Często Zadawane Pytania

Co kryje się za nowym ogólnym rozporządzeniem o ochronie danych (RODO)?

25 maja 2018 r. dobiega końca dwuletni okres przejściowy obowiązywania rozporządzenia UE RODO (nazwa międzynarodowa to GDPR – General Data Protection Regulation). Od tego momentu nowe ogólne rozporządzenie o ochronie danych będzie stanowić prawo obowiązujące we wszystkich krajach członkowskich Unii Europejskiej (UE). Rozporządzenie to jest istotną regulacją prawną, pozwalającą na poprawę i ujednolicenie ochrony danych na terenie całej Europy. Powodem jego powstania jest rosnąca internacjonalizacja codziennej działalności biznesowej oraz postęp technologiczny uwarunkowany cyfryzacją. Dodatkowo w tym samym momencie zostanie wprowadzona nowelizacja niemieckiej ustawy o ochronie danych. Zachowany zostanie ogólny charakter najważniejszych fundamentów obowiązującej ustawy, jak np. zasady przetwarzania danych. Jednakże wraz z RODO wprowadzone zostaną istotne przepisy dodatkowe. I tak nowe rozporządzenie reguluje dalsze podstawy prawne przetwarzania danych, zwiększa prawa osób, których to dotyczy i nakłada nowe obowiązki na administratorów. W celu zapewnienia zgodności z RODO należy skupić się na technologiach stosowanych w organizacjach, obowiązujących przepisach RODO i aspektach organizacyjnych.

Ze względu na nowe obowiązki organizacji związane z przejrzystością i udzielaniem informacji wzmocnieniu ulegają prawa użytkowników. Oznacza to, że osoby, których dane dotyczą, muszą mieć na żądanie zapewniony łatwiejszy dostęp do swoich danych i informacji na temat celu ich wykorzystywania. Ponadto żądanie usunięcia danych osobowych (prawo do wykasowania z pamięci) otrzyma jasne ramy prawne. RODO reguluje jednolite przetwarzanie danych osobowych na terenie UE w artykule 4: „'dane osobowe' oznaczają 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;"

Których kluczowych rozporządzeń RODO organizacje muszą przestrzegać?

- Organizacje są zobowiązane do przygotowania zestawienia danych osobowych i podania miejsca ich przechowywania. Dotyczy to przede wszystkim infrastruktury IT obecnej w większej liczbie oddziałów oraz w chmurze.
- Ze względu na wytyczne o przejrzystości i podawaniu informacji obywatele UE mają prawo do żądania wglądu, wydania i usunięcia danych przez organizacje. W związku z tym organizacje są zobowiązane do wdrożenia procedur umożliwiających szybkie odszukanie i w razie potrzeby usunięcie danych.

- Organizacje są zobowiązane do ograniczenia ilości danych osobowych do minimum. Ponadto dane osobowe mogą być gromadzone tylko w konkretnym celu i tylko na określony okres.
- W związku z atakami takimi jak WannaCry wzrosło w ostatnich miesiącach znaczenie kwestii związanych przede wszystkim z cyberbezpieczeństwem. W następstwie tego dane osobowe należy chronić przed niewłaściwym wykorzystaniem w wyniku ataków od wewnątrz i z zewnątrz. Jeśli nastąpi naruszenie przepisów o ochronie danych osobowych, wówczas zachodzi obowiązek poinformowania w przeciągu 72 godzin osoby, której to dotyczy. W celu identyfikacji wycieku danych organizacje są zobowiązane do stosowania nowoczesnych narzędzi technologicznych, co pozwoli na szybkie i jednoznaczne ustalenie utraconych danych.

W jaki sposób organizacje muszą udowodnić przestrzeganie przepisów RODO?

Jednym z kluczowych elementów obok technologii i utworzenia procedur jest obowiązek prowadzenia dokładnej dokumentacji i „rozliczalność" organizacji. Zgodnie z art. 5. ust. 2 RODO administrator musi być w stanie wykazać przestrzeganie przepisów tego rozporządzenia. Inaczej niż w niemieckiej ustawie o ochronie danych osobowych w przypadku RODO nie wystarczy już wykazanie przestrzegania postanowień związanych z przetwarzaniem danych, lecz w o wiele większym zakresie udzielenie na żądanie informacji na temat zgodnego z prawem gromadzenia, przetwarzania i zapisu danych.

Co dzieje się w przypadku naruszenia przepisów RODO przez organizacje?

Organizacje, które w sposób nieumyślny lub umyślny naruszają przepisy wynikające z RODO muszą liczyć się ze znacznymi karami finansowymi, wynoszącymi albo 4% globalnego obrotu organizacji, albo 20 mln euro, w zależności od tego, która suma jest wyższa.

Czy oprogramowanie baramundi Management Suite (bMS) zapewnia zgodność z przepisami RODO?

W ramach jednolitego zarządzania urządzeniami końcowymi bMS zapewnia administratorom ważne narzędzia, takie jak baramundi Inventory czy też baramundi Compliance-Management, które pozwalają na prowadzenie działań zgodnych z RODO. Dzięki samodzielnie tworzonemu rozwiązaniu („Made in Germany") baramundi software AG nieustannie zwraca uwagę na zgodność z aktualnie obowiązującymi i mającymi obowiązywać w przyszłości przepisami prawa, by w ten sposób zapewnić administratorom skuteczną pomoc w ich przestrzeganiu.

Przykładowe obszary zastosowania można znaleźć w arkuszu danych baramundi w związku z RODO. Chętnie odpowiemy na wszelkie indywidualne pytania.

Jaki wpływ ma RODO na państwa trzecie spoza UE?

Nawet jeśli Szwajcaria znajduje się w Europie, w myśl RODO należy ją traktować jako państwo trzecie. Państwem trzecim jest każdy kraj niebędący członkiem Unii Europejskiej. Zgodnie z art. 3, ust. 2 państw trzecich dotyczyć będzie tzw. zasada prawa miejsca, gdzie ma być spełnione świadczenie. Zasada ta w określonych okolicznościach obejmuje także organizacje, które nie mają siedziby na terenie UE. Organizacje pozaeuropejskie, do których czynności przetwarzania ma zastosowanie RODO, muszą zasadniczo wyznaczyć przedstawiciela w jednym z krajów członkowskich UE objętych RODO. W myśl RODO organizacje są zobowiązane do wyraźnego, pisemnego zlecenia swoim przedstawicielom obowiązku zapewnienia przestrzegania wszystkich przepisów RODO w swoim imieniu. Za niedotrzymanie obowiązku wyznaczenia przedstawiciela nałożona zostanie kara finansowa.

Jaki wpływ na RODO ma zbliżający się Brexit?

Po wyjściu z Unii Europejskiej Wielką Brytanię należy również traktować jako państwo trzecie. Oznacza to, że, o ile prowadzone są interesy z wewnętrznym rynkiem UE lub gromadzone, przetwarzane i zapisywane są dane obywateli UE, Wielka Brytania jest zobowiązana do przestrzegania tych samych rozporządzeń. Na ten moment Wielka Brytania jest jeszcze aktywnym członkiem UE, i tym samym w odniesieniu do niej RODO znajduje bezpośrednie zastosowanie.