RODO

OCHRONA DANYCH OSOBOWYCH PO 25 MAJA 2018 R.

JAK PRZYGOTOWAĆ FIRMĘ DO RODO?

Wprowadzenie

25 maja 2018 r. to przełomowa data dla przedsiębiorców w całej Unii Europejskiej. Z tym dniem zacznie obowiązywać 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.

Jako że rozporządzenie jest aktem unijnym obowiązującym bezpośrednio we wszystkich państwach członkowskich, również polscy przedsiębiorcy stają przed wyzwaniem dostosowania się do przyjętych w toku wieloletnich prac regulacji.

Rozporządzenie wprowadza do systemu ochrony danych osobowych zmiany, które przez wielu nazywane są "rewolucyjnymi". W przygotowanej specjalnie dla Państwa broszurze postaramy się wyjaśnić w formie pytań i odpowiedzi najistotniejsze kwestie związane z tym aktem prawnym oraz wskazać obszary, w których konieczne może okazać się podjęcie prac dostosowawczych na poziomie Państwa firmy.

Opracowanie nie ma charakteru porady prawnej.

W celu uzyskania szczegółowych informacji na temat procesu dostosowania przedsiębiorstwa do wymogów RODO, prosimy o kontakt Kancelarią RGW.

Anna Porebska, LL.M.
adwokat
a.porebska@rgw.com.pl

Podstawowe informacje

CO KRYJE SIĘ POD SKRÓTEM RODO?

Jako "RODO" lub "GDPR" określa się w skrócie 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).

RODO weszło w życie już 17 maja 2016 r., jednakże zgodnie z przepisami przejściowymi zacznie obowiązywać od 25 maja 2018 r.

JAKI JEST CEL RODO?

RODO jest wynikiem prac legislacyjnych wiele lat na szczeblu unijnym, których celem było ujednolicenie zasad ochrony danych osobowych we wszystkich państwach członkowskich. RODO zastępuje obowiązującą od 24 października 1995 r. Dyrektywę 95/46/WE w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych.

Aby zapewnić wysoki i spójny stopień ochrony osób fizycznych oraz usunąć przeszkody w przepływie danych osobowych w Unii, należy zapewnić równorzędny we wszystkich państwach członkowskich stopień ochrony praw i wolności osób fizycznych w związku z przetwarzaniem takich danych. Należy zapewnić spójne i jednolite w całej Unii stosowanie przepisów o ochronie podstawowych praw i wolności osób fizycznych w związku z przetwarzaniem danych osobowych.

Motyw 10 Preambuly RODO

DLACZEGO OCHRONA DANYCH OSOBOWYCH W UNII EUROPEJSKIEJ JEST TAK WAŻNA?

Ochrona osób fizycznych w związku z przetwarzaniem danych osobowych jest jednym z praw podstawowych. Art. 8 ust. 1 Karty praw podstawowych Unii Europejskiej oraz art. 16 ust. 1 Traktatu o funkcjonowaniu Unii Europejskiej stanowią, że każda osoba ma prawo do ochrony danych osobowych jej dotyczących.

Zakres obowiązywania RODO

CZY KAŻDY PRZEDSIĘBIORCA MUSI PRZESTRZEGAĆ RODO?

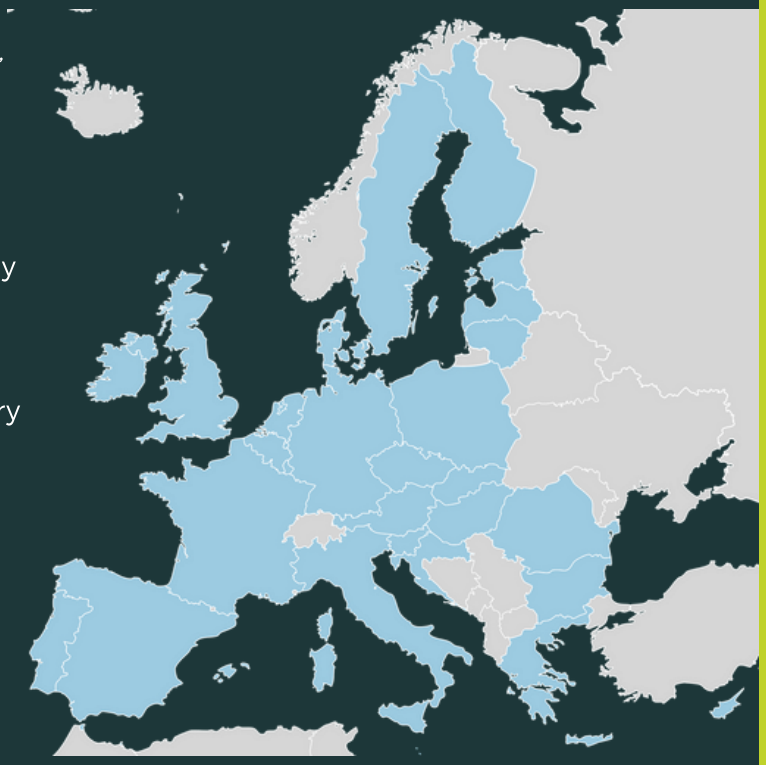
RODO ma zastosowanie do wszystkich podmiotów przetwarzajacych dane osobowe w sposób całkowicie lub częściowo zautomatyzowany oraz w sposób innych niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

