sklepu czy serwisu internetowego będzie to klient sklepu/serwisu, który podał swoje dane osobowe w celu przeprocesowania zamówienia osoba, która podała swoje dane osobowe za pośrednictwem formularza kontaktowego na stronie www, jak również osoba, która podała swoje dane do subskrypcji newslettera.

Natomiast osoba możliwa do zidentyfikowania, to np. potencjalny klient, w przypadku którego posiadamy np. jedynie numer rejestrowy, czy też adres prowadzenia działalności.

Dane osobowe dzielimy na:

a) dane osobowe zwykłe, do których należą również dane osobowe dotyczące wyroków skazujących,

b) szczególne kategorie danych osobowych (potocznie zwane dane wrażliwe).

Do szczególnej kategorii danych osobowych należą: dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby.

Podstawa prawna art. 4 ust. 1 art. 9, 10 RODO.

2.1. Imię i nazwisko oraz adres

Samo imię i nazwisko nie stanowi danych osobowych. Na przykład wskazanie Jan Kowalski daje nam informację o jakiejś bliżej nieokreślonej osobie, ale nie jesteśmy w stanie na tej podstawie wskazać konkretnie która to osoba. Imię i nazwisko stanie się daną osobową w momencie powiazania go z informacją dodatkową, pozwalającą na identyfikację danej osoby.

Przykład:

Adam Mickiewicz – pisarz, poeta

Karolina Dobrowolska – Słodków

Adam Maciejewski – lekarz, chirurg onkologiczny

Analogicznie będzie w przypadku adresu. Sam adres nie identyfikuje konkretnej osoby ponieważ pod danym adresem może zamieszkiwać kilka osób, adres określa nam jedynie miejsce przebywania osoby. Po połączeniu adresu, najczęściej z imieniem i nazwiskiem możemy już zidentyfikować konkretną osobę.

Przy takim połączeniu możemy mówić, że dane będą stanowiły daną osobową.

2.2. Wizerunek osoby fizycznej

W przypadku sklepów/serwisów internetowych dobrze jest wiedzieć na jakich zasadach możemy wykorzystywać wizerunek osoby fizycznej. Bardzo często zdarza się, że w ramach prowadzonej działalności Administrator strony www (sprzedawca, usługodawca) chciałby zorganizować np. konkurs dla swoich klientów/użytkowników. Zdarza się, że w ramach zadania konkursowego nadsyłane jest zdjęcie. W niektórych przypadkach sam charakter działalności gospodarczej, szczególnie w branży usługowej związany jest z wykorzystywaniem czyjegoś wizerunku, np. biura podróży, ośrodki aktywnego wypoczynku, które prezentują wizerunki osób korzystających z oferowanych przez nie usług.

W motywie 51 RODO określa, że przetwarzanie fotografii nie powinno zawsze stanowić przetwarzania szczególnych kategorii danych osobowych, gdyż fotografie są objęte definicją „danych biometrycznych" tylko w takich przypadkach, w których są przetwarzane specjalnymi metodami technicznymi, umożliwiającymi jednoznaczną identyfikację osoby fizycznej lub potwierdzenie jej tożsamości.

Zatem zezwolenie na rozpowszechnienie wizerunku możemy mieć w dowolnej formie jednakże ze względów dowodowych, rekomendujemy aby posiadać je w formie pisemnej, czy też mailowej informacji, że dana osoba zgadza się na wykorzystanie wizerunku, w jakim zakresie, i na jakich serwisach czy też w jakich publikacjach.

Jedynie w dwóch przypadkach nie ma konieczności pozyskiwania zgody na rozpowszechnienie wizerunku:

a) Jeżeli wizerunek wykonano w związku z pełnieniem przez nią funkcji publicznych, w szczególności politycznych, społecznych, zawodowych. Będzie to miało zastosowanie do polityków, sportowców, aktorów, dziennikarzy lub osoby powszechnie nieznanej, która urządza happening.

b) Jeżeli osoba stanowi jedynie szczegół większej całości, czyli np. zgromadzenia publicznego, krajobrazu, imprezy masowej itd. Osoba decydująca się na udział w zgromadzeniu publicznym wyraża w sposób dorozumiany zgodę na upublicznienie jej wizerunku.

2.3. Numer IP

Adres IP może być w pewnych przypadkach uznany za dane osobowe.

Opinia Grupy Roboczej ds. Ochrony Danych, powołanej przez Parlament Europejski i Radę Europejską uznała literalnie adres IP za dane dotyczące osoby możliwej do zidentyfikowania, stwierdzając, że: *„dostawcy usług internetowych oraz menedżerowie lokalnych sieci mogą, stosując rozsądne środki, zidentyfikować użytkowników internetu, którym przypisali adresy IP ponieważ systematycznie zapisują w plikach daty, czas trwania oraz dynamiczny adres IP (czyli ulegający zmianie po każdym zalogowaniu) przypisany danej osobie. To samo odnosi się do dostawców usług internetowych, którzy prowadzą rejestr (logbook) na serwerze HTTP. Nie ma wątpliwości, że w takich przypadkach można mówić o danych osobowych, w rozumieniu art. 2 Dyrektywy".*

W związku z powyższym należy uznać, że w przypadkach, gdy adres IP jest na stałe lub na dłuższy okres czasu przypisany do konkretnego urządzenia, które przypisane jest z kolei konkretnemu użytkownikowi, należy uznać, że stanowi on daną

osobową. W praktyce możemy się spotkać jednak z sytuacjami, gdy jednoznaczne przypisanie adresu IP do konkretnej, zidentyfikowanej osoby nie jest praktycznie możliwe. Sytuacja taka może wystąpić np. w kawiarenkach internetowych, gdzie komputery udostępniane są klientom bez odnotowywania ich danych identyfikacyjnych. Są to jednak sytuacje wyjątkowe. W wielu przypadkach, nawet przy korzystaniu z komputera w kawiarence internetowej, wykorzystując dane zarejestrowane przez system nadzoru wizyjnego w zestawieniu z innymi danymi (np. dotyczących płatności przy użyciu karty kredytowej), możliwe jest zidentyfikowanie osoby korzystającej w danym czasie z danego komputera. Ponieważ definicja danych osobowych sformułowana w art. 2 Dyrektywy 2002/58/WE pokrywa się z definicją podaną w ustawie o ochronie danych osobowych (art. 6 ustawy), adresy IP można uznać za dane osobowe. Podstawa prawna Art. 6 ust. 1 ustawy z 29 sierpnia o ochronie danych osobowych Dyrektywa 94/46/WE Parlamentu Europejskiego.

2.4. Numer PESEL

Numer PESEL (Powszechnego Elektronicznego Systemu Ewidencji Ludności) w naszym prawodawstwie, jest przyznawany każdej osobie fizycznej, ponieważ nie ma dwóch takich samych numerów PESEL, jest to niewątpliwie identyfikator osoby fizycznej. Jest to 11-cyfrowy, stały, symbol numeryczny, jednoznacznie identyfikujący osobę fizyczną, gdzie sześć pierwszych cyfr oznacza datę urodzenia, kolejne cztery liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do komputerowej kontroli poprawności nadanego numeru ewidencyjnego.

O tym, że PESEL jest daną osobową mówi wprost GIODO w informatorze publikowanym na stronie internetowej poświęconej tematyce ochrony danych osobowych, cytuję: *„Przykładem pojedynczej informacji stanowiącej daną osobową jest natomiast numer PESEL, który zgodnie z art. 15 ust. 2 ustawy z dnia 24 września 2010 r. o ewidencji ludności (Dz.U. z 2015 r. poz. 388) jest 11-cyfrowym symbolem numerycznym, jednoznacznie identyfikującym osobę fizyczną, w którym sześć pierwszych cyfr oznacza datę urodzenia (rok, miesiąc, dzień), kolejne cztery - liczbę porządkową i płeć osoby, a ostatnia jest cyfrą kontrolną służącą do elektronicznej kontroli poprawności nadanego numeru ewidencyjnego. Można więc stwierdzić, że numer PESEL ex definitione stanowi daną osobową, a jej przetwarzanie podlega wszelkim rygorom przewidzianym w ustawie o ochronie danych osobowych”.* https://giodo.gov.pl/317/id_art/973/j/pl

2.5. Adres e-mail

Adres poczty elektronicznej (e-mail) w niektórych przypadkach będzie daną osobową. Co do zasady w adresie poczty mamy podane imię, nazwisko osoby oraz informacje, które w połączeniu pozwalają na identyfikację właściciela adresu poczty elektronicznej w sposób pośredni lub bezpośredni. Oczywiście nie każdorazowo, będą również wyjątki w tym zakresie. Jeśli będzie to np. adres skierowany na biuro, czy ogólnie sklep nie będzie to dana osobowa.

Przykład:

Gdy jest to dana osobowa: maria.kozlowska@nazwaprzedsiębiorstwa.pl, m.kowalski@nazwaprzedsiębiorstwa.pl

Gdy nie jest to dana osobowa: biuro@nazwaprzedsiębiorstwa.pl, sklep@nazwaprzedsiębiorstwa.pl

2.6. Numer rachunku bankowego

Numer rachunku bankowego sam w sobie nie będzie stanowił danej osobowej. Posiadając sam numer nie jesteśmy w stanie sprecyzować, kto jest jego właścicielem, do kogo należy. Jest to tylko ciąg cyfr i dla przeciętnej osoby nie będzie stanowił danej osobowej. Sytuacja ta ulegnie zmianie w powiązaniu jednak z innymi informacjami identyfikującymi osobę. Analogicznie należy traktować również numer legitymacji, indeksu studenckiego, dowodu osobistego czy nawet dowodu rejestracyjnego.

3.
Przetwarzanie danych osobowych – obowiązki Administratora Danych

3.1. Ogólne zasady przetwarzania danych osobowych

RODO w art. 5 mocno akcentuje zasady dotyczące przetwarzania danych osobowych.

Dane osobowe muszą być:

a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą **(„zgodność z prawem, rzetelność i przejrzystość”)**;

b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 RODO za niezgodne z pierwotnymi celami (**„ograniczenie celu”);**

c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane **(„minimalizacja danych”);**

d) 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 **(„prawidłowość”);**

e) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą **(„ograniczenie przechowywania”);**

f) 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 **(„integralność i poufność”).**

Dodatkowo Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 powyżej i musi być w stanie wykazać ich przestrzeganie **(„rozliczalność”).**

Podstawa prawna art. 5 RODO.

3.2. Kiedy i jak długo można przetwarzać dane osobowe?

Dane osobowe można przetwarzać wyłącznie wtedy gdy istnieje podstawa prawna przetwarzania danych. Co do zasady w przypadku danych zwykłych jest to 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.

Natomiast w przypadku szczególnej kategorii danych:

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 art. 9 ust. 1 RODO;

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, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;

c) 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;

d) przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;

e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;

f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;

g) 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;

h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 9 ust. 3 RODO;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

Jak wspomniano powyżej w art. 5 RODO wprowadza tzw. zasadę minimalizacji przetwarzania danych osobowych. Zgodnie z tą zasadą Administrator może przetwarzać tylko takie dane osobowe, które są niezbędne do osiągnięcia celu przetwarzania danych.

Przykład

Jeśli prowadzimy sklep/serwis internetowy i na stronie www zmieszczony jest formularz kontaktowy, to wystarczy że klient będzie mógł podać imię i nazwisko, adres e-mail lub numer telefonu, z czego adres e-mail oraz numer telefonu nie powinny być wymagane łącznie, czyli klient powinien mieć wybór jaką drogą Administrator powinien się z nim skontaktować.

Bardzo często zdarza się, że formularze rejestracyjne w sklepach, serwisach internetowych posiadają pole o nazwie data urodzenia/płeć. Natomiast w praktyce Administrator nie wykorzystuje tych danych, w takim przypadku, zasadnym jest usunięcie tych punktów z formularzy. Jeśli natomiast dana taka jak data urodzenia, potrzebna jest Administratorowi w celu wysyłania np. elektronicznej kartki urodzinowej, lub przydzielenia w ten dzień solenizantowi stosownego rabatu na dokonanie zakupów, jest to jak najbardziej uzasadniony cel dla jakiego zbierana jest wskazana dana. Dodatkowo oczywiście potrzebna jest zgoda na wysyłanie informacji handlowych drogą elektroniczną.

Jeśli celem przetwarzania danych osobowych w sklepie/serwisie internetowym jest realizacja zamówienia, to zbieranie przy tej okazji danych np. o stanie rodzinnym klienta nie jest dopuszczalne.

Dane, które zbiera Administrator nie mogą być również zbierane w nieskończoność o czym mówi zasada ograniczenia przechowywania danych wyrażona w art. 5 ust. 1 lit. e) RODO.

Jeśli podstawą przetwarzania danych osobowych jest zgoda, wówczas dane osobowe mogą być przetwarzane tak długo aż zgoda nie zostanie odwołana. Po odwołaniu zgody - przez czas odpowiadający okresowi przedawnienia roszczeń, jakie mogą być podnoszone wobec niego. Obecnie okres ten wynosi 10 lat. Jeśli podstawą przetwarzania danych jest wykonanie umowy, dane mogą być przetwarzane tak długo jak jest to niezbędne do wykonania umowy, a po tym czasie przez okres odpowiadający okresowi przedawnienia roszczeń. W przypadku relacji między przedsiębiorcami wynosi on 3 lata i jest dodatkowo uzależniony od rodzaju umowy.

Czas przetwarzania może zależeć od przepisów szczególnych, np. przepisów o rachunkowości, które nakazują przechowywać dowody księgowe umów handlowych, czy też roszczeń dochodzonych w postępowaniach podatkowych przez okres 5 lat.

Uwaga! Zmiana w prawie 1.01.2019 r., dokumentację w sprawach związanych ze stosunkiem pracy i akt osobowych pracownika można przechowywać w formie elektronicznej oraz należy ją przechowywać przez okres 10 lat.

