KSP
LEGAL & TAX ADVICE

RODO – PRZEWODNIK PRAKTYCZNY

CZYLI DANE OSOBOWE PO NOWEMU

WSTĘP

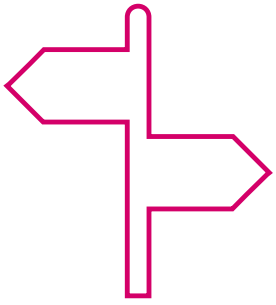
Przetwarzanie danych osobowych powinno odbywać się w granicach prawa. Dotychczas granice te wyznaczała polska ustawa z 29 sierpnia 1997 r. o ochronie danych osobowych. 25 maja 2018 r. zacznie obowiązywać **Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/41/WE (zwane RODO lub GDPR – General Data Protection Regulation).** Podmioty publiczne, organizacje oraz przedsiębiorcy ze wszystkich państw członkowskich Unii Europejskiej będą zobowiązani bezpośrednio stosować nowe regulacje.

Najistotniejszym i największym wyzwaniem, jakie RODO stawia przed podmiotami gromadzącymi dane osobowe jest przerzucenie ciężaru przeprowadzenia we własnym zakresie oceny, jakie środki skutecznie zapewnią właściwą ochronę przetwarzanych danych oraz bezpieczne ich usuwanie. Nowe przepisy nie dają bowiem gotowych rozwiązań. Mając na względzie, że naruszenie przepisów o ochronie danych osobowych skutkować może od 25 maja 2018 roku nałożeniem na przedsiębiorcę kary do 20 milionów euro lub 4% całkowitego rocznego światowego obrotu, warto już dziś podjąć działania w celu wdrożeniach nowych środków oraz narzędzi ochrony danych i odpowiednich procedur.

Życzymy Państwu przyjemnej lektury naszego przewodnika po RODO. Mamy nadzieję, że także dzięki niemu w sposób płynny uda się Państwu wejść w nowe realia prawne.

Zespół KSP

SPIS TREŚCI



CO TO JEST RODO I KOGO BĘDZIE DOTYCZYĆ?

RODO, czyli Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/41/WE stanowi jednolitą dla całej Unii Europejskiej regulację kwestii ochrony danych osobowych. Dla wyznaczenia zakresu stosowania jego przepisów kluczowe znaczenie będzie miało pojęcie danych osobowych.

Dane osobowe to informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej. Dane osobowe stanowić będą w szczególności informacje takie jak imię i nazwisko, numer identyfikacyjny (np. NIP, PESEL), dane o lokalizacji (np. adres zameldowania), identyfikator internetowy (np. adres IP, e-mail) lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość danej osoby. Ponadto pod pojęciem danych osobowych należy rozumieć wszystkie inne informacje dotyczące danej osoby, które przetwarzane są razem z danymi pozwalającymi na jej identyfikację.

Ochrona danych osobowych związana jest z ich przetwarzaniem. Nie każde działanie związane z wykorzystaniem danych osobowych stanowić będzie przetwarzanie danych osobowych w rozumieniu RODO. Opisane w niniejszym Przewodniku regulacje powinny być stosowane przez przedsiębiorców jeżeli:

- przetwarzają oni dane osobowe w sposób całkowicie lub częściowo zautomatyzowany lub
- jeżeli przetwarzanie dokonywane jest w zbiorach danych osobowych (czyli w uporządkowanych zestawach danych).

Doraźne skorzystanie z danych osobowych niemające zautomatyzowanego charakteru lub nieznajdujących się w uporządkowanym zbiorze, nie będzie stanowić przetwarzania danych osobowych w rozumieniu RODO.

Biorąc pod uwagę, że RODO stanowi część prawa Unii Europejskiej, zakresem jego zastosowania objęci będą wszyscy polscy oraz unijni przedsiębiorcy, niezależnie od tego, czy pełnią rolę administratora danych osobowych, czy działają na zlecenie administratora. Nowa regulacja wpłynie także na te procesy pozyskiwania, przetwarzania, wykorzystywania lub udostępniania danych osobowych, które wprawdzie mają miejsce poza UE, ale są związane z oferowaniem towarów i usług osobom przebywającym na terenie UE lub monitorowaniem zachowania mieszkańców Unii. Niniejszy przewodnik ma na celu przybliżenie ogólnych zasad wprowadzonych przez RODO dotyczących przedsiębiorców. Kwestie szczegółowe, w tym reguły dotyczące przetwarzania danych w sektorach o zwiększonej wrażliwości jak sektor bankowy, ubezpieczeniowy bądź medyczny, pozostają poza zakresem niniejszego opracowania.

Administrator danych osobowych to osoba fizyczna, osoba prawna, organ publiczny albo inna jednostka lub podmiot, który samodzielnie lub wspólnie z innymi podmiotami wyznacza cele i sposoby przetwarzania danych osobowych, a tym samym sprawuje władztwo nad przetwarzaniem danych osobowych. Co istotne, podmiot taki może przetwarzać dane osobowe samodzielnie lub przekazać je osobie trzeciej do przetwarzania w określonym przez niego celu i przy zastosowaniu wyznaczonego przez siebie sposobu przetwarzania danych.

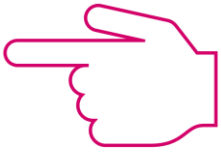
Podmiot przetwarzający dane osobowe to osoba fizyczna, prawna, organ publiczny albo inna jednostka lub podmiot, który dokonuje operacji na danych osobowych (przetwarzania danych) w imieniu administratora danych osobowych.

OD CZEGO ZACZĄĆ? ANALIZA RYZYKA W PRZETWARZANIU DANYCH OSOBOWYCH

W przeciwieństwie do obowiązującej ustawy o ochronie danych osobowych i jej przepisów wykonawczych, RODO nie wskazuje wprost jakie środki powinien podjąć administrator lub podmiot przetwarzający, aby skutecznie chronić dane osobowe. RODO wymaga od administratora i podmiotu przetwarzającego, aby wdrożone środki zabezpieczające dane były odpowiednie przy uwzględnieniu m.in. ryzyka naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia. Analiza tych ryzyk powinna stanowić punkt wyjścia dla ochrony danych osobowych u każdego administratora. **Analiza ryzyka** powinna identyfikować poszczególne zagrożenia wskazując dla każdego z nich prawdopodobieństwo wystąpienia i wagę zagrożenia. W oparciu o wyniki tej analizy, administrator dobierać będzie odpowiednie środki ochrony danych.

UWAGA

Oprócz podstawowej analizy ryzyka, niektórzy administratorzy będą zobowiązani do przeprowadzania dodatkowych pogłębionych analiz. Taka analiza nosi nazwę oceny skutków dla ochrony danych (Data Protection Impact Assessment). Jej przeprowadzenie będzie obowiązkowe przede wszystkim w przypadku, gdy z wstępnej analizy przeprowadzonej przez administratora wynikać będzie, że ryzyko naruszenia praw lub wolności osób fizycznych należy ocenić jako wysokie.