O ile przedsiębiorca z państwa członkowskiego przetwarza dane, niezależnie od tego, czy przetwarzanie odbywa się w Unii, wiążą go przepisy rozporządzenia. Dotyczy to zarówno administratora danych, jak i podmiot przetwarzający dane na jego zlecenie.

CZY RODO MA RÓWNIEŻ ZNACZENIE DLA FIRM SPOZA UNII?

Dane osobowe osób przebywających w Unii, jesli czynności tych podmiotów wiążą się z oferowaniem towarów lub usług lub monitorowaniem zachowań na terenie Unii.

Zgodnie z postanowieniami RODO podmioty spoza Unii mają obowiązek wyznaczenia na terytorium UE swojego przedstawiciela, mającego swoją siedzibę w państwie członkowskim, gdzie przebywają osoby, który dane osobowe są przetwarzane.



Zasady obowiązujące przy przetwarzaniu danych osobowych

Art. 5 RODO wprowadza sześć głównych zasad, które obowiązują przy przetwarzaniu danych osobowych.

Są to zasady:

- zgodności z prawem, rzetelności i przejrzystości,
- ograniczenia celu,
- minimalizacji danych,
- prawidłowości,
- ograniczenia przechowywania,
- integralności i poufności,
- rozliczalności.

KIEDY PRZETWARZANIE DANYCH JEST ZGODNE Z PRAWEM?

Dopuszczalność przetwarzania danych osobowych uwarunkowana jest istnieniem co najmniej jednej z wymienionych w art. 6 RODO przesłanek. Przetwarzanie danych osobowych jest zgodne z prawem, jeśli:

- osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
- 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;
- przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
- przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
- przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- 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.

KIEDY ZGODA NA PRZETWARZANIE DANYCH OSOBOWYCH JEST SKUTECZNA?

Zgoda może zostać wyrażona w dowolny sposób, ale administrator musi być w stanie to wykazać. W RODO podkreśla się, że zgoda musi mieć charakter dobrowolny. W szczególności wyrażenie zgody nie powinno warunkować wykonania zawartej umowy, jeśli przetwarzanie danych osobowych nie jest do tego niezbędne. Jeśli pisemne oświadczenie o zgodzie stanowi część dokumentu zawierającego również inne kwestie, to zapytanie o zgodę musi być przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i ławo dostępnej formie, jasnym i prostym językiem. Nie jest wiążące oświadczenie, które zostało pozyskane wbrew przepisom rozporządzenia.

Obowiązki podmiotów przetwarzających dane osobowe

CZY W DALSZYM CIĄGU KONIECZNA BĘDZIE REJESTRACJA ZBIORÓW DANYCH W GIODO?

Dotychczas istniał obowiązek rejestracji zbiorów danych w GIODO. Rozporządzenie znosi ten obowiązek, wprowadzając w jego miejsce rejestrowanie czynności przetwarzania danych osobowych przez administratora lub podmiot przetwarzający dane. Rejestr powinien być prowadzony w formie pisemnej, w tym w formie elektronicznej. Administrator ma obowiązek udostępnienia rejestru na żądanie organu nadzoru.

Prowadzenie rejestru nie jest obligatoryjne dla przedsiębiorców, którzy zatrudniają mniej niż 250 pracowników, chyba że przetwarzanie może powodować ryzyko naruszenia praw lub wolności osób, których dane dotyczą, nie ma charakteru sporadycznego lub obejmuje szczególne kategoria danych osobowych lub dane dotyczące wyroków skazujących i naruszeń prawa.

CO MUSI ZAWIERAĆ REJESTR CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH PROWADZONY PRZEZ ADMINISTRATORA?

- imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora oraz inspektora ochrony danych,
- cele przetwarzania,
- opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
- kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
- ewentualnie informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej (z ich wskazaniem),
- planowane terminy usunięcia poszczególnych kategorii danych (o ile to możliwe),
- ogólny opis technicznych i organizacyjnych środków bezpieczeństwa (o ile to możliwe).

NA CZYM POLEGA SZACOWANIE SKUTKÓW PRZETWARZANIA DANYCH?