Podstawa prawna art. 5, 6, 9 RODO.

3.3. Zgoda na przetwarzanie danych – przykładowe klauzule zgód

Ogólne rozporządzenie o ochronie danych osobowych (RODO) nie zmieniło w znacznym stopniu aktualnie obowiązującej definicji zgody na przetwarzanie danych osobowych. Wprowadziło natomiast obok dotychczas funkcjonującej zgody w formie oświadczenia woli – możliwość uznania za ważną zgody wyrażonej w sposób dorozumiany poprzez wyraźne działanie potwierdzające. Wypracowane zostały także niezbędne elementy okazania zgody, a są nimi: dobrowolność, konkretność, świadomość i jednoznaczność.

Zgoda dobrowolna

Wymóg dobrowolności zgody oznacza, że osoba, której dane dotyczą ma faktycznie wolny wybór co do udzielenia zgody oraz może jej odmówić lub ją wycofać w dowolnym czasie. RODO odmawia miana dobrowolności zgodzie, od której złożenia zostało uzależnione wykonanie umowy.

Dopuszczalne jest – z uwzględnieniem innych przepisów prawa – zachęcanie do wyrażenia zgody na przetwarzanie danych osobowych, np. w celu uczestnictwa w programie lojalnościowym. Możliwe jest także zastosowanie umowy o świadczenie usług wzajemnych o charakterze niepieniężnym, mianowicie – zaoferowanie osobie np. darmowego e-booka lub dostępu do płatnej platformy w zamian za wyrażenie zgody na przetwarzanie jej danych w celach marketingowych.

Zgoda konkretna i odrębna

Administrator nie może odebrać ogólnej zgody na przetwarzanie danych osobowych bez określenia konkretnego celu (zgoda blankietowa). W klauzuli zgody powinien być określony cel przetwarzania danych osobowych oraz zakres tych danych.

Jeśli Administrator chciałaby zapytać o zgodę na przetwarzanie danych osobowych w formie elektronicznej, wysłane do osoby pytanie powinno być wyraźne, zwięzłe i niezakłócające niepotrzebnie korzystania z usługi. Powinno też mieć charakter odrębny, np. od pozostałej korespondencji e-mailowej.

Zgoda świadoma

Z wymogiem świadomości zgody na przetwarzanie danych osobowych związany jest obowiązek informacyjny, jaki nakłada na Administratora Danych RODO. Osoba wyrażająca zgodę powinna co najmniej znać tożsamość Administratora oraz zamierzone przez niego cele przetwarzania danych osobowych. Zgodnie z zasadą przejrzystości informacje przekazywane osobie, której dane dotyczą powinny być sformułowane w sposób zrozumiały, jasnym i prostym językiem. Istotna jest także dostępność tych treści – klauzule powinny być widoczne i wyczerpujące.

Zgoda jednoznaczna

Wymóg jednoznaczności oznacza, że nie mogą istnieć wątpliwości co do intencji osoby wyrażającej zgodę. Wyrażenie zgody może mieć formę oświadczenia woli lub wyraźnego działania potwierdzającego. Dopuszczalne jest zaznaczenie okna wyboru (checkboxa) podczas przeglądania strony internetowej, czy wybranie odpowiednich ustawień technicznych lub inna czynność – wskazująca akceptację osoby i możliwa do wykazania przez Administratora.

Zakazaną praktyką pozostanie sformułowanie klauzul zgód w regulaminie i odebranie ich poprzez oświadczenie o akceptacji tego regulaminu. Wykluczone jest także odebranie zgody poprzez milczenie, dlatego rekomendowanym jest wyrażenie zgody w systemie *double-opt-in*, wymagającym określonej czynności od osoby, której dane dotyczą. Przykładowo, aby zapisać się do newslettera osoba musi otworzyć link, przesłany na adres e-mail, który podała przy rejestracji.

Zgoda powinna mieć charakter uprzedni do rozpoczęcia przetwarzania danych, a więc ma zostać odebrana w momencie zbierania danych.

Obowiązek wykazania odebrania zgody

Fakt uzyskania zgody powinien być możliwy do udowodnienia. Obowiązek ten wpisuje się w zasadę rozliczalności, na której oparte są nowe przepisy unijne dotyczące ochrony danych osobowych. Administratorzy Danych otrzymali dużą dowolność w zakresie ochrony procesów przetwarzania danych osobowych, z tym, że powinni być w stanie wykazać, że faktycznie realizują nałożone przez rozporządzenie wymogi. Dlatego w przypadku zbierania zgód w formie pisemnej należy archiwizować podpisane formularze. W przypadku odbierania zgód w formie elektronicznej, np. za pomocą checkboxa, system informatyczny powinien zapisywać adres IP oraz datę zaznaczenia checkboxa. Dopuszczalne jest również zbieranie zgody na przetwarzanie danych osobowych w rozmowie telefonicznej. Rozmowa taka powinna być jednak nagrywana, o czym uprzednio należy poinformować osobę, której dane dotyczą.

Zgody, z jakimi najczęściej Administratorzy sklepów/serwisów internetowych będą mieli do czynienia to:

1) akceptacja regulaminu, (w tym również regulaminu konkursu);
2) zapis na newsletter;
3) formularz kontaktowy;
4) zapis na szkolenie on-line/webinar.

Formularz rejestracji konta i jednorazowego zamówienia

Poprawna treść zgody pod formularzem:

„Oświadczam, iż zapoznałem się z treścią Regulaminu <tu link>."

RODO nakłada na Administratora obowiązek, aby podczas zbierania danych osobowych Administrator spełniał obowiązek informacyjny (art. 13 RODO). Zalecamy, aby obowiązek informacyjny zrealizować umieszczając stosowne klauzule (patrz poniżej poradnika) w treści Polityki Prywatności.

Rekomendujemy zamieszczenie pod checkboxem o akceptacji regulaminu linku do Polityki Prywatności zatytułowanego:

„Zasady ochrony danych osobowych <tu link>."

https://www.politykabezpieczenstwa.pl/pl/a/nowe-obowiazki-informacyjne-Administratora-danych

Subskrypcja Newslettera

Obowiązujące ustawy w zakresie świadczenia usług drogą elektroniczną oraz RODO, zobowiązują aby przy subskrypcji na newsletter zadbać o (w zależności od różnych wariantów):

1) i. klauzulę zgody na przesyłanie informacji handlowych drogą elektroniczną zgodnie z art. 10 ust. 1 i 2 ustawy o świadczeniu usług drogą elektroniczną;

   ii. klauzulę zgody na przetwarzanie danych osobowych na podstawie (art. 172 Prawa telekomunikacyjnego);

   iii. podanie informacji, że cofnięcie zgody jest tak łatwe jak jej wyrażenie (art. 7 ust. 3 RODO)

2) spełnienie obowiązku informacyjnego. Podczas zbierania danych osobowych Administrator spełnia obowiązek informacyjny (art. 13 RODO). Obowiązek można zrealizować umieszczając stosowne klauzule w treści Polityki Prywatności;

Rekomendujemy pozostawienie na stronie głównej wyłącznie okna: *„Zapisz się na Newsletter”* bez pola na wpisanie adresu e-mail. Kliknięcie tego okna przenosi do formularza rejestracyjnego na Newsletter, w którym znajduje się pole do wypełnienia adresu e-mail oraz następujące elementy, w zależności od kanału komunikacji z Klientem:

1) Klauzula zgody z checkboxem o treści:

   Wyrażam zgodę na przesyłanie informacji handlowych za pomocą środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 roku o świadczenie usług drogą elektroniczną (Dz.U.2017.1219 tj..) na podany adres e-mail na temat usług oferowanych przez ABC Sp. z o.o. przy ul. [x] z siedzibą w [x].

   Zgoda jest dobrowolna i może być w każdej chwili wycofana, klikając w odpowiedni link na końcu wiadomości e-mail. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

   Wyrażam zgodę na przesyłanie informacji handlowych za pomocą środków komunikacji elektronicznej w rozumieniu ustawy z dnia 18 lipca 2002 roku o świadczenie usług drogą elektroniczną (Dz.U.2017.1219 tj..) w formie wiadomości tekstowej sms na podany numer telefonu na temat usług oferowanych przez ABC Sp. z o.o. przy ul. [x] z siedzibą w [x].

   Zgoda jest dobrowolna i może być w każdej chwili wycofana, klikając w odpowiedni link na końcu wiadomości e-mail. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

   Komentarz: Gdyby Administrator chciał pozyskiwać dane klientów (w tym numery ich telefonów) do wysyłania wyłącznie informacji handlowych drogą elektroniczną (wiadomości e-mail i sms) – patrz powyższe dwie zgody, zbędnym będzie zbieranie zgody określonej w art. 172 Prawa Telekomunikacyjnego. Jeśli jednak ten sam Administrator chciałby poza wysyłaniem informacji handlowych, kontaktować się z klientem poprzez wykonywanie połączeń głosowych, podczas których przedstawiałby treści marketingowe, ww. odrębna zgoda będzie wymagana o treści:

   Wyrażam zgodę na przetwarzanie moich danych osobowych przez ABC Sp. z o.o. przy ul. [x] z siedzibą w [x], dla celów marketingu bezpośredniego, wykonywanego przy użyciu telekomunikacyjnych urządzeń końcowych oraz automatycznych systemów wywołujących, tj. numer telefonu, zgodnie z art. 172 ustawy z dnia 16 lipca 2004r. Prawo telekomunikacyjne (Dz.U. z 2017 r., poz. 1907 ze zm.).” Zgoda jest dobrowolna i może być w każdej chwili wycofana, kierując wiadomość na adres e-mail Administratora. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

2) Link do Polityki Prywatności zatytułowany:

   „Zasady ochrony danych osobowych<tu link>.”

https://www.politykabezpieczenstwa.pl/pl/a/jak-powinna-wygladac-zgoda-na-przetwarzanie-danych-osobowych

Formularz kontaktowy

Podczas zbierania danych osobowych Administrator zgodnie z RODO spełnia obowiązek informacyjny (art. 13 RODO). Obowiązek można zrealizować umieszczając stosowne klauzule w treści Polityki Prywatności (patrz poniżej).

Administrator tak jak w powyższych przypadkach i w tym również powinien stosować zasadę minimalizacji danych (art. 5 ust. 1 lit. c), co oznacza zbieranie danych adekwatnie, stosownych danych, oraz ograniczonych danych do niezbędnego celu, w którym są przetwarzane. Administrator w praktyce musi rozważyć aby zbierać odpowiednią ilość danych.

Dla przykładu zastosowanie obowiązkowych pól w formularzu kontaktowym zarówno dla adresu e-mail i numeru telefonu jest nieadekwatne w stosunku do celu jednorazowego kontaktu z klientem (art. 26 ust. 1 pkt. 3 ustawy o ochronie danych osobowych/art. 5 ust. 1 lit. c RODO). Jeżeli Administrator w formularzu kontaktowym przewiduje możliwość kontaktu z klientem zarówno drogą elektroniczną, jak i telefoniczną, to klient powinien mieć możliwość wyboru jednej opcji. Jak na przykładzie poniższym, żadne z pól nie jest obligatoryjne.

Imię i nazwisko:

Adres e-mail:

Numer telefonu:

Treść wiadomości:

Rekomendujemy zamieszczenie pod formularzem linku do Polityki Prywatności zatytułowanego:

„Zasady ochrony danych osobowych <tu link>."

Zapis na szkolenie on-line webinar

Poprawna treść zgody pod formularzem:

„Oświadczam, iż zapoznałem się z treścią Regulaminu szkolenia on-line <tu link>."

RODO nakłada na Administratora obowiązek aby podczas zbierania danych osobowych Administrator spełniał obowiązek informacyjny (art. 13 RODO). Zalecamy aby obowiązek informacyjny zrealizować umieszczając stosowne klauzule (patrz. poniżej artykułu) w treści Polityki Prywatności.

Rekomendujemy zamieszczenie pod checkboxem o akceptacji regulaminu linku do Polityki Prywatności zatytułowanego:

„Zasady ochrony danych osobowych<tu link>."

https://www.politykabezpieczenstwa.pl/pl/a/nowe-obowiazki-informacyjne-Administratora-danych

Ważne: jeżeli klient skorzysta z formularza kontaktowego, wówczas firma ma podstawę prawną do korespondowania/ kontaktowania się z klientem w sprawie, w której się zwraca. Jeżeli w przyszłości pozyskane dane osobowe miałyby być wykorzystane do celów marketingowych, a w szczególności promowania innych produktów/usług wówczas w formularzu kontaktowym powinna znaleźć się zgoda na wiadomości handlowe – zgodnie z podanym wyżej przykładem.

Jak wskazano powyżej dobrym miejscem na spełnienie obowiązku informacyjnego zgodnie z RODO jest Polityka Prywatności.

RODO nakłada na Administratora konieczność działania w zakresie realizacji obowiązku informacyjnego. Po stronie Administratora powinna leżeć wymagana aktywność związana z podaniem wymaganych przepisami prawa informacji – niezależnie od tego czy osoba podaje dane z własnej inicjatywy czy na skutek działań Administratora. Niedopuszczalne jest wymuszenie na osobie, od której dane są zbierane, aby ta poszukiwała klauzuli informacyjnej, np. na stronie internetowej, podczas gdy dane są zbierane od niej w formie papierowej. Administrator powinien również zadbać o to, aby osoba miała możliwość zapoznania się ze skierowanymi do niej informacjami zanim poda swoje dane.

3.4. Obowiązek informacyjny przy zbieraniu zgody na przetwarzanie danych osobowych

Wyrażona w RODO zasada transparentności przetwarzania danych osobowych wymaga, aby przede wszystkim powiadomić podmiot danych o **tożsamości Administratora Danych** oraz podać do niego dane kontaktowe. Ma to umożliwić osobie faktyczną realizację jej uprawnień. Jeżeli jest to zasadne, należy podać tożsamość i dane kontaktowe przedstawiciela, np. gdy Administratorem jest spółka prawa handlowego.