O CZYM PRZETWARZAJĄCY DANE MUSI PAMIĘTAĆ? – *PRIVACY BY DESIGN* I *PRIVACY BY DEFAULT*

RODO zmienia podejście do procedur przetwarzania danych osobowych, wprowadzając nowe zasady – ***privacy by design*** oraz ***privacy by default***. Administratorzy i podmioty przetwarzające dane będą musieli stosować nowe zasady systemowego podejścia do tworzenia usług, procesów i produktów (np. aplikacji), które nakazują uwzględnianie prywatności już na etapie projektowania (privacy by design) oraz tworzenie możliwości konfiguracji opcji prywatności przez osobę, której dane dotyczą. Prywatność w tych ustawieniach musi być stanem wyjściowym (privacy by default).

UWZGLĘDNIANIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA – *PRIVACY BY DESIGN*

Zgodnie z regułą *privacy by design*, administrator danych jest zobowiązany zapewnić, aby na etapie projektowania systemu, aplikacji lub procesu oraz na etapie wykorzystywania ich do przetwarzania danych wprowadzone zostały odpowiednie środki techniczne i organizacyjne, które zapewnią właściwą ochronę danych osobowych.

Najważniejszym elementem tej reguły jest nakaz stosowania się do reguł ochrony danych osobowych na etapie planowania, czy innymi słowy „przy określaniu sposobów przetwarzania".

UWAGA

Najprościej mówiąc ***privacy by design*** to obowiązek przewidywania i przeciwdziałania możliwym problemom w zakresie ochrony danych, zanim one powstaną, a nie dopiero, gdy staną się faktem.

Implementacja tej reguły powinna polegać przede wszystkim na wdrożeniu metodycznego podejścia do ochrony danych osobowych od etapu planowania (przykładowo przy projektowaniu, monitorowaniu, testach bezpieczeństwa, zmianach aplikacji czy nadawaniu uprawnień ich użytkownikom). Spełnienie tych wymogów powinno być także właściwie udokumentowane. Oznacza to, że stosowanie odpowiedniej metodologii – z punktu widzenia właściwego zabezpieczenia danych – powinno znaleźć wyraz w prowadzonej dokumentacji.

UWAGA

Do tej pory idea ***privacy by design*** nie była obowiązkiem wynikającym z ustawy. Nowa regulacja wymusza jej stosowanie na wszystkich podmiotach przetwarzających dane osobowe. W przypadku projektowania bądź opracowywania aplikacji, usług czy produktów jednym z najważniejszych aspektów stanie się ochrona danych osobowych na każdym etapie ich zbierania, przetwarzania czy usuwania.

Reguła *privacy by design* nie kończy się jednak na etapie tworzenia czy projektowania. W każdej fazie realizacji konieczna jest troska o ochronę danych osobowych oraz reagowanie na nowe, dające się przewidzieć zagrożenia. Regularne przeglądy systemów informatycznych, bieżąca aktualizacja regulaminów oraz cykliczna analiza zgodności zakresu przetwarzania danych z treścią poszczególnych zgód – tak kształtować się będą obowiązki administratorów danych osobowych pod rządami RODO.

DOMYŚLNA OCHRONA DANYCH – *PRIVACY BY DEFAULT*

Zasada ***privacy by default*** została określona w art. 25 ust. 2 RODO. Zgodnie z jej treścią administrator jest zobowiązany wdrożyć takie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania. Dotyczy to ilości zbieranych danych, zakresu przetwarzania, okresu ich przechowywania oraz sposobu udostępniania. Przedsięwzięte środki powinny więc zapewnić domyślność ustawień chroniących prywatność osób, których dane są przetwarzane. W myśl zasady *privacy by default*, udostępnienie bliżej nieokreślonej liczbie innych osób danych osobowych przez użytkownika aplikacji, systemu, programu czy usługi jest możliwe dopiero wtedy, gdy użytkownik podejmie w tym zakresie „interwencję", czyli np. zmieni domyślne ustawienia aplikacji.

PRYWATNOŚĆ OD SAMEGO POCZĄTKU

Stosowanie omawianych reguł może być przedmiotem kontroli ze strony organu ochrony danych osobowych, a w przypadku stwierdzenia naruszenia którejkolwiek z nich, organ ten uprawniony będzie do nałożenia kary finansowej.

UWAGA

Administrator danych może wykazać, że wywiązał się z obowiązków płynących z zasad *privacy by default* oraz *privacy by design* poprzez poddanie się mechanizmowi dobrowolnej certyfikacji, którą ustanawia RODO. W Polsce certyfikacji ma dokonywać Prezes Urzędu Ochrony Danych Osobowych.

KIEDY MOŻNA PRZETWARZAĆ DANE I JAK SKUTECZNIE UZYSKAĆ ZGODĘ NA ICH PRZETWARZANIE?

Obowiązująca obecnie ustawa o ochronie danych osobowych stanowi, że przetwarzanie danych jest dopuszczalne tylko wtedy, gdy osoba, której dane dotyczą, wyrazi na to zgodę, chyba że chodzi o usunięcie jej danych, względnie gdy zachodzą inne wymienione przesłanki (np. jest to niezbędne dla zrealizowania uprawnienia lub spełnienia obowiązku wynikającego z przepisu prawa, dane przetwarzane są w celu wykonania umowy, której stroną jest osoba udostępniająca swoje dane, czy w sytuacji, gdy dane przetwarzane są dla dobra publicznego).

W przypadku braku szczególnych przesłanek, przetwarzanie danych wymaga zatem zgody osoby, której dotyczy. Zasada ta została utrzymana na gruncie RODO.

KIEDY NALEŻY UZYSKAĆ ZGODĘ NA PRZETWARZANIE DANYCH

W dotychczasowym systemie prawnym brak było jednoznacznego określenia momentu, w którym przedsiębiorca powinien uzyskać zgodę osoby zainteresowanej na przetwarzanie jej danych osobowych. Bardzo często zgoda była uzyskiwana po przystąpieniu do przetwarzania danych osobowych. RODO nie pozostawia już wątpliwości – **zgoda na przetwarzanie danych ma mieć charakter uprzedni względem samego przetwarzania**. Innymi słowy, należy ją uzyskać zanim przedsiębiorca przystąpi do wykonywania operacji na cudzych danych osobowych, tj. już przed rozpoczęciem ich gromadzenia.

TREŚĆ ZGODY

Wyrażenie zgody na przetwarzanie danych osobowych następuje zwykle poprzez podpisanie lub zaakceptowanie w inny sposób klauzuli zgody. Klauzula ta, zgodnie z RODO, powinna zostać sformułowana jasnym, prostym i zrozumiałym językiem, a w jej treści powinny zostać uwzględnione elementy wskazane poniżej. Klauzula zgody na przetwarzanie danych osobowych powinna wskazywać:

1. jakie dane osobowe będą przetwarzane przez przedsiębiorcę,
2. w jakich konkretnie celach będą one przetwarzane,
3. jakie operacje będą na nich wykonywane (właściciel danych powinien mieć możliwość wyrażenia bądź niewyrażenia zgody na każdą operację przetwarzania danych z osobna),
4. kto będzie administratorem danych osobowych (nazwa i dane kontaktowe).

