lsw | Leśnodorski Ślusarek i Wspólnicy

RODO

W PYTANIACH I ODPOWIEDZIACH

CO TO JEST RODO?

Skrótem „RODO" powszechnie określa się rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych), które weszło w życie w dniu 24 maja 2016 r., a zacznie obowiązywać od 25 maja 2018 r. Z chwilą wejścia w życie RODO we wszystkich krajach UE zacznie obowiązywać nowy – ujednolicony – system ochrony danych osobowych, a w konsekwencji wszyscy przedsiębiorcy z krajów UE będą zobowiązani do stosowania tych samych zasad ochrony danych osobowych. RODO zastąpi stare i nie nadążające za postępem i rozwojem technologii zasady ochrony danych osobowych, ujednolici system ochrony danych w całej UE oraz zwiększy ochronę danych osobowych osób fizycznych.

CZY OCHRONA DANYCH OSOBOWYCH RÓWNIEŻ MNIE DOTYCZY?

Przepisy rozporządzenia RODO obejmują zarówno przedsiębiorców i osoby fizyczne, będące administratorami danych osobowych, jak również podmioty przetwarzające dane osobowe w imieniu administratora, którzy prowadzą działalność na terenie Unii Europejskiej (niezależnie gdzie przetwarzają dane osobowe). Dodatkowo nowe przepisy obejmą również podmioty z państw trzecich, jeżeli będą oni przetwarzać dane osobowe osób przebywających na terenie UE, w związku z oferowaniem towarów lub usług takim osobom w UE (nawet za darmo) oraz monitorowaniem ich zachowania (na terenie UE). Podmioty z spoza UE będą musiały wyznaczyć swojego przedstawiciela na terytorium Unii Europejskiej.

JAKIE NOWE SANKCJE PRZEWIDUJĄ RODO?

Nowe rozporządzenie **wprowadza surowe kary administracyjne za naruszenie przepisów ochrony danych osobowych.** Kary będą mogły sięgać kwoty 20 mln Euro (lub w przypadku przedsiębiorstwa do 4% światowego obrotu za poprzedni rok obrotowy), a w przypadku spraw mniejszej wagi do 10 mln Euro (lub odpowiednio do 2% obrotu). Każdy przypadek nałożenia kary będzie rozpatrywany indywidualnie przez organ nadzoru, który będzie brał pod uwagę w szczególności: skalę naruszenia, umyślność, podjęte działania zapobiegawcze, a także wcześniejsze przypadki naruszeń przez przedsiębiorcę.

CZY DALEJ REJESTROWAĆ ZBIORY DANYCH OSOBOWYCH?

Zgodnie z nowymi zasadami, administrator danych osobowych **będzie musiał prowadzić rejestr czynności przetwarzania danych osobowych** – zamiast dotychczasowego obowiązku rejestracji zbiorów danych w GIODO. Rejestr czynności powinien uwzględniać w szczególności informacje o: administratorze, inspektorze ochrony danych, celach przetwarzania danych, kategorii danych osobowych, planowanym terminie usuwania danych oraz środkach bezpieczeństwa. Rozporządzenie wprowadza wyjątki od obowiązku prowadzenia rejestru czynności przetwarzania danych (np. wybrani przedsiębiorcy zatrudniający do 250 pracowników), jednakże przewiduje również kary za naruszenie obowiązku rejestracji czynności.

CO Z OBOWIĄZKIEM INFORMOWANIA OSÓB, KTÓRYCH DANE DOTYCZĄ?

RODO istotnie poszerza zakres informacji, które mają być przekazywane podmiotom danych. **Zgodnie z nowymi przepisami administrator będzie zobowiązany poinformować w szczególności o:** podstawie prawnej przetwarzania danych, zamiarze przekazania danych do państwa trzeciego (jeśli administrator przewiduje), okresie, przez który dane te maja być przetwarzane albo kryterium ustalenia tego okresu, profilowaniu oraz o prawie wniesienia skargi do organu nadzoru. Nowe obowiązki informacyjne skutkować będą koniecznością weryfikacji wykorzystywanych przez przedsiębiorców formularzy oraz ewentualnego dostosowania ich do nowych wymagań.

JAKIE UŁATWIENIA DLA GRUP PRZEDSIĘBIORCÓW?

RODO wprowadza znaczne ułatwienie dla grup przedsiębiorców wspólnie przetwarzających dane osobowe. Zgodnie z przepisami rozporządzenia, jeżeli przynajmniej dwóch administratorów wspólnie ustala cele i sposoby przetwarzania danych osobowych są oni „współadministratorami" i mogą wówczas „podzielić się" prawami i obowiązkami dotyczącymi ochrony danych osobowych. Zakres obowiązków oraz relacje pomiędzy nimi a podmiotami, których dane dotyczą, określą w ramach wspólnych uzgodnień, których treść powinni udostępnić podmiotom danych osobowych.

CO ZROBIĆ W PRZYPADKU INCYDENTÓW NARUSZENIA OCHRONY DANYCH OSOBOWYCH?