Nowością na gruncie RODO jest obowiązek podania **danych kontaktowych Inspektora Ochrony Danych**. Powołanie osoby na tę funkcję przez Administratora Danych jest obligatoryjne tylko w przypadkach określonych w art. 37 ust. 1 lit. a-c RODO, w pozostałych przypadkach jest fakultatywne.

Kolejnym wymogiem jest **podanie celów przetwarzania danych**. Należy mieć na uwadze, że cele powinny zostać wskazane wyraźnie w momencie zbierania danych oraz mieć swoje uzasadnienie. Zakazane jest przetwarzanie danych osobowych, jeżeli cel przetwarzania można osiągnąć innymi sposobami. Dane osobowe powinny zaś być zbierane w ograniczonym, stosownym zakresie, adekwatnym do celu przetwarzania. Przykładowo nie ma konieczności zbierania daty urodzenia w celu przygotowania dla klienta diety i planu treningowego, jeśli firma (Administrator Danych) potrzebuje tej informacji wyłącznie w celu dopasowania swojej usługi do wieku osoby. Wystarczającym będzie w takim przypadku podanie roku życia, tzn. zapytanie ile osoba ma lat, bez wymagania podania przez nią pełnej daty urodzenia. Informacji o celu nie może zastępować stwierdzenie, że dane będą przetwarzane zgodnie z ogólnym rozporządzeniem o ochronie danych osobowych. Warto o tym wspomnieć, ponieważ często na gruncie aktualnie obowiązujących przepisów w treściach klauzul informuje się, że podanie danych osobowych jest dobrowolne i będzie przetwarzane zgodnie z ustawą o ochronie danych osobowych. W jakim jednak celu – to z klauzuli już nie wynika.

Jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu realizowanego przez Administratora lub stronę trzecią, Administrator podaje ten interes.

Jeżeli istnieją odbiorcy danych (podmioty, którym dane są udostępnione), podaje się ich tożsamość lub jeśli nie jest ona znana w momencie zbierania danych – kategorie tych odbiorców.

Gdy ma to zastosowanie, Administrator informuje o przekazywaniu danych do państwa trzeciego, tj. państwa spoza Europejskiego Obszaru Gospodarczego lub do organizacji międzynarodowej wraz ze wzmianką, czy Komisja uznała dla ww. odpowiedni stopień ochrony danych.

Informowanie o prawach osoby, okresie retencji i zautomatyzowanym przetwarzaniu (art. 13 ust. 2 RODO)

Wynikający z RODO obowiązek informowania osoby o wszelkich aspektach związanych z przetwarzaniem danych osobowych ma w zamyśle prawodawcy unijnego podnieść jej świadomość. Prawodawca zakłada, że podmiot danych dowie się od Administratora o ryzykach przetwarzania danych, zabezpieczeniach danych, a nade wszystko zyska wiedzę o swoich prawach w zakresie przetwarzania oraz sposobach wykonywania tych praw.

Między innymi dlatego Administrator powinien ustalić **okres retencji (czyli przechowywania) danych osobowych** oraz podać go już w momencie zbierania danych. Jeżeli nie jest w stanie określić terminu usunięcia danych, podaje przynajmniej termin okresowego przeglądu.

W obowiązku Administratora leży również poinformowanie osoby o prawie żądania dostępu do jej danych, do sprostowania, usunięcia, przeniesienia lub ograniczenia przetwarzania danych oraz prawie wniesienia sprzeciwu wobec przetwarzania

danych, a w przypadku gdy przetwarzanie odbywa się na podstawie zgody – o prawie jej cofnięcia w dowolnym momencie. Cofnięcie zgody nie będzie miało jednak wpływu na zgodność z prawem przetwarzania danych przed jej cofnięciem. Administrator powinien ustalić procedury w zakresie realizacji tych praw przez podmioty danych.

W ramach szeroko rozumianego obowiązku informacyjnego, Administrator informuje osobę również o tym, iż ma ona prawa wniesienia skargi do organu nadzorczego.

W zakresie dobrowolności lub obowiązku podania danych, Administrator powiadamia, czy podanie danych jest obowiązkiem ustawowym, umownym, czy warunkiem zawarcia umowy. Osoba powinna również zostać poinformowana, czy ma obowiązek podania danych i jakie ewentualnie poniesie konsekwencje, jeżeli tego nie zrobi.

Nowością na gruncie RODO jest informowanie o zautomatyzowanym podejmowaniu decyzji – w tym profilowaniu. Treść informacji powinna obejmować istotne zasady podejmowania takich decyzji oraz konsekwencjach, jakie mogą one nieść dla osoby, której dane dotyczą.

Rekomendujemy, aby pod klauzulami zgód zamieścić link o nazwie **Zasady Ochrony Danych Osobowych**, który będzie linkował do Polityki Prywatności.

3.5. Przykładowe klauzule spełnienia obowiązku informacyjnego

1) Administratorem Danych Osobowych jest *[należy podać nazwę oraz siedzibę];*

2) Inspektorem Ochrony Danych jest *[podać imię i nazwisko oraz kontakt np. e-mail], (ten obowiązek spełniamy jeśli ma zastosowanie);*

3) dane osobowe przetwarzane będą w celu *[należy podać cel przetwarzania zgodnie z art. 6 RODO];*

4) odbiorcą danych osobowych będą *[można wymienić kategorię odbiorców o ile istnieją np. kurierom, bankom, ubezpieczycielom, kancelariom prawnym, spółkom z naszej grupy kapitałowej];*

5) dane osobowe będą przekazywane do państwa trzeciego/organizacji międzynarodowej *[jeśli ma zastosowanie].* Mogą Państwo uzyskać kopię danych osobowych przekazywanych do państwa trzeciego [*wskazać sposób uzyskania kopii danych lub miejsce udostępnienia danych];*

6) dane osobowe będą przechowywane przez okres [*np. do czasu odwołania zgody, jeżeli nie ma możliwości wskazania okresu przechowywania należy podać kryterium ustalania tego okresu np. do czasu zakończenia rekrutacji itp.)*;

7) posiadają Państwo prawo dostępu do treści swoich danych oraz prawo ich sprostowania, usunięcia, ograniczenia przetwarzania, prawo do przenoszenia danych, prawo wniesienia sprzeciwu, prawo do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

8) mają Państwo prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych w zakresie naruszenia prawa do ochrony danych osobowych lub innych praw przyznanych na mocy RODO.

9) podanie danych osobowych jest [*należy wskazać czy podanie danych jest wymogiem ustawowym/warunkiem umownym/ warunkiem zawarcia umowy].* Są Państwo zobowiązani do ich podania a konsekwencją niepodania danych osobowych będzie *[jeżeli osoba, której dane dotyczą, jest zobowiązana do ich podania należy wskazać ewentualne konsekwencje niepodania danych];*

10) Państwa dane będą przetwarzane w sposób zautomatyzowany w tym również w formie profilowania. Zautomatyzowane podejmowanie decyzji będzie odbywało się na zasadach *[należy podać zasady profilowania jakie Państwo wprowadzili w organizacji],* konsekwencją takiego przetwarzania będzie [*należy wskazać istotne informacje o zasadach zautomatyzowanego podejmowania decyzji oraz informacje o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą].*

3.6. Odwołanie zgody na przetwarzanie danych osobowych

Zgodnie z art. 7 ust. 3 RODO, 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, musi być o tym poinformowana, zanim wyrazi zgodę, (patrz przykładowe treści zgód in fine). Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Odnosząc powyższe do konkretnego przykładu. Jeżeli osoba, której dane dotyczą zapisuje się na subskrypcję newslettera, zwrotnie na jej adres e-mail powinien zostać wysłany link do potwierdzenia zapisania się na newsletter oraz wypisania się z subskrypcji.

3.7. Ocena skutków dla ochrony danych

Z dniem 25 maja 2018 r., zostaje zniesiony obowiązek rejestrowania przez Administratora zbiorów danych osobowych. W zamian w RODO pojawił się nowy instrument – ocena skutków dla ochrony danych (ang. Data Protection Impact Assessment – DPIA). Ocena skutków przetwarzania jest oszacowaniem prawdopodobieństwa i powagi naruszenia bezpieczeństwa danych osobowych, szczególnie w sytuacji, gdy są zbierane dane osobowe na dużą skalę oraz gdy są wprowadzane nowatorskie technologie, zwłaszcza te, które wykorzystują dane genetyczne bądź biometryczne lub inteligentny monitoring, który automatycznie może rozpoznawać twarze.

Przeprowadzenie oceny skutków dla ochrony danych jest zatem wymagane w szczególności w przypadku:

a) systematycznej, kompleksowej oceny 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 lub w podobny sposób znacząco wpływających na osobę fizyczną;

b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa;

c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.

Prawdopodobieństwo, że trzeba przeprowadzić ocenę, jest większe, im więcej poniższych sytuacji nastąpi równocześnie u danego Administratora, w tym:

a) ocena i scoring, w tym profilowanie i przewidywanie, w szczególności dotyczące takich aspektów podmiotu danych jak świadczenie pracy, sytuacja ekonomiczna, zdrowie, osobiste preferencje, zainteresowania, wiarygodność, zachowanie, lokalizacja czy poruszanie się;

b) zautomatyzowane podejmowanie decyzji, w tym profilowanie, wywołujące skutki prawne lub wpływające na podmiot danych w podobny sposób;

c) systematyczne monitorowanie mające na celu obserwowanie, monitorowanie lub kontrolowanie podmiotu danych, w tym systematyczne monitorowanie miejsc dostępnych publicznie. Chodzi tutaj np. o stosowanie monitoringu w hotelu, restauracji czy na stacji benzynowej w sytuacji, w której klient nie może wejść do obiektu lub skorzystać z usługi bez uprzedniego nagrania go przez monitoring wizyjny;

d) przetwarzanie szczególnych kategorii danych;

e) przetwarzanie danych na dużą skalę;

f) przetwarzanie danych osobowych podlegających łączeniu lub dopasowywaniu;

g) przetwarzanie danych dotyczących wrażliwych podmiotów danych;

h) wykorzystanie do przetwarzania danych innowacyjnych rozwiązań technicznych lub organizacyjnych, zwłaszcza w kontekście nowatorskich technologii wykorzystujących np. biometrię;

i) transfer danych poza granice Unii Europejskiej, a zwłaszcza do USA;

j) przetwarzanie danych samo w sobie utrudniające podmiotom danych wykonywanie przysługujących im praw lub korzystanie z usługi lub z umowy.

Zgodnie z treścią art. 35 ust. 7 RODO ocena powinna zawierać co najmniej:

a) systematyczny opis planowanych operacji przetwarzania danych i celów przetwarzania, czyli w jaki sposób oraz w jakim celu przedsiębiorca przetwarza dane osobowe pomiędzy poszczególnymi zbiorami;

b) ocenę niezbędności i proporcjonalności przetwarzania w stosunku do celów, tj. wskazanie, czy określonego potencjalnie ryzykownego działania można uniknąć lub, jeśli nie ma takiej możliwości, jakie środki zastosowano, aby ryzyko zostało zminimalizowane;

c) ocenę ryzyka naruszenia praw i wolności podmiotów danych, w szczególności, aby przedsiębiorca zdawał sobie sprawę z ryzyka, jakie niesie wykorzystywana technologia;

d) środki planowane w celu zaradzenia ryzyku oraz wykazanie zgodności operacji przetwarzania danych z RODO.

RODO nie nakłada w jakiej konkretnej formie oraz strukturze należy dokonać oceny, pozostawia to do oceny Administratora.

Są również okoliczności w których nie trzeba dokonywać DPIA. RODO wskazuje na:

a) charakter, zakres, kontekst i cele przetwarzania, gdy są bardzo podobne do przetwarzania, dla którego już została dokonana ocena. W takich przypadkach mogą być wykorzystane wyniki DPIA przeprowadzonej dla podobnego przetwarzania (art. 35 ust. 1 RODO);

b) operacja przetwarzania ma podstawę prawną. Oceny skutków dla ochrony danych osobowych nie trzeba przeprowadzać wtedy, kiedy prawo UE lub państwa członkowskiego, któremu podlega Administrator, reguluje już daną operację i jednocześnie oceny skutków dokonano w związku z przyjęciem tej regulacji. Taka redakcja artykułu uprawnia państwa członkowskie do podjęcia decyzji o konieczności dokonania oceny mimo spełnienia powyższych przesłanek (art. 35 ust. 10 RODO);

c) przetwarzanie jest uwzględnione w ustanowionym przez Prezesa Urzędu Danych Osobowych opcjonalnym wykazie operacji przetwarzania niepodlegających wymogowi dokonania DPIA (art. 35 ust. 5 RODO).

Należy pamiętać, że to Administrator samodzielnie podejmuje decyzję o konieczności przeprowadzenia oceny.

3.8. Dokumentacja przetwarzania danych

Zgodnie z art. 30 RODO Administrator prowadzi rejestr czynności przetwarzania danych osobowych.

Powyższe dotyczy przedsiębiorców zatrudniających więcej niż 250 osób. RODO jednakże przewiduje od tego wyjątki. Prowadzenie rejestru czynności będzie obowiązkowe również dla małego i średniego przedsiębiorcy gdy:

- przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą,
- nie ma charakteru sporadycznego,
- obejmuje szczególne kategorie danych osobowych (art. 30 ust. 5).

Sporadyczny charakter przetwarzania danych w tym kontekście oznacza, że przetwarzanie danych nie stanowi nieodłącznego elementu wykonywania przez przedsiębiorcę działalności. W związku z tym prowadzenie akcji marketingowych np. poprzez wysyłkę wiadomości e-mail wyklucza sporadyczność przetwarzania danych. Z kolei sklep stacjonarny sprzedający materiały budowlane, który nie wykorzystuje w swojej działalności platformy elektronicznej, najprawdopodobniej będzie przetwarzał dane osobowe jedynie sporadycznie.