SPOSÓB WYRAŻENIA ZGODY

RODO nie narzuca formy, w jakiej powinna zostać wyrażona zgoda na przetwarzanie danych osobowych. Może ona przybrać formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia woli. Wyrażenie zgody może również polegać na zaznaczeniu okienka wyboru podczas przeglądania strony internetowej, na wyborze ustawień technicznych do korzystania z usług społeczeństwa informacyjnego (np. portale społecznościowe) lub też na innym oświadczeniu bądź zachowaniu, które w danym kontekście jasno wskazuje, że osoba udostępniająca swoje dane zaakceptowała proponowany sposób ich przetwarzania.

Nie uznaje się za wyrażenie zgody na przetwarzanie danych milczenia osoby, której dane dotyczą, czy też braku jej aktywności. Zakazane jest również domyślne (automatyczne) zaznaczanie przez administratorów na stronach internetowych pól z wyrażeniem zgody na przetwarzanie danych. Dotychczas proceder ten był dosyć powszechny i nadal można spotkać się z nim na niektórych portalach internetowych.

UWAGA

Mając na względzie, że administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych, najbezpieczniejszą formą zgody będą rozwiązania pozwalające na archiwizowanie złożonych oświadczeń. W tym zakresie zdecydowaną przewagę – ze względu na ułatwienia dowodowe – ma tradycyjna forma pisemna lub forma elektroniczna.

ZAKAZ NAKŁANIANIA DO WYRAŻENIA ZGODY

Dążąc do uzyskania zgody na przetwarzanie danych osobowych, nie można stosować żadnych form nacisku na właściciela danych. W przeciwnym razie nie zostanie spełniona przesłanka dobrowolności jej wyrażenia. Oceniając, czy zgodę wyrażono dobrowolnie, bierze się pod uwagę przede wszystkim, czy od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi. Zakaz ten nie dotyczy jednak sytuacji, gdy dane są niezbędne do wykonania tejże umowy/usługi (w tym przypadku wyrażenie zgody na przetwarzanie danych osobowych nie jest konieczne).

PRAWO DO COFNIĘCIA ZGODY

Osoba, której dane dotyczą, powinna mieć prawo do wycofania zgody na ich przetwarzanie w dowolnym momencie, o czym należy ją poinformować.

Uwaga! **Cofnięcie zgody musi być równie łatwe jak jej wyrażenie.**

Najprościej, gdy cofnięcie zgody będzie następowało na podstawie oświadczenia osoby, której dane dotyczą, złożonego w takie samej formie, w jakiej została wyrażona zgoda na przetwarzanie.

LISTA ZADAŃ

Co zatem zrobić, żeby uczynić zadość stawianym przez RODO wymaganiom dotyczącym zgody na przetwarzanie danych osobowych?

- Uzyskaj zgodę na przetwarzanie danych osobowych od osób, których dane będziesz przetwarzać (lub upewnij się co do braku obowiązku pozyskiwania takiej zgody);
- Sformułuj klauzulę zgody prostym i zrozumiałym językiem;
- Dokładnie wskaż dane administratora danych osobowych, oznacz jakie dane osobowe oraz w jakim celu lub celach będą przetwarzane;
- Określ operacje, jakie będą wykonywane na danych osobowych oraz sformułuj zgodę w taki sposób, by osoba zainteresowana mogła wyrazić zgodę na każdą z nich;
- Nie uzależniaj zawarcia umowy od wyrażenia zgody na przetwarzanie danych, jeżeli zgoda taka nie jest niezbędna do jej wykonania, ani też nie nakłaniaj do wyrażenia zgody w inny sposób, który może skutkować wątpliwościami co do dobrowolności jej wyrażenia;
- Poinformuj osobę, której dane planujesz przetwarzać o przysługującym jej prawie do cofnięcia zgody, wskazując jednocześnie, w jaki sposób z niego skorzystać;
- Przechowuj uzyskane oświadczenia.

INSPEKTOR OCHRONY DANYCH OSOBOWYCH – CZY MUSI BYĆ W MOJEJ FIRMIE?

RODO wprowadza nową funkcję w przedsiębiorstwie – Inspektora ochrony danych osobowych. Zastąpi on ABI (Administratora Bezpieczeństwa Informacji), a jego rolą będzie nadzorowanie przestrzegania przepisów w zakresie ochrony danych osobowych i współpraca z organem nadzorczym, którym ma być Prezes Urzędu Ochrony Danych Osobowych.

UWAGA

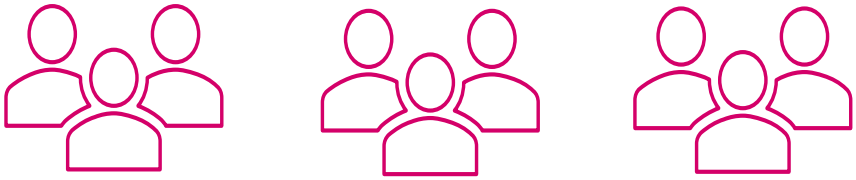
Ustanowienie inspektora ochrony danych osobowych będzie obowiązkowe nie tylko u administratorów danych (podmiotów decydujących o celach i środkach przetwarzania danych), ale także u podmiotów, którym powierzono przetwarzanie danych. Jednak nie zawsze.

UWAGA

Przypadki obligatoryjnego powołania **Inspektora ochrony danych osobowych:**

1. Gdy przetwarzanie danych dokonywane będzie przez podmiot publiczny, za wyjątkiem sądów w zakresie sprawowania przez nie wymiaru sprawiedliwości;
2. Gdy główna działalność administratora danych lub podmiotu przetwarzającego polegać będzie na operacjach przetwarzania, które wymagają regularnego i systematycznego monitorowania osób, których dane dotyczą, na dużą skalę;
3. Gdy główna działalność administratora danych lub podmiotu, któremu powierzono przetwarzanie polega na przetwarzaniu na dużą skalę szczególnych kategorii danych (danych wrażliwych).

Spośród ustanowionych przez RODO przesłanek powołania inspektora dla przedsiębiorców istotna będzie ocena wypełnienia przesłanki 2 lub 3.



PRZETWARZANIE DANYCH NA DUŻĄ SKALĘ, CZYLI JAK?

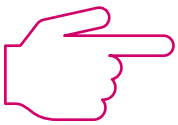
Obowiązek powołania inspektora ochrony danych przez podmioty prywatne dotyczyć będzie tylko podmiotów, których główna działalność polega na przetwarzaniu danych na dużą skalę. Przede wszystkim należy sprawdzić, czy administrator danych lub podmiot przetwarzający spełniają następujące przesłanki:

1. Główna działalność podmiotu polega na przetwarzaniu danych.
   Główna działalność oznacza takie czynności, które polegają na bezpośredniej realizacji celów gospodarczych danej organizacji.

PRZYKŁAD:
zatrudnianie pracowników nie jest zazwyczaj celem biznesowym przedsiębiorcy, tylko niezbędnym działaniem dla realizacji podstawowej działalności: produkcji, handlu, świadczenia usług etc. W związku z tym niezależnie od ilości pracowników, samo przetwarzanie ich danych osobowych związanych z zatrudnieniem nie będzie wywoływało obowiązku powołania inspektora danych.

Jeżeli jednak główna działalność podmiotu jest nieodłącznie związana z przetwarzaniem danych osobowych, jak ma to miejsce np. w wypadku świadczenia opieki zdrowotnej na rzecz pacjentów lub agencji pośredniczącej w zatrudnianiu pracowników, to wtedy podstawowa przesłanka dla obowiązku powołania inspektora ochrony danych osobowych będzie spełniona.