Proces przetwarzania danych musi być poprzedzony przeprowadzaniem przez administratora oceną ryzyka, która pozwala na dobranie odpowiednich środków bezpieczeństwa. Jest to szczególnie istotne jeśli przetwarzanie odbywa się z użyciem nowych technologii i ze względu na charakter, zakres, kontekst i cel wiąże się z wysokim ryzykiem naruszenia praw i wolności osób fizycznych. W szczególnie obarczonych ryzykiem przypadkach konieczna może być uprzednia konsultacja administratora danych z organem nadzoru, który może udzielić administratorowi pisemnego zalecenia lub skorzystać z przysługujących mu wobec administratora uprawnień.

Prawa osób fizycznych

JAKIE GŁÓWNE PRAWA NALEŻY ZAPEWNIĆ OSOBIE FIZYCZNEJ, KTÓREJ DANE OSOBOWE DOTYCZĄ?

- prawo dostępu do danych i informacji,
- prawo żądania sprostowania i uzupełnienia danych,
- prawo sprzeciwu wobec przetwarzania danych,
- prawo do przeniesienia danych,
- prawo do usunięcia danych.

O CZYM NALEŻY POINFORMOWAĆ OSOBĘ FIZYCZNĄ PODCZAS POZYSKIWANIA JEJ DANYCH OSOBOWYCH?

Rozporządzenie reguluje zakres obowiązków informacyjnych administratora, które muszą zostać spełnione w chwili ich pozyskiwania.

Konieczne jest wskazanie przez administratora m.in. następujących informacji:

- tożsamość i dane kontaktowe ew. tożsamość i dane kontaktowe przedstawiciela, ew. dane kontaktowe inspektora ochrony danych,

- cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania,

- prawnie uzasadnione interesy realizowane przez administratora lub przez stronę trzecią (jeśli taka jest podstawa przetwarzania),

- informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,

- ew. informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,

- okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,

- informacje o prawie do żądania od administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych,

- informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem,
- informacje o prawie wniesienia skargi do organu nadzorczego,

- informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,

- informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu.

Nadzór nad przestrzeganiem RODO

JAKIE BĘDĄ UPRAWNIENIA KRAJOWEGO ORGANU OCHRONY DANYCH OSOBOWYCH?

Z projektu ustawy o ochronie danych osobowych przygotowanego przez Ministerstwo Cyfryzacji wynika, że polski organ nadzorczy (dotychczas Generalny Inspektor Ochrony Danych Osobowych, tj. GIODO) będzie nosił nazwę Prezes Urzędu Ochrony Danych Osobowych (UODO).

Uprawnienia UODO będą w dużym zakresie pokrywać się z uprawnieniami GIODO, jednakże struktura UODO ma zostać rozbudowana, a oprócz rozpatrywania skarg, monitorowania naruszeń i prowadzenia ich rejestru, nakładania kar administracyjnych za stwierdzone naruszenia, UODO będzie również odpowiedzialny za przyjmowanie standardowych klauzul umownych, prowadzenie wykazu ocen skutków przetwarzania, udzielanie zaleceń dotyczących przetwarzania danych, akredytację podmiotów certyfikujących, współpracę z organami nadzorczymi z innych państw.

JAKIE SANKCJE PIENIĘŻNE BĘDĄ GROZIĆ ZA NARUSZENIE PRZEPISÓW OCHRONY DANYCH OSOBOWYCH?

Za naruszenie przepisów w zakresie ochrony danych osobowych RODO przewiduje sankcję w postaci administracyjnej kary pieniężnej, która w zależności od rodzaju i wagi naruszenia może wynosić:

- do 10.000.000,00 EUR, a w przypadku przedsiębiorstwa do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego, lub

- do 20.000.000,00 EUR lub 4% procent całkowitego rocznego światowego obrotu.

JAKIE INNE UPRAWNIENIA PRZYSŁUGUJĄ ORGANOWI NADZORCZEMU?

Organ nadzorczy w przypadku stwierdzonego naruszenia może skorzystać z przysługujących mu uprawnień naprawczych, takich jak:
- wydawanie ostrzeżeń dotyczących możliwości naruszenia przepisów rozporządzenia,
- udzielanie upomnień,
- nakazanie administratorowi spełnienia żądań osoby, której dane dotyczą,
- nakazanie zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych,
- nakazanie dostosowania operacji przetwarzania danych do przepisów rozporządzenia,
- wprowadzenie czasowego lub całkowitego ograniczenia przetwarzania, w tym zakazu przetwarzania danych,
- nakazanie sprostowania lub usunięcia danych osobowych,
- cofnięcie certyfikacji.

JAKIE OKOLICZNOŚCI BĘDĄ BRANE PRZY WYMIARZE KAR?