Rejestr czynności przetwarzania jest dokumentem zawierającym wszystkie istotne z punktu widzenia przetwarzania informacje. Sporządza się go w wersji papierowej oraz wersji elektronicznej.

Rejestr czynności powinien zawierać:

a) imię i nazwisko lub nazwę oraz dane kontaktowe Administratora oraz wszelkich współAdministratorów, a także, gdy ma to zastosowanie, przedstawiciela Administratora oraz Inspektora Ochrony Danych;

b) cele przetwarzania danych osobowych, czyli np. marketing produktów i usług własnych, realizacja obowiązków zbierania danych nałożona przez przepisy prawa, np. przez kodeks pracy;

c) opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych. Do kategorii osób będą należeli pracownicy, uczniowie, członkowie, klienci. Możliwe jest przetwarzanie dwóch kategorii danych, tj. danych zwykłych (np. imię, nazwisko, adres zamieszkania, data urodzenia), jak i danych szczególnie chronionych (np. stan zdrowia);

d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych (definicja odbiorcy znajduje się w art. 4 pkt 9 RODO);

e) gdy ma to zastosowanie fakt przekazania danych osobowych do państwa trzeciego, czyli poza Unię Europejską. Komisja Europejska ma tu na myśli przede wszystkim Stany Zjednoczone Ameryki Północnej. Przekazywanie tam danych osobowych jest dozwolone, o ile kontrahenci z USA należą do programu Privacy Shield. Lista podmiotów uczestniczących jest dostępna pod linkiem https://www.privacyshield.gov/list. Za każdym razem, kiedy dane osobowe są przekazywane poza Unię Europejską, trzeba to zaznaczyć w rejestrze czynności przetwarzania;

f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych;

g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których jest mowa w art. 32 ust. 1 RODO.

RODO nie wymienia wymagań minimalnych w zakresie ochrony danych. Przedsiębiorca sam zatem powinien określić

środki bezpieczeństwa. Chodzi tutaj o zabezpieczenie fizyczne, np. poprzez politykę kluczy, zabezpieczenie osobowe, np. poprzez przeszkolenie personelu czy zabezpieczenie informatyczne, np. poprzez posiadanie odpowiedniego oprogramowania antywirusowego.

3.9. Obowiązek zgłoszenia naruszeń danych osobowych

W przypadku naruszenia ochrony danych osobowych, Administrator bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je organowi nadzorczemu, od 25 maja 2018 r. będzie nim Prezes Urzędu Danych Osobowych – chyba, że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. W nielicznych przypadkach organem nie będzie ww. Prezes. Dotyczy to sytuacji gdy przedsiębiorca prowadzi działalność transgraniczną (np. sprowadza sprzęt elektroniczny z Francji do Polski), wtedy będzie podlegał organowi właściwemu terytorialnie, gdzie znajduje się jego główna jednostka organizacyjna, czyli siedziba Administratora.

Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

Zgłoszenie co najmniej musi:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisywać środki zastosowane lub proponowane przez Administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

W art. 4 ust. 12 RODO zdefiniowano naruszenie ochrony danych osobowych jako naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Jak wskazano w Motywie 85 RODO, przy braku odpowiedniej i szybkiej reakcji naruszenie ochrony danych osobowych może skutkować powstaniem uszczerbku fizycznego, szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne. Dlatego natychmiast po stwierdzeniu naruszenia ochrony danych osobowych Administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki, jeżeli to wykonalne, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia, chyba że Administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych. Jeżeli nie można dokonać zgłoszenia w terminie 72 godzin, zgłoszeniu powinno towarzyszyć wyjaśnienie przyczyn opóźnienia, a informacje mogą być przekazywane stopniowo, bez dalszej zbędnej zwłoki.

Na Administratora nałożono obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze.

4.
Uprawnienia osób, których dane dotyczą a obowiązki Administratora

4.1. Prawo do cofnięcia zgody

Osoba, której dane dotyczą i przetwarzane są na podstawie zgody ma prawo do cofnięcia zgody. Cofnięcie zgody ma skutek od momentu wycofania zgody. Osoba, której prawa dotyczą wykonuje przysługujące jej uprawnienie za pośrednictwem stosownego formularza udostępnionego przez Administratora lub informuje na adres poczty elektronicznej Administratora. Cofnięcie zgody nie wpływa na przetwarzanie dokonywane przez Administratora zgodnie z prawem przed jej cofnięciem. Cofnięcie zgody nie pociąga za sobą dla osoby, której dane dotyczą żadnych negatywnych konsekwencji. Może jednak uniemożliwić dalsze korzystanie z usług lub funkcjonalności, które zgodnie z prawem Administrator może świadczyć jedynie za zgodą.

Podstawa prawna: art. 7 ust. 3 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.2. Prawo dostępu do danych

Osoba, której dane dotyczą ma prawo uzyskać od Administratora potwierdzenie, czy przetwarza dane osobowe, a jeżeli ma to miejsce, ma prawo:

a) uzyskać dostęp do swoich danych osobowych;

b) uzyskać informacje o celach przetwarzania, kategoriach przetwarzanych danych osobowych, o odbiorcach lub kategoriach odbiorców tych danych, planowanym okresie przechowywania danych lub o kryteriach ustalania tego okresu, o prawach przysługujących jej na mocy RODO oraz o prawie wniesienia skargi do organu nadzorczego, o źródle tych danych, o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz o zabezpieczeniach stosowanych w związku z przekazaniem tych danych poza Unię Europejską;

c) uzyskać kopię swoich danych osobowych.

Osoba, której dane dotyczą może skierować prośbę np. na adres poczty elektronicznej Administratora.

Podstawa prawna: art. 15 RODO.

Ustawodawca przewidział sytuację, w której prawo dostępu może stać się przedmiotem nadużyć ze strony osób, którym ono przysługuje, np. gdyby klienci danego przedsiębiorstwa/sklepu internetowego celowo korzystali z przysługujących im uprawień w taki sposób, żeby wywołać określone negatywne konsekwencje w działalności firmy. Działając w kilka osób wielokrotnie w ciągu dnia wnioskując o dostęp do ich danych, całkowicie uniemożliwiliby normalne funkcjonowanie przedsiębiorstwa/ sklepu internetowego. Mając to na uwadze art. 15 ust. 3 RODO precyzuje, że Administrator jest zobowiązany do dostarczenia osobie, której dane dotyczą, jednej nieodpłatnej kopii danych osobowych podlegających przetwarzaniu. Jednak za każdą kolejną Administrator ma prawo pobrać opłatę w rozsądnej wysokości. Wynika ona z kosztów administracyjnych związanych z dostarczeniem kopii danych osobowych. Po uiszczeniu stosownej opłaty przez wnioskodawcę nie ma możliwości odmówienia mu dostępu do danych, niezależnie od liczby dotychczasowych wniosków.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.3. Prawo do sprostowania danych

Osoba, której dane dotyczą ma prawo do żądania od Administratora niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym przez przedstawienie dodatkowego oświadczenia, kierując prośbę np. na adres poczty elektronicznej Administratora.

Podstawa prawna: art. 16 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.4. Prawo do usunięcia danych („prawo do bycia zapomnianym")

Osoba, której dane dotyczą ma prawo do żądania usunięcia wszystkich lub niektórych danych osobowych.

Osoba, której dane dotyczą ma prawo żądania usunięcia danych osobowych, jeżeli:

a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w których były przetwarzane;

b) wycofała określoną zgodę, w zakresie w jakim dane osobowe były przetwarzane w oparciu o jej zgodę;

c) wniosła sprzeciw wobec wykorzystywania jej danych w celach marketingowych;

d) dane osobowe są 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 Administrator podlega;

f) dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Pomimo żądania usunięcia danych osobowych, w związku z wniesieniem sprzeciwu lub wycofaniem zgody, Administrator może zachować pewne dane osobowe w zakresie niezbędnym do celów ustalenia, dochodzenia lub obrony roszczeń. Dotyczy to w szczególności danych osobowych obejmujących: imię, nazwisko, adres e-mail, które to dane zachowujemy dla celów rozpatrywania skarg oraz roszczeń związanych z korzystaniem z naszych usług, czy też dodatkowo adresu zamieszkania/ adresu korespondencyjnego, numeru zamówienia które to dane zachowujemy dla celów rozpatrywania skarg oraz roszczeń związanych z zawartymi umowami sprzedaży/ świadczenia usług. Osoba, której dane dotyczą może skierować prośbę np. na adres poczty elektronicznej Administratora.

Zgodnie z art. 17 ust. 2 RODO nakłada na Administratorów Danych Osobowych, o których mowa w ustępie 1, obowiązek poinformowania innych Administratorów posiadających te dane o żądaniu usunięcia wszelkich łączy do nich, kopii i replikacji. Jednocześnie ten obowiązek powinien zostać zrealizowany przy użyciu „dostępnych dla Administratora rozwiązań i kosztów realizacji". Można zatem wywnioskować, że w przypadku gdy Administrator będzie zmuszony ponieść nadmiernie wysokie koszty lub nie będzie dysponował odpowiednimi środkami technicznymi, może odmówić wykonania obowiązku. Jego działania w kierunku zrealizowania swojej powinności muszą być zatem rozsądne.

Artykuł 17 ust. 3 wskazuje również przypadki (katalog zamknięty), które wyłączają prawo do bycia zapomnianym osobie, która udostępnia swoje dane. Są to:

a) korzystanie z prawa do wolności wypowiedzi i informacji.

   Np. Właściciel gazety nie musi usuwać informacji o osobie w ramach przeprowadzonego śledztwa dziennikarskiego ujawniającego niewygodne czy nawet krepujące fakty z jej życia, bowiem w ten sposób jest realizowana wolność wypowiedzi i informacji;

b) wykonywanie prawnego obowiązku przetwarzania danych na mocy prawa UE lub państwa członkowskiego, któremu podlega Administrator, lub do wykonywanie zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Administratorowi.

   Np. Przedsiębiorca, nawet na wniosek pracownika, nie może usunąć jego danych po wygaśnięciu stosunku pracy, bowiem przepisy wymagają przechowywania ich przez 50 lat, a od 1 stycznia 2019 roku przez 10 lat. W przypadku zorganizowania akcji promocyjnej – przedsiębiorca jest zobowiązany przechowywać określone dane przez 5 lat od końca roku kalendarzowego, w którym odbywał się konkurs;

c) względy interesu publicznego w dziedzinie zdrowia publicznego w związku z art. 9 ust.2 lit. h) oraz i), a także art. 9 ust. 3 RODO to wyłączenie prawa do bycia zapomnianym dotyczy różnych danych związanych ze zdrowiem i zabezpieczeniem społecznym zatrudnionego, przetwarzanych przez lub na odpowiedzialność osoby (lub pracownika podmiotu administrującego), który podlega tajemnicy zawodowej. Dotyczy także danych, których przetwarzanie jest niezbędne ze względu na interes publiczny w dziedzinie zdrowia publicznego (np. ochrona przed poważnymi, transgranicznymi zagrożeniami zdrowotnymi czy zapewnienie wysokich standardów jakości opieki zdrowotnej i produktów leczniczych).

   Np. Powiatowy Inspektor Sanitarny prowadzi rejestr osób uchylających się od szczepień. Rejestr ten jest prowadzony ze względu na zdrowie publiczne, tj. zdrowie społeczeństwa jako całości. Osoby tam figurujące nie mogą wykorzystać prawa do bycia zapomnianym (usunięcia danych), aby usunąć informacje o sobie lub o swoich dzieciach;

d) ze względu na cele archiwalne w interesie publicznym, badania naukowe, historyczne, statystyczne – jeżeli

prawdopodobne jest, że skorzystanie z prawa do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania. Takiemu przetwarzaniu danych towarzyszyć musi wdrożenie środków technicznych i organizacyjnych służących zachowaniu zasady minimalizacji danych. Środki te mogą obejmować także pseudonimizację danych, jeśli pozwala ona realizować powyższe cele. Jeśli cele można realizować w drodze dalszego przetwarzania przy użyciu danych, które nie pozwalają na identyfikację osoby, należy je realizować w ten sposób.

Np. Lekarz do celów naukowych zbiera zdjęcia pacjentów ze zdiagnozowanym rakiem skóry. Realizacja prawa do bycia zapomnianym utrudni realizację celów przetwarzania, czyli badania naukowe;

e) ustalanie, dochodzenie oraz ochronę roszczeń.

Podstawa prawna: art. 17 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.5. Prawo do ograniczenia przetwarzania danych

Osoba, której dane dotyczą ma prawo do żądania ograniczenia przetwarzania jego danych osobowych. Zgłoszenie żądania, do czasu jego rozpatrzenia uniemożliwia korzystanie z określonych funkcjonalności lub usług, z których korzystanie będzie się wiązało z przetwarzaniem danych objętych żądaniem.

Klient ma prawo do żądania ograniczenia wykorzystania danych osobowych w następujących przypadkach:

a) gdy kwestionuje prawidłowość swoich danych osobowych – wówczas Administrator ogranicza ich wykorzystanie na czas potrzebny do sprawdzenia prawidłowości danych, nie dłużej jednak niż na 7 dni;

b) gdy przetwarzanie danych jest niezgodne z prawem, a zamiast usunięcia danych osoba, której dane dotyczą zażąda ograniczenia ich wykorzystania;

c) gdy dane osobowe przestały być niezbędne do celów, w których zostały zebrane lub wykorzystywane, ale są one potrzebne osobie, której dane dotyczą w celu ustalenia, dochodzenia lub obrony roszczeń;

d) gdy osoba, której dane dotyczą wniosła sprzeciw wobec wykorzystania jej danych – wówczas ograniczenie następuje na czas potrzebny do rozważenia, czy – ze względu na szczególną sytuację – ochrona interesów, praw i wolności osoby, której dane dotyczą przeważa nad interesami, które realizuje Administrator, przetwarzając dane osobowe osoby, której dane dotyczą.