2. Przetwarzanie danych dokonywane jest na dużą skalę.
   Obecnie brak jest wytycznych wskazujących konkretne liczby, które mogłyby jednoznacznie określać, kiedy następuje przetwarzanie na dużą skalę.



PRZYKŁAD:
przetwarzanie danych osób ubezpieczonych dokonywane przez towarzystwo ubezpieczeniowe będzie działaniem na dużą skalę, podczas gdy operowanie na danych osobowych tych samych kategorii osób przez samodzielnego agenta ubezpieczeniowego raczej takim przetwarzaniem nie będzie. Przetwarzanie danych przez szpital, będzie przetwarzaniem na dużą skalę, podczas gdy przetwarzanie ich przez lekarza prowadzącego indywidualną praktykę, może nie kwalifikować się do tej kategorii.

Jeżeli przesłanki wymienione powyżej są spełnione łącznie, dla powstania obowiązku ustanowienia inspektora ochrony danych konieczne będzie dodatkowo wystąpienie jednej z dwóch poniższych okoliczności:

3. Operacje przetwarzania danych wymagają regularnego i systematycznego monitorowania osób, których te dane dotyczą.
   Monitorowanie osób występować będzie w szczególności w środowisku internetowym (aplikacje mobilne, usługi lokalizacyjne, rozwiązania typu smart), ale nie jest to pojęcie ograniczone wyłącznie do tej sfery, przesłanka ta będzie spełniona wszędzie tam, gdzie w sposób zorganizowany i stały obserwowane jest zachowanie osób fizycznych, co ma także miejsce w przypadku m.in. usług bankowych, telekomunikacyjnych, leczniczych, ubezpieczeniowych, programów lojalnościowych itd.

ALBO

4. Przetwarzanie danych następuje na dużą skalę i dotyczy danych wrażliwych.
   Chodzi tu o dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej, dane dotyczące zdrowia, seksualności lub orientacji seksualnej, a także dane dotyczące wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa.

UWAGA

W razie łącznego zaistnienia przesłanek wskazanych w pkt 1 i 2, a także przesłanki objętej pkt 3 albo 4, przedsiębiorca lub inny podmiot niebędący organem administracji będzie miał obowiązek powołania inspektora ochrony danych osobowych.

KWALIFIKACJE I ZADANIA INSPEKTORA OCHRONY DANYCH OSOBOWYCH

Inspektor ochrony danych osobowych powinien zostać wyznaczony na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań mu przypisanych. RODO nie precyzuje formalnych wymagań w zakresie wykształcenia lub posiadanych dyplomów, bądź uprawnień, które inspektor powinien spełniać. Ocena, czy dana osoba nadaje się do pełnienia tej funkcji należeć będzie do podmiotu, u którego inspektor będzie działał.

Zadania inspektora danych osobowych:

1. Informowanie administratora, podmiotu przetwarzającego oraz pracowników o ich obowiązkach i doradzanie im;
2. Monitorowanie przestrzegania ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia oraz audyty;
3. Udzielanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie wykonania oceny;
4. Współpraca z organem nadzorczym;
5. Pełnienie funkcji punktu kontaktowego.

JAKIE UPRAWNIENIA PRZYSŁUGIWAĆ BĘDĄ OSOBIE FIZYCZNEJ?

Przepisy RODO kładą mocny nacisk na prawa osób, których dotyczy przetwarzanie, choć istnienie wielu z opisanych w nim uprawnień nie jest niczym nowym.

EWOLUCJA ISTNIEJĄCYCH UPRAWNIEŃ

Każdej osobie fizycznej na mocy ustawy o ochronie danych osobowych przysługuje obecnie:

1. prawo dostępu do danych zgromadzonych przez przedsiębiorcę,
2. prawo do sprostowania danych,
3. prawo do uzupełnienia danych,
4. prawo do usunięcia danych.

Istniejące uprawnienia zostały doprecyzowane przez RODO.

Od maja 2018 roku każdy z nas będzie mógł zażądać dostarczenia mu kopii danych przetwarzanych przez przedsiębiorcę, a jeśli będzie to kopia elektroniczna to musi zostać dostarczona w powszechnie używanym formacie (np. PDF). Dzięki temu każda osoba fizyczna, każdy konsument będzie mógł sprawować bezpośrednią kontrolę nad zakresem danych, jakie udostępnił. Będzie można żądać usunięcia całości lub części danych, np. numeru telefonu. Ponadto osoby fizyczne zawsze mogą zażądać wskazania wszystkich podmiotów, którym dane zostały przekazane, a przedsiębiorca musi takiej informacji udzielić.

Istotnym uprawnieniem jest również to, że w przypadku zgłoszenia przez osoby fizyczne żądania sprostowania lub uzupełnienia danych, przedsiębiorca, który je przetwarza ma obowiązek niezwłocznego powiadomienia o żądaniu wszystkich innych podmiotów, którym dane zostały przekazane.

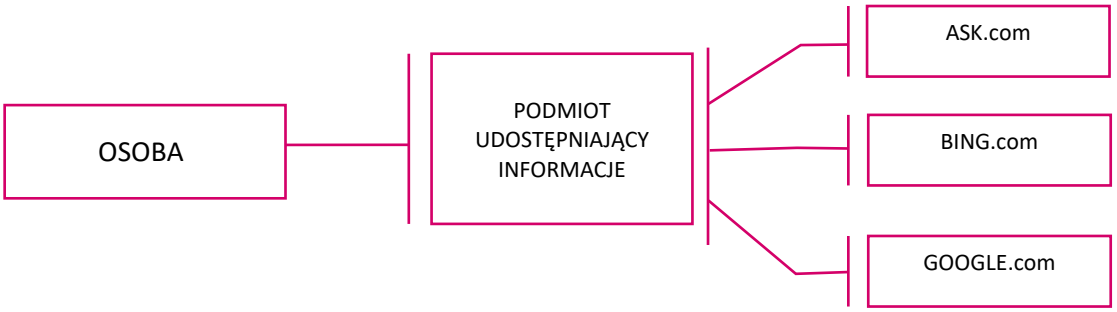
NOWE UPRAWNIENIE: PRAWO DO PRZENIESIENIA DANYCH

Każda osoba fizyczna będzie mogła zażądać przekazania danych, które jej dotyczą i są przetwarzane w sposób zautomatyzowany oraz nie ma przeszkód technicznych do ich przekazania. Uprawnienie do żądania przeniesienia danych będzie dotyczyć zarówno zwykłego skopiowania danych i przesłania ich do wskazanego podmiotu, jak i żądania usunięcia danych po ich przesłaniu do wskazanego administratora. Trudno w chwili obecnej stwierdzić, czy przeszkody techniczne, o jakich mowa w RODO będą oceniane obiektywnie, czyli przez pryzmat ogólnie dostępnych na rynku technologii, czy też subiektywnie, a więc na podstawie technologii będącej w posiadaniu przedsiębiorcy.

NOWE UPRAWNENIE: PRAWO DO BYCIA ZAPOMNIANYM

RODO przewiduje tzw. prawo do bycia zapomnianym, które polega na żądaniu usunięcia danych osobowych ze wszystkich rejestrów podmiotu, który dane zgromadził.