Wymiar administracyjnej kary pieniężnej ustalany jest dla każdego przypadku naruszenia indywidualnie z uwzględnieniem takich okoliczności jak charakter, waga i czas trwania naruszenia, liczba poszkodowanych osób i rozmiar ich szkody, umyślny lub nieumyślny charakter naruszenia, działania podjęte w celu zminimalizowania szkody, stopień odpowiedzialności administratora, wcześniejsze naruszenia, stopień współpracy z organem nadzorczym, kategorie danych osobowych, sposób powzięcia przez organ nadzoru informacji o naruszeniu, stosowanie zatwierdzonych kodeksów postępowania lub mechanizmów certyfikacji, innych czynników łagodzących lub obciążających.

CZY OSOBA, KTÓREJ DANE OSOBOWE BYŁY PRZETWARZANE NIEZGODNIE Z PRAWEM, MOŻE DOCHODZIĆ ODSZKODOWANIA?

Z naruszeniem ochrony danych osobowy związana jest odpowiedzialność cywilna administratora danych lub podmiotu przetwarzającego dane. Zgodnie z art. 82 RODO każda osoba, która poniosła szkodę majątkową lub niemajątkową w wyniku naruszenia rozporządzenia, ma prawo uzyskać od tych podmiotów odszkodowanie za poniesioną szkodę.

RODO wprowadza w tym zakresie domniemanie winy. Warunkiem uwolnienia się od odpowiedzialności jest udowodnienie, że w żaden sposób dany podmiot nie ponosi winy za zdarzenie, które doprowadziło do powstania szkody. Postępowania prowadzone będą przez właściwe sądy państw członkowskich.

CZY POWOŁANIE INSPEKTORA OCHRONY DANYCH JEST OBOWIĄZKOWE?

Dotychczasową funkcję administratora bezpieczeństwa informacji (ABI) przejmie inspektor ochrony danych. Powołanie ABI było dotychczas dobrowolne, natomiast RODO określa sytuacje, w których należy obowiązkowo wyznaczyć inspektora ochrony danych.

Nic nie stoi na przeszkodzie powołaniu inspektora dobrowolnie również tam, gdzie nie ma takiego obowiązku.

Szczegółowe zasady dotyczące wyboru osoby pełniącej funkcję inspektora ochrony danych zostały określone w Wytycznych Grupy Roboczej art. 29 dotyczących inspektorów ochrony danych z 13 grudnia 2016 r.

JAKIE ZADANIA MA INSPEKTOR OCHRONY DANYCH?

Obowiązkiem inspektora jest m.in. informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach spoczywających na nich z mocy prawa oraz doradzanie im w tej sprawie, monitorowanie przestrzegania przepisów o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty, udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania, współpraca z organem nadzorczym.

JAKĄ DOKUMENTACJĘ DOTYCZĄCĄ OCHRONY DANYCH OSOBOWYCH NALEŻY PROWADZIĆ W PRZEDSIĘBIORSTWIE?

Przypomnijmy, że zgodnie z dotychczas obowiązującymi przepisami ustawy o ochronie danych osobowych dokumentacja dotycząca ochrony danych osobowych obejmuje m.in. politykę bezpieczeństwa, instrukcję zarządzania systemem informatycznym, upoważnienia do przetwarzania danych oraz ich ewidencja.

RODO nie przewiduje obowiązku prowadzenia takiej dokumentacji, jednak w razie kontroli przedsiębiorca będzie musiał i tak wykazać za pomocą jakiejś dokumentacji, że przetwarza dane zgodnie z prawem.

Dlatego tak istotne jest wdrożenie w firmie obowiązków wynikających z RODO, uaktualnienie polityki ochrony danych osobowych oraz uzupełnienie prowadzonej dokumentacji przed 25 maja 2018 r. Pomoże to uniknąć grożących za naruszenie Rozporządzenia sankcji.

JAKIE KROKI NALEŻY PODJĄĆ W CELU DOSTOSOWANIA SIĘ DO WYMOGÓW RODO?

- Zapoznanie się z nowymi przepisami
- Przegląd dotychczas stosowanych procedur przetwarzania danych osobowych
- Zidentyfikowanie rodzaju i sposobu zbierania oraz przetwarzania danych w organizacji
- Przygotowanie lub zaktualizowanie polityki bezpieczeństwa danych oraz planu wdrożenia nowych regulacji i szacowania ryzyka
- Przeszkolenie kadr kierowniczych i pracowników, których obowiązki związane są z przetwarzaniem danych osobowych
- Wdrażanie zmian według przyjętego planu poprzez m.in. przydzielenie ról odpowiednim osobom, wzmocnienie zabezpieczeń technicznych i prawnych w wymaganym zakresie
- Prowadzenie rejestru czynności przetwarzania danych, dokumentowanie przypadków naruszeń bezpieczeństwa danych i prowadzenie ich rejestru