Osoba, której dane dotyczą może skierować prośbę, np. na adres poczty elektronicznej Administratora.

Przykład: Administrator sklepu/serwisu internetowego, zbiera dane osobowe klientów dokonujących zakupu towarów/usług. Klient nie wyraził zgody na przesyłanie newslettera, jednakże regularnie dostaje newsletter z aktualną ofertą handlową. Osoba, której dane dotyczą kwestionuje zatem legalność przetwarzania danych osobowych w tym zakresie, jednocześnie chcąc nadal pozostać klientem tego sklepu. Do czasu wyjaśnienia zaistniałej sytuacji, klient ma prawo żądać ograniczenia przetwarzania jego danych – Administrator nie ma prawa wysyłać mu newslettera z ofertą, ale nie powinno przeszkadzać to klientowi w robieniu zakupów w tym sklepie.

Jeśli na mocy powyższych przypadków przetwarzanie zostało ograniczone dane, które zostały objęte ograniczeniem, mogą być przetwarzane:

a) wyłącznie za zgodą osoby, do której dane należą;

b) w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej;

c) z uwagi na ważne względy interesu publicznego Unii Europejskiej lub państwa członkowskiego.

Podstawa prawna: art. 18 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.6. Prawo do przenoszenia danych

Osoba, której dane dotyczą ma prawo otrzymać swoje dane osobowe, które dostarczyła Administratorowi, a następnie przesłać je do innego, wybranego przez siebie, Administratora Danych Osobowych. Osoba, której dane dotyczą ma również prawo żądać, by dane osobowe zostały przesłane przez nas bezpośrednio innemu Administratorowi, o ile jest to technicznie możliwe.

Osoba, której dane dotyczą może skierować prośbę np. na adres poczty elektronicznej Administratora.

W takim przypadku Administrator może przesłać dane osobowe w postaci pliku w formacie csv, który jest formatem powszechnie używanym, nadającym się do odczytu maszynowego i pozwalającym na przesłanie otrzymanych danych do innego Administratora Danych Osobowych.

Podstawa prawna: art. 20 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna: art. 12 ust. 3 i 4 RODO.

4.7. Prawo do sprzeciwu wobec wykorzystania danych

Osoba, której dane dotyczą ma prawo w dowolnym momencie wnieść sprzeciw wobec wykorzystania jej danych osobowych, w tym profilowania, jeżeli Administrator przetwarza jej dane w oparciu o prawnie uzasadniony interes, np. marketing produktów i usług Administratora, prowadzenie statystyki korzystania z poszczególnych funkcjonalności sklepu/serwisu internetowego oraz ułatwienie korzystania ze sklepu/serwisu internetowego, a także badanie satysfakcji.

Rezygnacja w formie wiadomości e-mail z otrzymywania komunikatów marketingowych dotyczących produktów lub usług, będzie dla Administratora oznaczać sprzeciw osoby, której prawa dotyczą na przetwarzanie jego danych osobowych, w tym profilowanie w tych celach.

Jeżeli sprzeciw osoby, której dane dotyczą okaże się zasadny *(Prawo do wniesienia sprzeciwu przysługuje osobie, której dane dotyczą, w przypadku gdy przetwarzanie danych jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej, a także gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów Administratora lub strony trzeciej (opiera się na podstawie określonej w art. 6 ust. 1 lit. e lub f* RODO) i Administrator nie będzie miał innej podstawy prawnej do przetwarzania danych osobowych, dane osobowe osoby, której dotyczą zostaną usunięte, wobec wykorzystania których osoba, której dane dotyczą wniosła sprzeciw.

Podstawa prawna: art. 21 RODO.

Zgodnie z art. 22 RODO 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 niej skutki prawne lub w podobny sposób istotnie na nią wpływa. Jednakże profilowanie będzie dozwolone wyłącznie wtedy, kiedy:

a) jest niezbędne do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a Administratorem;

b) jest dozwolona prawem Unii lub prawem państwa członkowskiego;

c) opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

W przypadku wykonywania czynności profilowania Administrator wdraża właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony Administratora do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji.

Podstawa prawna: art. 22 RODO.

O spełnieniu żądania Administrator informuje osobę, której dane dotyczą, wskazując sposób realizacji żądania. Administrator bez zbędnej zwłoki - a w każdym razie w terminie miesiąca od otrzymania żądania - udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Administrator informuje osobę, której dane dotyczą, o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.

W sytuacji, gdy Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, niezwłocznie - najpóźniej w terminie miesiąca od otrzymania żądania - informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

Podstawa prawna art. 12 ust. 3 i 4 RODO.

5.
Privacy by design oraz Privacy by default

RODO wprowadza dwie nowe definicje mające wpływ na sposób, w jaki w firmie wprowadza się nowe rozwiązania, czyli na co dodatkowo trzeba zwracać uwagę przy definiowaniu nowych produktów lub usług, za pośrednictwem których będą dane osobowe przetwarzane.

Privacy by design to wkomponowanie problemu ochrony danych osobowych, w działania Administratora, począwszy od etapu planowania procesu, a więc jeszcze przed nadaniem mu warstwy technicznej, wyłącznie na etapie warstwy koncepcyjnej. Pomocny w tym przypadku jest artykuł 25 RODO, który mówi, że „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 wynikające z przetwarzania, 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 realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi niniejszego rozporządzenia oraz chronić prawa osób, których dane dotyczą". W praktyce przedsiębiorca planujący przeprowadzenia np. akcji marketingowej lub konkursu, będzie zobowiązany do przeprowadzenia oceny, czy zakładane operacje na danych osobowych oraz sposoby ich zabezpieczenia, będą zgodne z obowiązującymi przepisami. Zatem już na tym etapie przedsiębiorca powinien rozważyć na jakiej przesłance zostanie oparty proces przetwarzania danych osobowych. Należy również pamiętać, że **privacy by design** nie ogranicza się jedynie do etapu planowania. Z przepisów RODO wynika, że ocena zgodności z przepisami dotyczy również etapu realizacji procesu. Zatem, aby zapewnić zgodność z **privacy by design** zasadnym będzie regularny przegląd funkcjonowania procesu przetwarzania danych oraz jego elementów. Przy czym proces przetwarzania danych często nie kończy się w momencie zakończenia akcji, np. w przypadku konkursu dane osobowe będą przetwarzane dłużej niż do dnia przyjmowania zgłoszeń, pozostaje później jeszcze kwestia wydania nagród, odprowadzenia podatków, rozpatrzenia reklamacji i archiwizacji zgłoszeń.

Privacy by design nie jest pojęciem nowym, funkcjonuje na rynku już od dłuższego czasu, niemniej jednym z bardziej istotnych dla przedsiębiorcy wiarygodnych źródeł informacji w tym zakresie może być interpretacja, która powstała w wyniku prac Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności z 2010 r. Zgodnie z nią ochrona prywatności w fazie projektowania powinna się opierać na siedmiu zasadach:

1) podejście proaktywne, nie reaktywne i zaradcze, nie naprawcze;
2) prywatność jako ustawienie domyślne;
3) prywatność włączona w projekt;
4) pełna funkcjonalność: suma dodatnia, nie suma zerowa;
5) ochrona od początku do końca cyklu życia informacji;
6) widoczność i przejrzystość;
7) poszanowanie dla prywatności użytkowników.

Privacy by default jest zapewnieniem, aby domyślnie były przetwarzane dane wyłącznie niezbędne do osiągnięcia konkretnego celu przetwarzania; zapewnienie ustawień gwarantujących ochronę danych jako pierwotnych ustawień systemu informatycznego czy oprogramowania. Zmiana tych ustawień powinna następować jedynie na wyraźne żądanie użytkownika oprogramowania/systemu. Co za tym idzie **privacy by default** wymaga ustawień oprogramowania/systemu zapewniających możliwie najszerszą ochronę prywatności wszystkich użytkowników. Użytkownicy, którzy chcą ograniczyć swoją prywatność, muszą podjąć aktywne działania w tym kierunku. ADO tworząc oprogramowanie/system nie mogą wobec tego wprowadzać domyślnych ustawień ingerujących w prywatność użytkowników. To czy dane osobowe są niezbędne dla osiągnięcia konkretnego celu przetwarzania należy rozpatrywać w odniesieniu do:

- ilości zbieranych danych;
- zakresu ich przetwarzania;
- okresu ich przechowywania;
- ich dostępności.

W zakresie istniejących rozwiązań, tj. produktów lub usług należy uwzględnić nowe wymogi w zakresie RODO i odpowiednio dostosować produkty lub usługi do nich.

6.
Profilowanie

Profilowanie – jako proces przetwarzania danych osobowych, w wyniku którego dochodzi do oceny osoby – zostało uregulowane w RODO (Rozporządzenie unijne dotyczące ochrony danych osobowych czyli 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). Nowe unijne przepisy nadają osobom prawo do niepodlegania decyzjom, podejmowanym bez ingerencji człowieka – wyłącznie w procesach zautomatyzowanych, jeśli decyzje te wywołują skutki prawne dla osoby, której dane dotyczą. Prawo to nie będzie przysługiwało osobie, jeżeli decyzja podjęta została na podstawie zgody osoby lub kiedy była podjęta w celu realizacji umowy. Każdorazowo zautomatyzowane podejmowanie decyzji będzie wiązało się z dodatkowymi, nowymi obowiązkami informacyjnymi Administratora Danych.

Czym jest profilowanie według RODO?

Można wyróżnić dwie kategorie profilowania: polegające na ocenie prawdziwych informacji pozyskanych na temat danej osoby albo na wytworzeniu nowej informacji o osobie, wywnioskowanej na podstawie wiedzy pozyskanej na jej temat. W drugim przypadku nowa informacja będzie jedynie statystycznie prawdziwa, a co za tym idzie pojawia się ryzyko przypisania podmiotowi danych cech, których w istocie on nie posiada, co z kolei może doprowadzić do dyskryminacji rozumianej tu jako nieusprawiedliwione pozbawienie go dostępu do pewnych dóbr i usług.

Można wyróżnić profilowanie zwykłe (z udziałem czynnika ludzkiego) oraz zautomatyzowane, w którym cały proces oceny oraz podjęcie decyzji dokonują systemy informatyczne. Należy zauważyć, że wskazane wyżej kategorie profilowania mogą przybierać zarówno formę profilowania zwykłego, jak i zautomatyzowanego.

RODO jest pierwszym aktem prawa unijnego, które zdefiniowało pojęcie profilowania. Zgodnie z art. 4 pkt 4 RODO, profilowanie to dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej. RODO podaje przykłady czynników osobowych, które w szczególności mogą podlegać analizie lub prognozowaniu. Będą to m.in. aspekty dotyczące efektów pracy osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Zgodnie z RODO profilowaniem będzie tylko takie przetwarzanie danych, które spełnia jednocześnie dwa warunki.

Po pierwsze, profilowanie zachodzi gdy procesy z nim związane mają wyłącznie zautomatyzowany charakter, tzn. odbywają się bez ingerencji człowieka. Po drugie, procesy te prowadzą do oceny osoby fizycznej, jej sytuacji lub przewidywanych zachowań. Podsumowując, nie każdy zautomatyzowany proces przetwarzania danych osobowych będzie profilowaniem, a jedynie taki, który powoduje poddanie ocenie osoby, której dane dotyczą.

Prawo osoby do niepodlegania zautomatyzowanemu podejmowaniu decyzji

Zgodnie z art. 22 RODO osoba, której dane dotyczą ma prawo do niepodlegania zautomatyzowanym decyzjom, jeżeli decyzja podjęta w wyniku takiego zautomatyzowanego profilowania **wywołuje skutki prawne dla osoby lub istotnie wpływa na jej sytuację.**

RODO przewiduje sytuacje, kiedy prawo niepodlegania automatycznie podjętej decyzji wywołującej skutki prawne zostaje wyłączone. W przypadku danych zwykłych będą to sytuacje gdy:

1. jest ono konieczne do zawarcia i wykonania umowy. Zawsze takie profilowanie powinno odbywać się przy zapewnieniu przez Administratora właściwych środków ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą, a co najmniej prawa do uzyskania interwencji ludzkiej ze strony Administratora, do wyrażenia własnego stanowiska i do zakwestionowania tej decyzji. Przykładem takiego profilowania, które nie generuje prawa do niepodlegania automatycznej decyzji jest automatyczne badanie zdolności kredytowej przez bank, czy ocena ryzyka przy zawieraniu umowy z ubezpieczycielem. Aby zapewnić warunki określone w RODO powinna zostać dopuszczona przez Administratora możliwość odwołania się od tej decyzji i złożenia wyjaśnień przez osobę, która np. otrzymała negatywną odpowiedź na swój wniosek kredytowy;
2. jest ono dozwolone prawem Unii lub prawem państwa członkowskiego, któremu podlega Administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.
3. osoba, której dane dotyczą wyraziła zgodę na takie profilowanie, np. przy otrzymywaniu specjalnych ofert od sklepu internetowego. W przypadku profilowania na podstawie zgody, Administrator również powinien wdrożyć wyżej wskazane środki tak jak przy profilowaniu w celu zawarcia i wykonania umowy.

Prawo niepodlegania automatycznie podjętej decyzji wywołującej skutki prawne zostaje wyłączone również w przypadku profilowania obejmującego dane szczególnych kategorii (tzw. dane wrażliwe, m.in. informacje o stanie zdrowia, orientacji seksualnej, przekonaniach religijnych), w sytuacjach gdy:

1. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
2. osoba, której dane dotyczą wyraziła wyraźną zgodę na takie profilowanie i istnieją właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą.