Najlepszą ilustracją obrazującą, na czym polega prawo do bycia zapomnianym jest żądanie usunięcia danych w wyszukiwarkach internetowych, które będzie można zgłosić do podmiotu, który w Internecie (na swojej witrynie internetowej) opublikował informację nas dotyczącą. Podmiot ten ma obowiązek nie tylko dane usunąć, ale także poinformować o tym wszystkie wyszukiwarki internetowe tak, aby dana informacja już się w nich nie pojawiała.



NOWE UPRAWNIENIE: PRAWO DO SĄDU I ODSZKODOWANIA

Obecnie obowiązująca ustawa o ochronie danych osobowych nie przewiduje odrębnej podstawy do żądania odszkodowania za naruszenie ochrony danych osobowych, a wszystkie procesy w tym zakresie oparte są na zasadach ogólnych wynikających z polskiego Kodeksu cywilnego. RODO wprowadza nie tylko procedurę ochrony prawnej przed sądem za naruszenie naszych praw, ale także prawo do wniesienia skargi na administratora danych do krajowego organu ochrony danych osobowych, który będzie miał 3 miesiące na poinformowanie o postępach w sprawie lub jej rozstrzygnięciu.

Osoba pokrzywdzona będzie miała także prawo do odszkodowania za szkodę majątkową lub niemajątkową powstałą w wyniku naruszenia przepisów przez administratora i podmiot przetwarzający jej dane osobowe.

UWAGA

W celu uwolnienia się od odpowiedzialności odszkodowawczej administrator danych lub podmiot przetwarzający dane musiałby wykazać, że nie ponosi w żadnym stopniu winy za zdarzenie, które doprowadziło do powstania szkody.

JAKIE OBOWIĄZKI INFORMACYJNE DOTYCZĄ PRZEDSIĘBIORCÓW?

Podstawowym celem RODO jest wzrost świadomości osób, które udostępniają swoje dane osobowe na temat celu, procesu i ryzyka związanego z przetwarzaniem danych. Firmy będą więc musiały opracować nowe sposoby komunikacji z klientami oraz pracownikami, aby byli świadomi, że ich dane osobowe są właściwie chronione.

ZAKRES OBOWIĄZKÓW INFORMACYJNYCH ADMINISTRATORA

Wypełnienie przez administratora obowiązków informacyjnych jest warunkiem legalnego przetwarzania danych osobowych. Dlatego wymagane informacje należy przekazać osobie zainteresowanej w momencie zbierania jej danych osobowych.

UWAGA

Informacje wymagane przez RODO należy przekazać w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą tego zażąda, informacji można udzielić również ustnie, o ile innymi sposobami potwierdzi się jej tożsamość. Przetwarzający dane musi być w stanie wykazać, że uczynił zadość obowiązkom informacyjnym.

WYJĄTKI

Administrator jest zwolniony z obowiązków informacyjnych, gdy osoba, której dane dotyczą, dysponuje już wszystkimi wymaganymi przez prawo informacjami, jakie administrator powinien jej przekazać. Ponadto, administrator nie musi wypełniać obowiązku informacyjnego, w przypadku pozyskiwania danych z innego źródła niż od osoby, której te dane dotyczą, gdy:

- Ich udzielenie jest niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku;
- Pozyskiwanie lub ujawnianie danych jest wyraźnie uregulowane i zabezpieczone prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator;
- Dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej.

UPRAWNIENIA KONTROLNE

Jak dotąd GIODO stosunkowo rzadko badał, czy i w jakim zakresie administratorzy danych osobowych przekazują zainteresowanym wymagane informacje. Biorąc jednak pod uwagę szerokie kompetencje przyznane przez RODO organom nadzorczym w zakresie weryfikacji prawidłowości procesów przetwarzania danych osobowych, w tym prawo do nakładania kar finansowych, a także nacisk, jaki Rozporządzenie kładzie na prawa osób, których dane są przetwarzane, należy spodziewać się wzrostu intensywności prowadzonych kontroli w tym zakresie. Kontrole te będą prowadzone przez Prezesa Urzędu Ochrony Danych Osobowych, który ma zastąpić GIODO.

LISTA ZADAŃ

Administrator danych osobowych, który wdrożył już w swojej firmie rozwiązania pozwalające na sprawne przekazywanie informacji wymaganych przez obowiązującą ustawę o ochronie danych osobowych, musi teraz dostosować je do wymagań stawianych przez RODO. W tym celu powinien:

1. Ustalić, czy dotychczas właściciele danych osobowych byli informowani, że ich dane osobowe są przetwarzanie, a także jakie informacje zostały im przekazane;
2. Zweryfikować, w jakiej formie oraz w jakim momencie zostały przekazane wymagane informacje osobom zainteresowanym, w szczególności, czy to były gotowe klauzule informacyjne;
3. Rozszerzyć treść klauzul informacyjnych o dodatkowe informacje wymagane przez RODO, a jeżeli dotąd ich nie uwzględniały, opracować gotowy formularz zawierający informacje o:

a) Nazwie, adresie i danych kontaktowych administratora;
b) Celu, w jakim dane osobowe są przetwarzane;
c) Przewidywanych odbiorcach lub kategoriach odbiorców danych;
d) Prawie dostępu do treści danych oraz prawie do ich poprawiania przez osobę, której dane dotyczą;
e) Dobrowolności albo obowiązku podania danych, w tym podstawie prawnej, z której taki obowiązek wynika;
f) Danych kontaktowych inspektora ochrony danych, jeżeli został powołany w firmie;
g) Podstawie prawnej przetwarzania danych osobowych;
h) Prawnych interesach administratora uzasadniających przetwarzanie danych;
i) Zamiarze przekazania danych osobowych do państwa trzeciego (tj. poza terytorium UE) oraz warunkach bezpieczeństwa przekazywanych danych;
j) Okresie, przez jaki dane będą docelowo przechowywane lub kryteriach ustalania tego okresu;
k) Wszystkich prawach przysługujących właścicielowi danych osobowych;
l) Wymogach ustawowych lub umownych podania danych osobowych, a także czy ich podanie jest warunkiem zawarcia umowy, czy dana osoba jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
m) Zautomatyzowanym podejmowaniu decyzji, w tym profilowaniu, zasadach ich podejmowania, a także znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą;
n) Źródle pochodzenia danych, a także prawie do skierowania żądania zaprzestania przetwarzania danych lub prawie do wniesienia sprzeciwu wobec przetwarzania danych w celach marketingowych lub wobec przekazywania danych osobowych innemu administratorowi (jeżeli dane osobowe nie zostały pozyskane od osoby, której one dotyczą, np. zakup bazy danych od podmiotu trzeciego);

4. Przestrzegać terminów przekazywania informacji osobom, których dane są przetwarzane.

JAK POWIERZYĆ PRZETWARZANIE DANYCH OSOBOWYCH?

Niektóre firmy przetwarzają ogromne ilości danych osobowych wykonując usługi dla swoich kontrahentów. Są to na przykład firmy prowadzące obsługę kadrowo-księgową przedsiębiorstw, czy zakłady realizujące usługi użyteczności publicznej wobec mieszkańców. Takie podmioty nazywa się podmiotami przetwarzającym lub procesorami. Ciążą na nich określone prawem obowiązki: muszą odpowiednio zabezpieczyć przetwarzane dane, prowadzić dokumentację i posiadać właściwe systemy informatyczne w celu przetwarzania danych.