RODO nakłada na przedsiębiorców **obowiązek niezwłocznego (nie później niż w przeciagu 72 godzin) informowania organu nadzoru o naruszeniu ochrony danych osobowych** (chyba, że nie będzie to skutkowało ryzykiem naruszeniem praw i wolności osób fizycznych). Jeżeli ryzyko naruszenia praw i wolności osób fizycznych będzie wysokie (np. wyciek danych wrażliwych), administrator bez zbędnej zwłoki będzie musiał poinformować również osoby, których dane dotyczą. Konieczne będzie zatem zweryfikowanie posiadanych zabezpieczeń, nieustanne monitorowanie stanu bezpieczeństwa oraz opracowanie planów awaryjnych na wypadek sytuacji zagrożenia.

CZY MUSZĘ STOSOWAĆ POLITYKĘ DANYCH?

Aktualne przepisy zobowiązują przedsiębiorców do **wdrożenia polityki bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych.** Również RODO zawiera ogólne wytyczne dotyczące tworzenia takich polityk przez administratorów danych. Mimo, że nie nakłada ono formalnego obowiązku ich stosowania, każdy z przedsiębiorców powinien je wdrożyć aby wykazać, że zapewnia odpowiednie środki i skuteczną ochronę danych osobowych. Jednocześnie istnieje konieczność weryfikacji dotychczas stosowanych polityk przez przedsiębiorców – pod kątem ich zgodności z RODO.

POWINIENEM POWOŁAĆ INSPEKTORA OCHRONY DANYCH?

RODO wprowadza instytucję Inspektora Ochrony Danych (IOD), który ma zastąpić dotychczasowych Administratorów Bezpieczeństwa Informacji (ABI). Powołanie IOD jest konieczne w przypadku, gdy dane osobowe są przetwarzane przez organ lub podmiot publiczny, oraz gdy główna działalność podmiotu polega na przetwarzaniu szczególnych kategorii danych osobowych na dużą skalę lub też w przypadku, gdy główna działalność podmiotu polega na operacjach przetwarzania danych. **Niewątpliwie w wielu przypadkach powołanie IOD będzie konieczne**, a sam Inspektor będzie pełnił niezwykle istotną rolę.

CZY KONIECZNE SĄ ZMIANY W UMOWACH Z DOSTAWCAMI / KLIENTAMI?

Aktualne przepisy ustawy o ochronie danych **wymagają zawierania umów powierzenia przetwarzania danych osobowych z dostawcami lub przynajmniej uwzględnienia odpowiednich postanowień w tym zakresie w umowach współpracy.** Jest to szczególnie istotne w przypadku outsourcowania usług do innych podmiotów. RODO nie tylko modyfikuje powyższe zasady, ale także wprowadza dodatkowe obowiązki związane z treścią takich umów. Dlatego też konieczna wydaje się analiza dotychczas stosowanych umów z dostawcami/klientami oraz ich dostosowanie do nowej rzeczywistości.

CO OZNACZA ZASADA PRIVACY BY DESIGN?

Ideą „privacy by design" jest to by eliminować problemy związane z ochroną danych osobowych już na etapie planowania wdrożenia nowych produktów lub usług. Założeniem RODO jest skuteczne przewidywanie i zapobieganie incydentom związanym z ochroną danych osobowych i w tym celu nakłada na administratorów obowiązek przeanalizowania skutków podejmowanych operacji przetwarzania danych osobowych pod kątem ochrony danych osobowych. Przykładowo agencja marketingowa przygotowująca akcję promocyjną dla klienta będzie zobowiązana - już na etapie planowania samej akcji - do oceny, czy zasady tej akcji są zgodne z przepisami o ochronie danych osobowych, a dane będą odpowiednio chronione. To samo dotyczy się tworzenia nowych produktów i usług takich jak np. aplikacje mobilne czy systemy informatyczne.

CZY KONIECZNE BĘDĄ ZMIANY SYSTEMÓW INFORMATYCZNYCH?

RODO wprowadza szereg nowych obowiązków w zakresie ochrony danych osobowych, których realizacja nie będzie możliwa bez odpowiedniej modyfikacji systemów IT, w oparciu o które przetwarzane są dane. Na przykład obowiązek prowadzenia rejestru czynności przetwarzania danych osobowych, czy prawo do żądania przez osoby fizyczne od administratora przenoszenia jego danych osobowych, wymuszą na przedsiębiorcach konieczność wprowadzenia odpowiednich zmian do systemów informatycznych, programów komputerowych i systemów CRM stosowanych w firmach.

ZESPÓŁ ODPOWIEDZIALNY

MACIEJ ŚLUSAREK
Adwokat / Wspólnik
m.slusarek@lsw.com.pl

MACIEJ KUBIAK
Adwokat / Wspólnik
m.kubiak@lsw.com.pl

MACIEJ DUDEK
Radca Prawny
m.dudek@lsw.com.pl