Obowiązki Administratora Danych

Rozporządzenie unijne wprowadza kilka wymogów, jakie Administratorzy Danych Osobowych zobowiązani są spełnić wobec osób, których dane planują „profilować".

Pierwszym wymogiem jest spełnienie obowiązku informacyjnego, a więc wskazania podmiotowi danych, że proces ten ma miejsce, jakie są jego konsekwencje i czy dzieje się to w sposób zautomatyzowany.

W przypadku wykorzystania danych zwykłych i danych szczególnych kategorii należy podać:

1. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO;
2. istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Wyżej wspomniany art. 22 ust. 1 i 4 RODO dotyczy przypadków, gdy profilowanie nie jest niezbędne do wykonania umowy, nie ma swojej podstawy w przepisach prawa i nie jest dokonywane na podstawie zgody, oraz gdy decyzje podjęte w takim procesie opierają się na szczególnej kategorii danych (danych wrażliwych). W takiej sytuacji należy dodatkowo przekazać:

1. informacje o zasadach podejmowania takich decyzji – czyli w jaki sposób ta ocena następuje oraz przy pomocy jakich narzędzi będzie dochodzić do takiej oceny;

2. informacje o znaczeniu i przewidywanych konsekwencjach dla osoby, której dane te dotyczą, tzn. wyjaśnienie, jakie skutki prawne może nieść za sobą taka decyzja lub w jaki sposób prawnie będzie ta decyzja na daną osobę wpływać – np. zwiększona składka ubezpieczeniowa, zmiana zakresu ubezpieczenia, odrzucenie lub odroczenie wniosku o zawarcie umowy.

Kolejnym obowiązkiem Administratora Danych jest umożliwienie podmiotowi danych wniesienia sprzeciwu wobec profilowania (art. 21 ust. 1 i 2 RODO). Obowiązek ten odnosi się do każdej kategorii profilowania (zarówno z udziałem czynnika ludzkiego, jak i zautomatyzowanego).

Najczęściej profilowanie będzie nieodłącznym elementem przetwarzania danych w celu marketingu własnych produktów i usług Administratora z zamiarem przygotowania zindywidualizowanej oferty handlowej. W takiej sytuacji podmiot danych będzie miał prawo wniesienia sprzeciwu zarówno wobec przetwarzania danych w celu marketingowym, jak i profilowania w celach marketingowych (jeżeli dane te są dodatkowo profilowane w celach marketingowych).

Ostatnim obowiązkiem Administratora Danych związanym z profilowaniem jest realizacja prawa podmiotu danych do dostępu do przetwarzanych danych. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące. Jeżeli takie przetwarzanie ma miejsce, osoba ma prawo do dostępu do danych oraz do uzyskania informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO 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. W razie wpłynięcia wniosku o umożliwienie dostępu do danych, Administrator może udzielić tych samych informacji co w klauzuli informacyjnej.

Nadmienić należy, że powyższe wymogi obejmują każde zautomatyzowane podejmowanie decyzji ze skutkiem dla osoby, a profilowanie jest tylko jednym z rodzajów automatycznego przetwarzania.

Profilowanie w handlu elektronicznym

Wiele sklepów działających w branży e-commerce stosuje profilowanie, które jest skutecznym sposobem na bardziej efektywną sprzedaż produktów, przy jednoczesnym zmniejszeniu nakładów finansowych na działania promocyjne. Jak profilowanie w sklepach internetowych wygląda w praktyce? Przykładem może być gromadzenie oraz analizowanie danych klienta takich jak jego wiek, płeć, data urodzenia, miejsce zamieszkania, zainteresowania, zachowanie na stronie czy ostatnio dokonane zakupy. Dzięki tym informacjom właściciel sklepu internetowego może przesyłać klientowi bardziej zindywidualizowaną ofertę, która z większym prawdopodobieństwem go zainteresuje.

Zgodnie z nowymi unijnymi przepisami właściciele sklepów internetowych (jako Administratorzy danych osobowych) powinni informować swoich klientów o fakcie profilowania, jeśli połączone jest ono ze zautomatyzowanym podejmowaniem decyzji, wywołującym skutki prawne lub w inny sposób istotnie wpływającym na klientów.

7.
Inspektor Ochrony Danych

Kiedy należy powołać Inspektora Ochrony Danych (dawniej Administratora Bezpieczeństwa Informacji – ABI) według RODO?

RODO przewiduje powołanie Inspektora Ochrony Danych (IOD, ang. *data protection officer*), którego status i obowiązki są zbliżone do tych przewidzianych na gruncie ustawy o ochronie danych osobowych dla Administratora Bezpieczeństwa Informacji (ABI), ale w istotny sposób rozszerzone. Ważną zmianą jaką wprowadza RODO jest to, iż w niektórych przypadkach obowiązkowym stanie się powołanie inspektora, czyli osoby zajmującej ochroną danych osobowych w jednostce organizacyjnej. Poniżej odpowiadamy na pytanie, czy i kiedy należy powołać Inspektora Ochrony Danych oraz na jakich zasadach.

Kiedy powołanie IOD jest obowiązkowe?

Na mocy art. 37 ust. 1 RODO istnieją **trzy przypadki, kiedy Administrator lub podmiot przetwarzający dane obligatoryjnie wyznaczają IOD**.

1. Dane przetwarza organ lub podmiot publiczny

Po pierwsze, gdy przetwarzania danych osobowych dokonują organ lub podmiot publiczny, z wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości. Sądy wyznaczają IOD, ale do zakresu jego kompetencji nie należy monitorowanie przestrzegania przepisów co do danych przetwarzanych w związku z czynnościami orzeczniczymi, jak np. dane zawarte w aktach sądowych, czy bazach prawnych.

2. Działalność wymaga regularnego i systematycznego monitorowania

Po drugie, gdy 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.

W tej przesłance zawartych jest kilka pojęć, które nie zostały wprost zdefiniowane i mogą budzić wątpliwości. Zgodnie z motywem nr 97 preambuły RODO, za główną działalność Administratora w sektorze prywatnym można uznać przetwarzanie danych osobowych, jeżeli stanowi ono jego zasadnicze, a nie poboczne czynności.

Kolejnym niejasnym elementem obowiązku jest konieczność przetwarzania danych na dużą skalę, która nie została w żaden sposób określona, choć na etapie projektowania RODO pojawiła się propozycja, by wskazać konkretną, minimalną liczbę,

określając ją jako średnio 5 tys. osób rocznie.

Trudność interpretacyjną może również budzić konieczność regularnego i systematycznego monitorowania osób, które należy rozumieć szerzej niż profilowanie oraz monitorowanie zachowania, raczej jako obserwowanie osób w sposób ciągły lub w określonych odstępach czasu w wykonaniu z góry powziętego planu, czy też w oparciu o określony system czy metodologię. Jako przykład można przytoczyć podmioty z sektora usług finansowych, IT, ubezpieczeniowych i transportu lotniczego.

3. Przetwarzanie danych wrażliwych i informacji o wyrokach

Po trzecie, gdy główna działalność Administratora lub podmiotu przetwarzającego polega na przetw arzaniu na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 (dane wrażliwe) oraz danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 (przetwarzanie tych danych odbywa się wyłącznie pod nadzorem władz publicznych). Przykładem są tu podmioty z sektora usług medycznych i farmaceutycznych oraz podmioty przetwarzające informacje o skazaniach.

Powołanie fakultatywne oraz przewidziane w odrębnych przepisach unijnych lub krajowych

Oprócz obligatoryjnych przypadków powołania IOD, na mocy art. 37 ust. 4, istnieje możliwość lub – jeżeli wymaga tego prawo UE lub prawo państwa członkowskiego – obowiązek powołania Inspektora Ochrony Danych przez Administratora, podmiot przetwarzający, zrzeszenia lub inne podmioty reprezentujące określone kategorie Administratorów lub podmiotów przetwarzających. Inspektor Ochrony Danych może działać w imieniu takich zrzeszeń i innych podmiotów reprezentujących Administratorów lub podmioty przetwarzające.

IOD wyznaczą Administratorzy i procesorzy

Nowością jaką wprowadziło RODO jest możliwość, a także w wyżej wymienionych sytuacjach obowiązek – identyczny z tym ciążącym na Administratorze Danych – by Inspektora Ochrony Danych wyznaczył podmiot przetwarzający dane. Zgodnie z definicją z art. 4 pkt. 8 RODO podmiot przetwarzający oznacza osobę fizyczną, prawną, organ publiczny lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora. Administrator, powierzając czynności przetwarzania powinien korzystać wyłącznie z usług podmiotów zapewniających wystarczające gwarancje wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO, w szczególności podmiotom reprezentującym wysoki poziom fachowej wiedzy, wiarygodność oraz zasoby. Z drugiej strony, by ocenić profesjonalizm procesora – dla Administratora znaczenie będą miały kwalifikacje Inspektora Ochrony Danych procesora i to, jaki poziom ochrony danych stara się on zapewnić.

Jeden IOD dla grupy przedsiębiorstw

RODO – w art. 37 ust. 2 – wprost dopuszcza możliwość wyznaczenia jednego Inspektora Ochrony Danych przez grupę przedsiębiorstw lub przez kilka podmiotów administracji publicznej. Warunkiem postawionym w przepisie jest konieczność łatwego nawiązania kontaktu z IOD z każdej jednostki organizacyjnej. Mimo że nie istnieje przepis dopuszczający powołania jednego ABI dla więcej niż jednej jednostki, w praktyce takie rozwiązanie funkcjonuje w obrocie. Z uwagi na to, że Administrator ma możliwość wyboru formy zatrudnienia, często funkcję ABI świadczy pracownik wyspecjalizowanej w dziedzinie ochrony danych osobowych firmy czy kancelarii. Zwraca się uwagę, że organ nadzorczy powinien określić swoje stanowisko – w oparciu o praktykę innych państw członkowskich, czy na gruncie RODO będzie możliwe, aby jedna osoba pełniła funkcję IOD w kilku podmiotach nie będących grupą przedsiębiorców. Mimo że w RODO nie zawiera wyrażonego wprost zakazu, to wydaje się, że wprowadzenie wymogu łatwego kontaktu dla IOD, wyznaczonego przez grupę przedsiębiorców – przesądza o stałej pozycji prawnej IOD – z którym powinna być możliwość nawiązania łatwego kontaktu. Rozwiązanie to ograniczyłoby sytuacje, gdy jedna osoba jest powoływana na inspektora przez nawet kilkudziesięciu Administratorów Danych. Takie sytuacje mają miejsce na gruncie obecnie obowiązujących przepisów, co z pewnością zaprzecza możliwości skutecznego realizowania kompetencji ABI.

Forma stosunku prawnego z IOD

RODO, podobnie jak ustawa o ochronie danych osobowych, dopuszcza zastosowanie różnych form stosunku prawnego łączącego Administratora (procesora) z inspektorem. Zgodnie z art. 37 ust. 6 RODO, IOD może być członkiem personelu Administratora lub podmiotu przetwarzającego, jak też wykonywać swoje kompetencje na podstawie umowy o świadczenie usług. Odnośnie miejsca w strukturze organizacyjnej, na mocy art. 38 ust. 3 inspektor podlega bezpośrednio najwyższemu kierownictwu Administratora lub podmiotu przetwarzającego.

Obowiązek podawania danych kontaktowych IOD

Na gruncie RODO nie przewidziano szczegółowych wymogów związanych z procedurą zgłoszenia organowi nadzorczemu powołania IOD. W art. 37 ust. 7 została zwięźle sformułowana konieczność poinformowania organu nadzorczego o danych kontaktowych inspektora. Przepisy RODO nie dają odpowiedzi jakie konkretnie dane powinny zostać przekazane organowi. Wydaje się, że za minimum należy uznać imię i nazwisko, adres korespondencyjny, może numer telefonu i adres e-mail. Mimo że RODO nie przewiduje obowiązku zgłoszenia odwołania IOD, konieczność zawiadomienia organu nadzorczego o danych kontaktowych inspektora determinuje Administratora do zaktualizowania tych danych, jeśli zmianie uległa osoba pełniąca omawianą funkcję.

W omawianym przepisie sformułowany został także wymóg opublikowania danych kontaktowych inspektora. Nie podana została jednak forma, w jakiej Administrator powinien te dane opublikować. Wymóg ten nie był dotychczas znany na gruncie UODO, choć jawność ogólnokrajowego rejestru ABI, opublikowanego w intrenecie przez GIODO dawała możliwość sprawdzenia czy dana jednostka organizacyjna powołała ABI, a jeśli tak, to kto pełni taką funkcję.

Kwalifikacje IOD

W RODO nie zostały wymienione żadne obiektywne kryteria, jakimi powinien kierować się Administrator i procesor przy wyborze IOD. Jedynym wymogiem – są kwalifikacje zawodowe i wyszczególniona w art. 37 ust. 5 wiedza fachowa na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia kompetencji IOD (z art. 39). Z regulacji można wyinterpretować takie kwalifikacje, jak znajomość problematyki ochrony danych osobowych nie tylko od strony prawnej, ale też praktycznej, np. rozeznanie w standardach zabezpieczeń danych. Kolejne kwalifikacje odpowiadające kompetencjom IOD, to np. umiejętność przeprowadzania szkoleń, czy komunikatywność, skuteczność w egzekwowaniu przestrzegania nałożonych przepisami i wewnętrzną dokumentacją zasad ochrony danych.

W konsekwencji w stosunku do IOD aktualne pozostaną komentarze do obecnie obowiązującego wymogu kwalifikacyjnego wobec ABI w postaci odpowiedniej wiedzy na gruncie UODO. „Wiedza fachowa" i „odpowiednia wiedza" stanowią pojęcia nieostre, które wymagają od Administratora powołującego osobę odpowiedzialną za ochronę danych osobowych – wykazania się własną interpretacją tego terminu z uwzględnieniem utrwalonych praktyk i piśmiennictwa w tej dziedzinie, a także specyfiki jednostki i branży, w której będzie funkcjonował powoływany ABI.