OBOWIĄZKI ZWIĄZANE Z POWIERZENIEM PRZETWARZANIA DANYCH

UWAGA

Administrator będzie miał obowiązek korzystania wyłącznie z usług takich procesorów, którzy będą zapewniać wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.

Pod rządami RODO Administrator będzie musiał wykazać, że wybierając podmiot, któremu powierzył przetwarzanie danych, opierał się na konkretnych gwarancjach zastosowania prawidłowych środków bezpieczeństwa.

Takie ukształtowanie wymogów dotyczących powierzenia przetwarzania sprawia, że istotne znaczenie będą miały w przyszłości certyfikaty i znaki jakości przyznawane podmiotom przetwarzającym. Art. 42 RODO przewiduje ustanawianie przez państwa członkowskie i instytucje nadzorujące mechanizmów certyfikacji oraz znaków jakości. Oznaczenia te mają mieć charakter dobrowolny. Zgodnie z aktualnym projektem ustawy o ochronie danych osobowych certyfikacji dokonywać ma Prezes Urzędu Ochrony Danych Osobowych. Podmioty, którym zostanie udzielona certyfikacja zostaną ujęte w publicznie dostępnym wykazie, który - zgodnie z obecnymi założeniami - ma prowadzić Prezes UODO.

UMOWA POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Powierzenie przetwarzania danych przez administratora innemu podmiotowi powinno być formalnie uregulowane między stronami. Może ono mieć formę osobnej umowy powierzenia przetwarzania danych lub klauzul dotyczących powierzenia zamieszczanych w ramach szerszego kontraktu.

Zapisy o powierzeniu przetwarzania danych osobowych powinny określać obowiązkowo: przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, a także obowiązki i prawa administratora.

Na uwagę zasługuje także konieczność wprowadzenia do treści umowy szeregu obowiązków po stronie podmiotu przetwarzającego, np. opracowania środków umożliwiających mu udzielenie pomocy administratorowi w wykonywaniu obowiązku odpowiadania na żądania osób, których dane dotyczą albo obowiązku współpracy z organem nadzorczym. Procesor będzie także zobowiązany do poddania się audytowi ze strony administratora.

CZY PRZEDSIĘBIORCY BĘDĄ MUSIELI DOKONYWAĆ ZGŁOSZEŃ DO URZĘDU OCHRONY DANYCH OSOBOWYCH?

Konieczność rejestracji zbiorów danych osobowych stanowiła dotychczas najbardziej uciążliwy obowiązek związany z ochroną danych osobowych. Nawet Generalny Inspektor Ochrony Danych Osobowych wyrażał wątpliwości, co do sensu ich rejestrowania i nazywał go nadmierną biurokracją. Od maja 2018 r. nie będzie już obowiązku rejestrowania zbiorów danych osobowych. RODO we właściwy sposób przywiązuje wagę już nie do samych zbiorów danych osobowych, ale do procesów zbierania danych, ich przetwarzania oraz przekazywania innym podmiotom.

ZAWIADOMIENIE O NARUSZENIU OCHRONY DANYCH

Notyfikacja naruszeń w ochronie danych osobowych będzie nowym obowiązkiem każdego administratora danych.

UWAGA

W przypadku naruszenia ochrony danych osobowych administrator bez zbędnej zwłoki, ale najpóźniej w ciągu 72 godzin od stwierdzenia naruszenia, notyfikuje organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) fakt naruszenia. Nie trzeba będzie zgłaszać każdego incydentu, a jedynie takie, których efektem jest naruszenie bezpieczeństwa danych.

Zgłoszenie naruszenia będzie musiało zawierać określone informacje, tj.:

- Opis charakteru naruszenia, w tym – o ile jest to możliwe – wskazanie kategorii i przybliżonej liczby osób, których dane dotyczą;
- Imię i nazwisko oraz dane kontaktowe inspektora ochrony danych (jeśli został powołany);
- Opis możliwych konsekwencji naruszenia ochrony danych osobowych;
- Opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu oraz minimalizowaniu negatywnych jego skutków.

RODO przewiduje także, że w przypadku, gdy poszczególne naruszenie skutkuje niewielkim prawdopodobieństwem zaistnienia ryzyka naruszenia praw lub wolności osób fizycznych, nie ma potrzeby jego zgłaszania.

OCENA SKUTKÓW DLA OCHRONY DANYCH

Tzw. ocena skutków to nowa procedura, która polega na dokonaniu przez administratora kompleksowej oceny jego zamierzenia (przedsięwzięcia) pod kątem ochrony danych osobowych oraz obowiązków wynikających z RODO.

Do niezbędnych elementów takiej oceny należą:

- Systematyczny opis planowanych operacji przetwarzania i celów tego przetwarzania, w tym opis prawnie uzasadnionych interesów administratora w przetwarzaniu danych osobowych;
- Analiza prowadzonych operacji przetwarzania – czy stosowane działania są niezbędne oraz proporcjonalne do celów przetwarzania danych osobowych;
- Ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
- Opis środków planowanych w celu zaradzenia ryzyku, w tym mających zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO.

Wnioski wynikające z oceny skutków należy stosować w praktyce, podjęcie konkretnych działań określonych w wynikach oceny pomoże wykazać, że przedsiębiorca działa zgodnie z przepisami RODO.

UPRZEDNIE KONSULTACJE

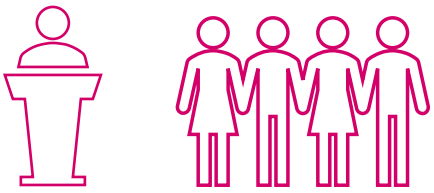
W przypadku, gdy w oparciu o ocenę skutków, poziom ryzyka naruszenia praw lub wolności osób, których dotyczą przetwarzane dane, oceniono jako wysoki, administrator ma obowiązek przeprowadzenia procedury tzw. uprzednich konsultacji z organem nadzorczym (Prezesem Urzędu Ochrony Danych Osobowych).

UWAGA

Procedura uprzednich konsultacji polegać będzie na:

- Określeniu obowiązków administratora, współadministratorów oraz podmiotów przetwarzających, w szczególności w ramach grup kapitałowych;
- Wskazaniu celów i sposobów zamierzonego przetwarzania danych osobowych;
- Określeniu, jakie środki i zabezpieczenia zostaną zastosowane w celu ochrony praw i wolności osób, których dane dotyczą;
- Podaniu danych kontaktowych inspektora ochrony danych;
- Ocenie skutków dla ochrony danych (impact assessment);

a następnie przekazaniu informacji w powyższym zakresie organowi nadzorczemu.



JAK PRZESYŁAĆ DANE OSOBOWE ZA GRANICĘ?

Warunki transferu danych osobowych za granicę są różne w zależności od tego, do jakiego kraju administrator planuje przekazać dane. Co do zasady, przesyłanie danych poza Unię Europejską będzie możliwie, jeżeli dany kraj zapewnia odpowiedni poziom ochrony danych.

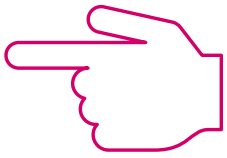
TRANSFER DANYCH OSOBOWYCH W RAMACH UNII EUROPEJSKIEJ

W przypadku udostępnienia danych w ramach UE, RODO przewiduje ich swobodny przepływ z zastrzeżeniem spełnienia przez administratora ogólnych wymogów związanych z przetwarzaniem danych. W szczególności w takim wypadku administrator powinien:

- Dysponować podstawą upoważniającą go do przesłania danych do innego podmiotu (np. zgodą osoby, której dane planuje udostępnić zagranicę);
- Dopełnić względem właściciela danych osobowych obowiązków informacyjnych;
- Wdrożyć odpowiednie środki techniczne i organizacyjne w celu zapewnienia bezpieczeństwa przesyłanych danych, np. przesyłać dane osobowe w postaci zaszyfrowanych plików.

UWAGA

W przypadku transferu danych osobowych pomiędzy podmiotami mającymi swoje siedziby w państwach UE (np. pomiędzy spółką polską a spółką niemiecką), transfer powinien odbywać się na takich samych warunkach, jak w przypadku przesyłania danych pomiędzy dwiema spółkami mającymi siedzibę na terytorium Polski.



TRANSFER DANYCH OSOBOWYCH POZA UNIĘ EUROPEJSKĄ

Podobne działania będą musiały zostać podjęte przez administratora w przypadku transferu danych osobowych poza terytorium Unii. Jednakże RODO wprowadza dodatkowe obostrzenia, którym administrator musi uczynić zadość, by uznać transfer danych za bezpieczny i legalny.

Przekazanie danych osobowych do państwa trzeciego będzie możliwe, gdy państwo, do którego dane mają zostać wysłane zapewnia adekwatny poziom ochrony danych osobowych. Jest on oceniany z uwzględnieniem wszystkich okoliczności dotyczących operacji przekazania danych, a także stosowanych w tym państwie środków bezpieczeństwa. O tym, czy dane państwo zapewnia odpowiedni poziom bezpieczeństwa danych obywateli UE decyduje bowiem Komisja Europejska

wydając stosowne decyzje (tzw. decyzje w sprawie adekwatności).

Przykładowo, krajami zapewniającymi adekwatny poziom bezpieczeństwa danych są Argentyna, Szwajcaria, Nowa Zelandia, czy Wyspy Owcze, a nie jest Japonia czy Stany Zjednoczone.

Co jednak w sytuacji, gdy w odniesieniu do kraju, w którym siedzibę ma podmiot, któremu polski administrator danych chce udostępnić dane, nie została wydana decyzja w przedmiocie adekwatności? Wówczas administrator będzie mógł przesłać dane osobowe poza Unię, jeżeli sam zapewni odpowiedni poziom ich zabezpieczenia.

Rozwiązania dla transferu danych osobowych do kraju bez wydanej decyzji o adekwatności:

- Wdrożenie wiążących reguł korporacyjnych, lub
- Wprowadzenie do umowy, na podstawie której następuje przekazanie danych osobowych, standardowych klauzul ochrony danych, lub
- Poddanie się procedurze certyfikacji.

SZCZEGÓLNE SYTUACJE WYSYŁANIA DANYCH OSOBOWYCH POZA UE

W niektórych przypadkach administrator będzie uprawniony do wysłania danych osobowych do kraju trzeciego, mimo że nie zostały spełnione warunki opisane powyżej. Dotyczyć to może następujących sytuacji:

- Osoba, której dane dotyczą, została poinformowana o ewentualnym ryzyku, z którym ze względu na brak decyzji w sprawie adekwatności oraz na brak odpowiednich zabezpieczeń może się dla niej wiązać transfer danych osobowych i wyraźnie wyraziła na to zgodę;
- Jest to niezbędne do wykonania umowy między osobą, której dane dotyczą a administratorem;
- Jest to niezbędne do zawarcia lub wykonania umowy zawartej w interesie osoby, której dane dotyczą;
- Jest to niezbędne ze względu na ważny interes publiczny lub do ustalenia, dochodzenia lub ochrony roszczeń;
- Jest to niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innych osób, jeżeli osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

CO GROZI ZA NARUSZENIE ZASAD PRZETWARZANIA DANYCH OSOBOWYCH?

Kary finansowe za nieprzestrzeganie wymogów RODO mogą sięgać do 20 milionów euro lub do 4% całkowitego rocznego światowego obrotu osiągniętego przez przedsiębiorcę w minionym roku obrotowym.

PRAWO DO WNIESIENIA SKARGI DO ORGANU NADZORCZEGO

Osoba, która uważa, że jej dane są przetwarzane niezgodnie z RODO, będzie miała prawo do wniesienia skargi do organu nadzorczego (w Polsce do Prezesa Urzędu Ochrony Danych Osobowych).

UWAGA

Skarga do organu nadzorczego będzie mogła zostać wniesiona w państwie członkowskim, w którym skarżący ma miejsce zamieszkania, miejsce pracy lub w którym doszło do domniemanego naruszenia.

Według projektu nowej ustawy o ochronie danych osobowych, postępowanie wszczęte wskutek skargi będzie toczyć się według przepisów kodeksu postępowania administracyjnego. Zakończy się wydaniem decyzji, w której organ nadzorczy stwierdzi, czy doszło do naruszenia przepisów dotyczących przetwarzania danych, czy nie. W przypadku stwierdzenia naruszenia Prezes Urzędu będzie mógł m.in. zastosować upomnienie, nakazać spełnienie żądania osoby, której dane dotyczą, nakazać dostosowanie operacji przetwarzania danych do wymogów prawa, wprowadzić czasowe lub całkowite ograniczenie lub zakaz przetwarzania danych, nakazać sprostowanie lub usunięcie danych, cofnąć certyfikację udzieloną podmiotowi naruszającemu przepisy, nakazać zawieszenie transferu danych do państw trzecich, względnie nałożyć administracyjną karę finansową.

PRAWO DO ZŁOŻENIA SKUTECZNEGO ŚRODKA OCHRONY PRAWNEJ PRZED SĄDEM PRZECIWKO ORGANOWI NADZORCZEMU

W przypadku, gdy wskutek opisanego powyżej postępowania wywołanego wniesieniem skargi na przetwarzanie danych osobowych niezgodnie z prawem, dojdzie do wydania decyzji niezadowalającej dla którejkolwiek z jego stron, każdej z nich będzie przysługiwało prawo do wniesienia do sądu tzw. skutecznego środka ochrony prawnej. W praktyce oznacza to prawo do zaskarżenia takiego rozstrzygnięcia – w Polsce poprzez wniesienie skargi do Wojewódzkiego Sądu Administracyjnego.

Z powyższych uprawnień będzie można skorzystać również wtedy, gdy organ nadzorczy nie rozpozna skargi wniesionej przez osobę, która uważa, że jej dane osobowe są przetwarzane niezgodnie z RODO, względnie, gdy nie poinformuje jej w terminie trzech miesięcy o postępach lub efektach postępowania.