Porównanie statusu ABI i IOD

Można zauważyć wiele wspólnych elementów statusu ABI oraz statusu IOD. Zarówno UODO, jak i RODO przewidują wobec osoby nadzorującej przestrzeganie przepisów o ochronie danych osobowych jej podległość Administratorowi Danych. Wymagają od Administratora (lub procesora) zapewnienia tej osobie niezależności oraz niezbędnych środków do sprawowania jej kompetencji. Na gruncie obu regulacji Administrator ma również obowiązek powiadomienia organu nadzorczego o wyznaczeniu ABI/IOD oraz podania i aktualizowania jego danych kontaktowych. RODO wprowadza też rozwiązania nieznane na gruncie UODO, jak obowiązek powołania inspektora w określonych przypadkach oraz powołanie IOD przez procesora – podmiot przetwarzający dane, a także wymóg opublikowania jego danych kontaktowych IOD. Nowością na gruncie RODO jest też bierne wspieranie IOD poprzez niemożność odwołania lub ukarania go za wykonywanie przez niego obowiązków przez Administratora. To faktyczne gwarancje nowego statusu i nowej jakości Inspektora Ochrony Danych Osobowych w stronę standardów jego niezależnej, władczej, a także proaktywnej pozycji w systemie ochrony danych osobowych i całej strukturze organizacyjnej Administratora lub podmiotu przetwarzającego.

8.
Powierzenie danych osobowych

Powierzenie danych według RODO

Jeśli podmiot dokonuje operacji na danych osobowych na zlecenie Administratora, wówczas mówimy o tzw. powierzeniu danych. Co ważne, w takiej sytuacji podmiot przetwarzający dane nie staje się ich Administratorem. Mimo wszystko, ciąży na nim dokładnie taka sama odpowiedzialność jak na ADO.

Podmiot działający w imieniu Administratora przetwarza dane zgodnie z ustaleniami ADO. To od Administratora zależy cel oraz sposób dokonywania operacji na danych. Czynności dokonywane w ramach powierzenia danych obejmują np. ich gromadzenie, usuwanie, przechowywanie, bądź edycję.

Należy mieć na uwadze, że przekazując dane osobowe podmiotowi nieupoważnionemu narażamy się na duże kary. Co więcej, możemy ponieść ogromne straty wizerunkowe. W związku z tym, powierzenie danych osobowych musi mieć zawsze odpowiednie uzasadnienie prawne.

Podmiot przetwarzający dane na zlecenie ADO, nie może wykorzystywać ich do realizacji własnych celów. Dalsze udostępnianie, bądź sprzedawanie danych osobowych jest niezgodne z prawem, gdyż w dalszym ciągu są one własnością Administratora.

Przykłady powierzenia danych

Z powierzeniem danych spotkamy się bardzo często w naszym codziennym życiu. Zazwyczaj dotyczą one outsourcingu usług. Dobrym przykładem jest powierzenie księgowości naszej firmy biuru rachunkowemu, czy zlecenie kampanii newsletterowej agencji marketingowej. W obu przypadkach mamy do czynienia z przetwarzaniem danych zgodnie z wytycznymi Administratora.

Przykładów powierzenia danych osobowych jest oczywiście więcej. Warto wspomnieć o funkcjonowaniu zewnętrznego działu prawnego, biura pomocy, czy też korzystaniu z zewnętrznej obsługi BHP lub przeprowadzaniu przez agencję reklamową konkursów na zlecenie Klienta, a kończąc na firmie hostingowej

Obecny stan prawny

Przepisy ustawy o ochronie danych osobowych są bardzo ogólne. Umowa powierzenia danych powinna być zawarta w formie papierowej, a dane przetwarzane wyłącznie w zakresie i celu wskazanym przez Administratora.

Analizując obecny stan prawny, nie sposób pominąć kwestii dotyczących odpowiedzialności cywilnej Administratora, jak i podmiotu przetwarzającego dane. W przypadku uchybień, zarówno Administrator, jak i podmiot działający w jego imieniu mogą zostać pociągnięci do odpowiedzialności. ADO odpowiada za przestrzeganie przepisów ustawy o ochronie danych osobowych. Podmiot przetwarzający dane odpowiada natomiast w zakresie działania niezgodnego z umową powierzenia oraz w zakresie zapewnienia odpowiedniego systemu zabezpieczeń.

Zmiany wprowadzane przez RODO

Jedną ze zmian wprowadzanych przez RODO jest możliwość zawarcia umowy powierzenia danych osobowych w formie elektronicznej.

Nowe rozporządzenie skupia się w dużej mierze na roli podmiotu przetwarzającego. Powinien on zapewnić takie środki techniczne i organizacyjne, aby dane osobowe, na których dokonywane są operacje były odpowiednio zabezpieczone.

Ważną zmianą jest również to, że podmiot przetwarzający dane ma obowiązek ich usunięcia, bądź zwrócenia Administratorowi po zakończeniu współpracy.

O ile UODO nie reguluje możliwości dalszego powierzenia przetwarzania danych, o tyle RODO rozstrzyga tę kwestię. Podmiot wykonujący operacje na danych Administratora będzie mógł skorzystać z innego podmiotu przetwarzającego, tak zwanego podprocesora.

Jest to możliwe wyłącznie po uprzednim wyrażeniu zgody Administratora. W tym zakresie może on zdecydować się na:

- zgodę szczegółową – Administrator wskazuje konkretnego podprocesora/podprzetwarzającego;
- zgodę ogólną – podmiot przetwarzający dane informuje Administratora o planach dotyczących dalszego przetwarzania danych; w takich przypadkach Administrator może nie zgodzić się na propozycje procesora.

Co powinna zawierać umowa powierzenia danych zgodna z RODO?

Umowa powinna obligatoryjnie zawierać:

- określenie Administratora Danych;
- określenie podmiotu przetwarzającego dane na zlecenie Administratora;
- przedmiot i czas trwania przetwarzania;
- charakter i cel przetwarzania;
- rodzaj powierzanych danych osobowych oraz kategorie osób, których dane dotyczą;
- obowiązki i prawa Administratora;
- oświadczenia procesora, wskazujące jego obowiązki.

Katalog obowiązków podmiotu przetwarzającego dane, o których powinna stanowić umowa powierzenia został określony w art. 28 ust. 3 pkt. a-h RODO. Procesor, podpisując umowę powierzania z ADO powinien oświadczyć między innymi, że:

- przetwarza dane osobowe wyłącznie na udokumentowane polecenie Administratora;
- zapewnia, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania tajemnicy;
- podejmuje wszelkie środki wymagane na mocy art. 32 RODO;
- pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą;
- po zakończeniu świadczenia usług związanych z przetwarzaniem zależnie od decyzji Administratora usuwa lub

zwraca mu wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że prawo Unii lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

Opisane powyżej elementy, które muszą być zawarte w umowie, choć stanowią stosunkowo obszerny katalog, w zależności od konkretnego przypadku mogą nie wyczerpywać całokształtu obszarów, które należy uwzględnić przy powierzeniu przetwarzania.

Katalog elementów umowy o przetwarzanie danych, zawarty w art. 28 ust. 3 został skonstruowany w sposób otwarty, pozostawiając tym samym Administratorowi pole do dalszych decyzji. Tym samym ustalenia między stronami relacji powierzenia mogą obejmować jeszcze inne elementy, obudowujące proces przetwarzania. W ramach takich ustaleń strony mogą uzgodnić także elementy fakultatywne umowy powierzenia, dotyczące m.in. kwestii związanych z:

- ewentualnym regresem w przypadku naruszenia przez podmiot przetwarzający przepisów w zakresie ochrony danych osobowych i ustaleniem rozkładu odpowiedzialności w relacjach wewnętrznych pomiędzy Administratorem a podmiotem przetwarzającym;
- zastrzeżeniem kar umownych w przypadku naruszenia przez podmiot przetwarzający postanowień umowy;
- wprowadzeniem szczegółowych zasad prowadzenia audytów lub inspekcji przez Administratora;
- skutecznością i mocą wiążącą zaleceń wydawanych w toku prowadzonych audytów lub inspekcji;
- wspieraniem Administratora w przypadku kontroli przestrzegania przepisów RODO;
- zasadami współpracy z inspektorem ochrony danych powołanym po stronie podmiotu przetwarzającego;
- wynagrodzeniem z tytułu przetwarzania danych w imieniu Administratora;
- możliwymi sposobami zakończenia współpracy;
- stosownymi obostrzeniami lub konkretnymi rozstrzygnięciami w zakresie obligatoryjnych środków technicznych i organizacyjnych, których zastosowania żąda Administrator;
- ustaleniem prawa właściwego w relacjach transgranicznych.

*Dodatek specjalny
Ochrona danych osobowych pracowników po wejściu w życie RODO

RODO wpłynie na zmiany w Kodeksie pracy. Zmodyfikowany będzie katalog danych osobowych pobieranych od osoby ubiegającej się o zatrudnienie oraz od pracownika. Unormowane zostaną zasady wyrażenia zgody przez osobę ubiegającą się o zatrudnienie lub pracownika na pobranie określonych danych osobowych przez pracodawcę (w przypadku pracownika chodzi np. o dane biometryczne). Ustawodawca wprowadza negatywny katalog danych, których pozyskanie nie może nastąpić nawet za zgodą osoby ubiegającej się o zatrudnienie lub pracownika. Zmiany nastąpią również w monitoringu pracowników. Wprowadzono także podstawę prawną (chodzi o zmianę w zakresie art. 229) do pozyskiwania i przechowywania przez pracodawcę skierowań na badania lekarskie oraz orzeczeń lekarskich wydawanych w wyniku tego skierowania, jeżeli osoba przyjmowana do pracy u innego pracodawcy posiada aktualne orzeczenie lekarskie stwierdzające brak przeciwskazań do pracy na danym stanowisku.

Poniżej omówienie poszczególnych zmian.

Zamiana art. 22 [1] Kodeksu pracy

Zgodnie z projektem pracodawca będzie mógł żądać podania od osoby ubiegającej się o zatrudnienie danych osobowych obejmujących:

1) imię (imiona) i nazwisko;

2) datę urodzenia;

3) adres do korespondencji;

4) adres poczty elektronicznej albo numer telefonu;

5) wykształcenie;

6) przebieg dotychczasowego zatrudnienia.

Choć kandydaci właściwie sami podawali w CV adres e-mail albo numer telefonu, od 25 maja 2018 r., są to dane, które pracodawca może pozyskiwać w procesie rekrutacji. Jednocześnie z listy danych, których można żądać, zniknęły imiona rodziców kandydata.

Natomiast § 2 art. 22 [1] dotyczy już pracownika. Pracodawca będzie mógł żądać od pracownika podania danych osobowych obejmujących:

1) adres zamieszkania;

2) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;

3) inne dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny, jeżeli podanie takich danych jest konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy.

W przypadku pracowników wprowadzono możliwość żądania – w przypadku braku numeru PESEL – danych o rodzaju i numerze innego dokumentu potwierdzającego tożsamość pracownika.

Zmieniono § 3 art. 22 [1], którego projekt stanowi, że „Udostępnienie pracodawcy danych osobowych następuje w formie oświadczenia osoby, której one dotyczą. Pracodawca żąda udokumentowania danych osobowych osób, o których mowa w § 1 i 2, jeżeli uzna za konieczne ich potwierdzenie**”.**

Zgodnie z art. 22 [1] § 4. przetwarzanie danych osobowych, o których mowa w § 1–3, będzie możliwe tylko w zakresie niezbędnym do realizacji stosunku pracy.

Znaczącą zmianę wprowadza § 5 art. 22 [1]. Zgodnie z nim przetwarzanie danych osobowych, uzyskanych na podstawie § 1 pkt 3 i 4 po nawiązaniu stosunku pracy, jest możliwe tylko w przypadku, gdy pracownik wyrazi na to zgodę, o której mowa w art. 22 [2] § 1. Co oznacza, że adres e-mail oraz prywatny numer telefonu pobrany od kandydata do pracy pracodawca będzie mógł przetwarzać po jego zatrudnieniu tylko za zgodą tego pracownika.

Przepis art. 22 [2] Kodeksu pracy

W projekcie ustawy nowelizującej Kodeks pracy znajdują się aż trzy nowe artykuły – art. 22 [2]-22 [4].

Art. 22 [2] § 1 ma otrzymać następujące brzmienie:

„§ 1. Przetwarzanie przez pracodawcę innych danych osobowych niż wymienione w art. 22 [1] § 1 i 2 jest dopuszczalne tylko wtedy, gdy dotyczą one stosunku pracy i osoba ubiegająca się o zatrudnienie lub pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej”.

Oznacza to, że dane osobowe inne niż:

1) imię (imiona) i nazwisko;

2) data urodzenia;

3) adres do korespondencji;

4) adres poczty elektronicznej albo numer telefonu;

5) wykształcenie;

6) przebieg dotychczasowego zatrudnienia;

7) adres zamieszkania;

8) numer PESEL, a w przypadku jego braku – rodzaj i numer dokumentu potwierdzającego tożsamość;

9) dane osobowe pracownika, a także dane osobowe dzieci pracownika i innych członków jego najbliższej rodziny konieczne ze względu na korzystanie przez pracownika ze szczególnych uprawnień przewidzianych w prawie pracy,

będą mogły być przetwarzane przez pracodawcę tylko za zgodą pracownika wyrażoną w formie elektronicznej (np. podane w mailu z informacją o wyrażonej zgodzie na ich przetwarzanie) lub pisemnej.