PRAWO DO SKUTECZNEGO ŚRODKA OCHRONY PRAWNEJ PRZED SĄDEM PRZECIWKO ADMINISTRATOROWI LUB PODMIOTOWI PRZETWARZAJĄCEMU ORAZ PRAWO DO ODSZKODOWANIA

Tzw. prawo do skutecznego środka ochrony prawnej przed sądem, w tym przypadku rozumianego jako prawo do wniesienia pozwu, będzie przysługiwało również przeciwko administratorowi danych osobowych lub podmiotowi, któremu administrator powierzył ich przetwarzanie. Będzie mógł z niego skorzystać każdy, kto uzna, że doszło do naruszenia jego praw.

UWAGA

Postępowanie sądowe przeciwko administratorowi lub podmiotowi przetwarzającemu dane w imieniu administratora będzie mogło zostać wszczęte: (i) przed sądem państwa członkowskiego, w którym administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną, względnie (ii) przed sądem państwa członkowskiego, w którym osoba, której dane dotyczą, ma miejsce zwykłego pobytu, chyba że administrator lub podmiot przetwarzający są organami publicznymi państwa członkowskiego wykonującymi swoje uprawnienia publiczne.

Przed sądem będzie można również dochodzić odszkodowania, gdy w wyniku naruszenia warunków przetwarzania danych określonych w RODO dojdzie do wyrządzenia szkody (majątkowej lub niemajątkowej). W sytuacji, gdy naruszenia dopuszczą się administrator i przetwarzający, ich odpowiedzialność za zapłatę odszkodowania będzie solidarna. Ma to zagwarantować osobie, której dane dotyczą, rzeczywiste uzyskanie odszkodowania.

KARY FINANSOWE

UWAGA

Wysokość kar administracyjnych za naruszenie zasad przetwarzania danych może wynosić do 20 milionów euro, a w przypadku przedsiębiorstwa aż do 4% jego całkowitego rocznego światowego obrotu osiągniętego w poprzednim roku obrotowym. Co istotne, zastosowanie będzie miała zawsze kwota wyższa.

Przy określaniu wysokości kar będą brane pod uwagę czynniki takie jak:

- Charakter, waga i czas trwania naruszenia przy uwzględnieniu charakteru, zakresu lub celu danego przetwarzania, liczba poszkodowanych osób, których dane dotyczą oraz rozmiar poniesionej przez nie szkody;
- Umyślny lub nieumyślny charakter naruszenia;
- Działania podjęte przez administratora lub podmiot przetwarzający w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą.

MAPA WDROŻENIA RODO

1. Powołanie zespołu wdrożeniowego, składającego się z przedstawicieli działów firmy biorących udział we wdrożeniu.

2. Inwentaryzacja:
   - procesów przetwarzania danych;
   - zbiorów danych osobowych;
   - zasobów, za pomocą których przetwarzane są dane osobowe.

3. Analiza czynności przetwarzania danych pod kątem analizy ryzyka.

4. Weryfikacja czynności przetwarzania pod kątem wymogów prawnych.

5. Przegląd i dostosowanie klauzuli zgody na przetwarzanie danych oraz klauzuli informacyjnej.

6. Przegląd środków technicznych i organizacyjnych oraz wybór takich środków, które zapewnią bezpieczeństwo danych (z uwzględnieniem ewentualnej analizy ryzyka).

7. Przegląd, dostosowanie lub opracowanie nowej dokumentacji ochrony danych osobowych, w tym w szczególności opracowanie:
   - polityki bezpieczeństwa danych;
   - instrukcji zarządzania systemami informatycznymi;
   - umów z dostawcami;
   - umów o powierzenie przetwarzania danych;
   - porozumień dot. transferu danych za granicę.

8. Wdrożenie procedur obsługi wniosków dotyczących danych osobowych, realizujących:
   - prawo do uzupełnienia danych;
   - prawo do sprostowania danych;
   - prawo do przeniesienia danych;
   - prawo do bycia zapomnianym.

9. Wdrożenie procedur wymaganych przez RODO w zakresie czynności przetwarzania (analizy ryzyka, uprzednich konsultacji z organem ochrony danych osobowych).

10. Stworzenie procedury reagowania na przypadki naruszenia w ochronie danych z uwzględnieniem obowiązków:
    - zgłaszania naruszeń do organu ochrony danych osobowych;
    - powiadamiania osoby, której dane dotyczą.

11. Wdrożenie reguł projektowania produktów i usług:
    - privacy by design;
    - privacy by default.

12. Szkolenie pracowników w zakresie nowych procedur i reguł.

13. Regularne przeglądy stosowanych zabezpieczeń oraz zgodności zakresu przetwarzanych danych osobowych z treścią przepisów prawa.

ZESPÓŁ DO SPRAW OCHRONY DANYCH OSOBOWYCH

Przeprowadzamy audyty danych osobowych. Identyfikujemy i weryfikujemy procesy przetwarzania danych, analizujemy dokumentację ochrony danych osobowych pod kątem jej aktualności oraz zgodności z prawem. Poddajemy analizie stosowane procedury bezpieczeństwa, weryfikujemy zawarte umowy, w ramach których następuje udostępnianie danych osobowych oraz opracowujemy zalecenia po audycie. Wspólnie z klientami wdrażamy ustalone rozwiązania.

Doradzamy w zakresie właściwej ochrony danych osobowych. Sporządzamy i aktualizujemy wewnętrzną dokumentację związaną z przetwarzaniem danych osobowych, w tym politykę bezpieczeństwa i instrukcję zarządzania systemami IT, przygotowujemy również umowy i klauzule umowne związane z przetwarzaniem danych osobowych. Umożliwiamy bezpieczne przekazywanie danych osobowych za granicę oraz doradzamy w przypadkach naruszeń bezpieczeństwa. Opracowujemy polityki prywatności dla użytkowników usług internetowych, jak również zawiadomienia, informacje i projekty zgód oraz oświadczeń dotyczących przetwarzania danych. Reprezentujemy klientów w postępowaniach kontrolnych toczących się przed organami ochrony danych osobowych oraz w postępowaniach sądowych i sądowo-administracyjnych. Przeprowadzamy także szkolenia administratorów danych osobowych i administratorów bezpieczeństwa informacji.

ZAPRASZAMY DO KONTAKTU:

Magdalena Patryas
magdalena.patryas@ksplegal.pl
+48 32 731 68 53

Tomasz Srokosz
tomasz.srokosz@ksplegal.pl
+ 48 32 731 68 52

Natalia Gaweł
natalia.gawel@ksplegal.pl
+48 32 731 68 63

Kamil Kozioł
kamil.koziol@ksplegal.pl
+48 32 731 6871

Kancelaria KSP Legal & Tax Advice działa od 2003 r. Należymy do grona największych na Śląsku i najbardziej innowacyjnych kancelarii prawnych w Polsce. Adwokaci, radcowie prawni, doradcy podatkowi i ekonomiści - cały nasz ponad 30 osobowy zespół efektywnie łączy wiedzę prawną i finansową, tworząc skuteczne rozwiązania dla biznesu.

Doświadczenie zdobyte w pracy przy najbardziej znaczących transakcjach na polskim rynku potwierdzone jest wieloma rekomendacjami. Zapewniając pomoc prawną i skuteczne doradztwo podatkowe, oferujemy rozwiązania praktyczne i możliwe do szybkiego wdrożenia.

KSP T. Srokosz i Wspólnicy Sp.k.
ul. Chorzowska 150
40-101 Katowice
www.ksplegal.pl