Przepis art. 22 [2] Kodeksu pracy w § 2 reguluje kwestię danych biometrycznych, zgodnie z którym: „Przetwarzanie przez pracodawcę danych biometrycznych obejmuje tylko dane osobowe pracownika, jeśli dotyczą one stosunku pracy i pracownik wyrazi na to zgodę w oświadczeniu złożonym w postaci papierowej lub elektronicznej”.

Dane biometryczne nie mogą być pobierane od kandydata do pracy, nie ma bowiem ku temu żadnego argumentu pozwalającego na uzasadnienie takiego działania. Definicja danych biometrycznych jest zawarta w RODO w art. 4. Zgodnie z RODO, dane biometryczne to dane osobowe wynikające ze specjalnego przetwarzania technicznego, dotyczą cech

fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, taką jak wizerunek twarzy lub dane daktyloskopijne. Co do zasady, przetwarzanie takich danych będzie zabronione, jednakże RODO zawiera wyjątki od tej zasady, w tym m.in. wyraźną i dobrowolną zgodę podmiotu, którego dane dotyczą.

Możliwe będzie np. pobranie odcisku palca, który zastąpi często dziś stosowaną kartę magnetyczną uprawniającą do wejścia na teren zakładu pracy i który jednocześnie pozwoli na kontrolę czasu pracy. Będzie to możliwe, ale za zgodą pracownika. Zgoda ta nie może być dorozumiana – ma być wyrażona w formie pisemnej lub elektronicznej.

Przepis art. 22 [2] § 3 reguluje kwestię zgody pracownika na przetwarzanie innych danych osobowych niż wskazane w art. 22 [1] Kodeksu pracy oraz danych biometrycznych, wprowadzając normę ochronną:

„§ 3. Brak zgody, wskazanej w § 1 i 2, nie może być podstawą niekorzystnego traktowania osoby ubiegającej się o zatrudnienie lub pracownika, a także nie może powodować wobec nich jakichkolwiek negatywnych konsekwencji, zwłaszcza nie może stanowić przyczyny uzasadniającej odmowę zatrudnienia, wypowiedzenia stosunku pracy lub jego rozwiązania bez wypowiedzenia przez pracodawcę".

W art. 22 [2] § 4., wskazano, iż: „Przetwarzanie, o którym mowa w § 1 i 2, dotyczy danych osobowych udostępnianych na wniosek pracodawcy lub danych osobowych przekazanych pracodawcy z inicjatywy osoby ubiegającej się o zatrudnienie lub pracownika". Mając to na uwadze, dane osobowe pracownika mają być udostępniane na wniosek pracodawcy lub z inicjatywy osoby, której dotyczą. Nie mogą być pozyskane od osób trzecich.

Ustawodawca wprowadza również w art. 22 [2] § 5 katalog danych, które nie mogą być przetwarzane nawet za zgodą osoby, której dane dotyczą. Ich gromadzenie możliwe będzie więc wyłącznie w przypadkach, gdy jest to konieczne dla wypełnienia obowiązku wynikającego z przepisu prawa. Dotyczy to danych osobowych o nałogach, o stanie zdrowia, o życiu seksualnym lub orientacji seksualnej.

Ponadto jest konieczne zapewnienie szczególnych warunków technicznych gromadzenia danych biometrycznych, które zawierać będzie rozporządzenie wydane przez ministra właściwego do spraw informatyzacji.

Dlatego też minister właściwy do spraw informatyzacji określi, w drodze rozporządzenia, sposób gromadzenia danych biometrycznych, uwzględniając zapewnienie ochrony przetwarzanych danych biometrycznych odpowiedniej do zagrożeń. Stanowi o tym ostatni – 6 paragraf art. 22 [2].

Przepis art. 22 [3] Kodeksu pracy

Nowy art. 22 [3] przybrał następującą treść:

„§ 1 Pracodawca żąda podania danych osobowych:

1) innych niż określone w art. 22 [1] § 1 i 2,

2) wskazanych w art. 22 [2] § 2 i 5

− jeżeli obowiązek ich podania wynika z odrębnych przepisów lub gdy jest to niezbędne do wypełniania

obowiązku pracodawcy nałożonego przepisem prawa.

§ 2. Przetwarzanie danych osobowych, o których mowa w § 1, jest możliwe tylko w zakresie niezbędnym do realizacji tego obowiązku".

Chodzi np. o karalność kandydatów do pracy – będzie możliwe pozyskanie takich danych tylko wtedy, kiedy w stosunku do określonej grupy zawodowej pozwala na to odrębny przepis.

Przepis art. 22 [4] Kodeksu pracy

Treść art. 22 [4] Kodeksu pracy brzmi:

"§ 1. Dla zapewnienia bezpieczeństwa pracowników lub ochrony mienia lub zachowania w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, pracodawca podejmuje decyzję o wprowadzeniu szczególnego nadzoru nad miejscem pracy lub terenem wokół zakładu pracy w postaci środków technicznych umożliwiających rejestrację obrazu (monitoring), jeżeli uzna to za konieczne. Monitoring nie może stanowić środka kontroli wykonywania pracy przez pracownika.

§ 2. Monitoring nie obejmuje pomieszczeń, które nie są przeznaczone do wykonywania pracy, w szczególności pomieszczeń sanitarnych, szatni, stołówek lub palarni.

§ 3. Dane osobowe uzyskane w wyniku zastosowania monitoringu pracodawca przetwarza wyłącznie do celów, dla których zostały zebrane i przechowuje przez okres niezbędny dla realizacji tych celów.

§ 4. Pracodawca informuje pracowników o wprowadzeniu monitoringu, w sposób przyjęty u danego pracodawcy nie później niż 14 dni przed uruchomieniem monitoringu. Pracodawca przed dopuszczeniem pracownika do pracy informuje go o stosowaniu monitoringu."

Z powyższego wynika, że wystarczy spełnienie jednej przesłanki, tj.: bezpieczeństwo pracowników lub ochrona mienia lub zachowanie w tajemnicy informacji, których ujawnienie mogłoby narazić pracodawcę na szkodę, aby można było wprowadzić monitoring. Kwestie związane z monitoringiem należy unormować np. w regulaminie pracy. Pracownik musi wiedzieć o wprowadzeniu monitoringu z 14-dniowym wyprzedzeniem.

Nowa treść art. 229 Kodeksu pracy

Nowa treść otrzyma również art. 229, dotyczący badań lekarskich:

a) § 1 [1] pkt 2 otrzyma brzmienie:

„2) przyjmowane do pracy u innego pracodawcy na dane stanowisko w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, jeżeli posiadają aktualne orzeczenie lekarskie stwierdzające brak przeciwwskazań do pracy w warunkach pracy opisanych w skierowaniu na badania lekarskie i pracodawca ten stwierdzi, że warunki te odpowiadają warunkom występującym na danym stanowisku pracy, z wyłączeniem osób przyjmowanych do wykonywania prac szczególnie niebezpiecznych".

Obecnie pracownik ma przedstawić to orzeczenie lekarskie pracodawcy. Nastąpiła zmiana jednego wyrazu – czasownik „przedstawić" zamieniono na „posiadać".

Dalsze zmiany art. 229 Kodeksu pracy dają pracodawcy prawo do żądania aktualnych orzeczeń lekarskich od konkretnych kategorii pracowników oraz skierowań na badania będących podstawą wydania takiego orzeczenia i przechowywania ich.

b) po § 1[2] dodaje się § 1[3] w brzmieniu:

„§ 1[3]. Pracodawca żąda od osoby, o której mowa w § 1 [1] pkt 2 oraz w § 1 [2], aktualnego orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku oraz skierowania na badania będące podstawą wydania tego orzeczenia."

Zgodnie z tą zmianą pracodawca żąda od osoby przyjmowanej, w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, do pracy na dane stanowisko, a także od osoby, która aktualnie pozostaje w stosunku pracy z innym pracodawcą, orzeczenia lekarskiego stwierdzającego brak przeciwwskazań do pracy na danym stanowisku oraz skierowania na badania będące podstawą wydania tego orzeczenia.

c) § 7 otrzymuje brzmienie:

„§ 7. Pracodawca przechowuje orzeczenia wydane na podstawie badań lekarskich, o których mowa w § 1, 2 i 5, orzeczenia i skierowania uzyskane na podstawie § 1[3] oraz skierowania, o których mowa w § 4a."

Zmiana polega na dodaniu podstawy prawnej do przechowywania przez pracodawcę konkretnych skierowań i orzeczeń lekarskich. Pracodawca ma również podstawę prawną do przechowywani skierowań wystawionych przez niego na badania wstępne, okresowe i kontrolne.

d) po § 7 dodaje się § 7[1] w brzmieniu:

„§ 7[1]. W przypadku stwierdzenia, że warunki określone w skierowaniu, o którym mowa w § 1[3], nie odpowiadają warunkom występującym na danym stanowisku pracy, pracodawca zwraca osobie przyjmowanej do pracy to skierowanie oraz orzeczenie lekarskie wydane w wyniku tego skierowania."

A zatem pracodawca nie ma podstawy prawnej do przechowywania u siebie skierowania oraz orzeczenia lekarskiego od osoby przyjmowanej w ciągu 30 dni po rozwiązaniu lub wygaśnięciu poprzedniego stosunku pracy, do pracy na dane stanowisko, a także od osoby, która aktualnie pozostaje w stosunku pracy z innym pracodawcą, jeżeli nie odpowiadają one potrzebom pracodawcy na danym stanowisku pracy.

Rzetelna Grupa - firma świadcząca kompleksowe usługi doradcze w zakresie prawa gospodarczego, prawa spółek handlowych, prawa konsumenckiego, praw autorskich oraz ochrony danych osobowych. Specjalizuje się w obsłudze podmiotów z branży e-commerce, nowoczesnych technologii IT oraz prowadzących szeroko rozumianą działalność w Internecie. Rzetelną Grupę tworzą doświadczeni eksperci, radcy prawni, prawnicy oraz menedżerowie, którzy wspierają przedsiębiorców w prowadzeniu bezpiecznego e-biznesu, zgodnego z obowiązującymi przepisami prawa i najlepszymi praktykami.

Rzetelna Grupa posiada w swoim portfolio sześć marek - produktów, które precyzyjnie definiują świadczone przez firmę usługi.

Rzetelny Regulamin: platforma certyfikacji sklepów i serwisów internetowych. W ramach Rzetelnego Regulaminu spółka dostarcza przedsiębiorcom, prowadzącym działalność w Internecie, usługi związane z audytem e-sklepów i serwisów branżowych, opracowaniem dedykowanego regulaminu oraz opieką prawną pod kątem zgodności prowadzonego e-biznesu z przepisami prawa, spełnienia obowiązków informacyjnych oraz poszanowania praw konsumenta.

Polityka Bezpieczeństwa: usługa kierowana jest do wszystkich przedsiębiorców przetwarzających dane osobowe w firmie. Polega na opracowaniu dokumentu polityki bezpieczeństwa oraz wdrożeniu procedur przetwarzania i ochrony danych osobowych, zgodnie z aktualnie obowiązującymi przepisami prawa. Usługa gwarantuje pełną ochronę danych osobowych oraz bezpieczeństwo procesu ich przetwarzania. Eksperci Rzetelnej Grupy pomagają także w rejestracji zbioru danych osobowych w GIODO.

Rzetelny Prawnik: to usługa skierowana do małych i średnich przedsiębiorstw, którzy nie posiadają w swoich strukturach działów prawnych, ale potrzebują rzetelnych konsultacji i opinii prawnych na najwyższym poziomie. Usługi świadczone są na jasno określonych zasadach w ramach abonamentu, który precyzuje zakres doradztwa i jego koszt. Model usługi zapewnia przedsiębiorcy wsparcie dedykowanego doradcy, indywidualnie opracowywane umowy i dokumenty prawne, a także bezpieczeństwo finansowe.

Rzetelna Umowa: usługa skierowana zarówno do przedsiębiorców jak i konsumentów, czyli stron wszelkiego rodzaju umów, realizowana za pośrednictwem elektronicznej platformy. Platforma ta umożliwia zabezpieczenie treści i praw autorskich, prawne poświadczenie spełnienia 21 obowiązków informacyjnych oraz generowanie i automatyczne uzupełnianie dokumentów i umów. Każdy dokument poświadcza podpis elektroniczny uprawnionego reprezentanta Rzetelnej Grupy wraz ze znacznikiem czasu wskazującym kiedy został podpisany.

Prawo Konsumenckie: platforma poświęcona edukacji konsumentów i przedsiębiorców działających w sieci. Jest zbiorem aktualnie obowiązujących przepisów i ich interpretacji, dotyczących zakupów i sprzedaży w Internecie, praw konsumentów i obowiązków e-sprzedawcy. Za pośrednictwem platformy eksperci Rzetelnej Grupy dzielą się swoją wiedzą i doświadczeniem, publikują merytoryczne artykuły oraz nagrania audio/video z udziału w kluczowych audycjach radiowych i programach TV.

Rzetelny Konkurs: to kompleksowe doradztwo w zakresie organizacji i obsługi konkursów oraz loterii. Eksperci Rzetelnej Grupy wspierają przedsiębiorców na każdym etapie projektu, począwszy od pomysłu, przez zabezpieczenie prawne i techniczne konkursu oraz zabezpieczenie obsługi uczestników konkursu, na przyznaniu Certyfikatu Rzetelnego Konkursu kończąc. Certyfikat Rzetelnej Grupy podnosi w oczach uczestników wiarygodność organizatora i poczucie bezpieczeństwa.

Zapraszamy do kontaktu

Rzetelna Grupa sp. z o.o.
ul. Ludwika Krzywickiego 34, 02-078 Warszawa
tel.: 22 390 91 05, mail.: biuro@rzetelnagrupa.pl

Sąd Rejonowy dla m. st. Warszawy I XIII Wydział Gospodarczy KRS 0000284065
NIP: 524-261-19-51 REGON: 141022624 Kapitał zakładowy: 50.000 złotych.