

## Przetwarzanie danych osobowych - zmiany w prawie unijnym

W zeszłym roku Parlament Europejski przyjął finalny tekst Rozporządzenia w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (dalej: „RODO”). Obecnie w podanym zakresie wciąż obowiązuje przywołana Dyrektywa 95/46/WE, jednakże jej zastąpienie nową regulacją istotnie zmieni funkcjonowanie zasad przetwarzania danych osobowych polskich przedsiębiorstw i przedsiębiorców w branży portowo - morskiej. Poniżej zwięźle przedstawiamy ogólną charakterystykę tego aktu i wybrane zagadnienia, które reguluje.

### Zakres zastosowania

Pod względem podmiotowym RODO obejmie swoimi postanowieniami zarówno administratorów posiadających swoje jednostki organizacyjne w UE jak i te spoza UE, jeżeli swoje towary lub usługi kierują do osób zamieszkujących państwa członkowskie UE. RODO akt znajdzie zastosowanie do przetwarzania danych osobowych w sposób całkowicie lub częściowo zautomatyzowany oraz do przetwarzania w sposób inny niż zautomatyzowany danych osobowych stanowiących część zbioru danych lub mających stanowić część zbioru danych.

### Obowiązki mniejszych podmiotów gospodarczych

W myśl obowiązujących na chwilę obecną rozwiązań prawnych, w zakresie ochrony danych osobowych takim samym regulacjom podlegają zarówno duże podmioty, grupy podmiotów, jak i osoby fizyczne prowadzące działalność gospodarczą na niewielką skalę. Nowe przepisy mają być natomiast dostosowane do rodzaju przedsiębiorstwa i uwzględniać specyfikę wynikającą z rozmiaru firm.

Obecnie każdy administrator danych w Polsce jest obowiązany prowadzić specjalną dokumentację ochrony danych osobowych. W jej skład wchodzi między innymi polityka bezpieczeństwa, instrukcja zarządzania systemem informatycznym, ewidencja upoważnień do przetwarzania danych osobowych. Specyfiką obecnego systemu jest brak elastyczności spowodowany istnieniem identycznego zakresu obowiązków dla każdego administratora danych. W rezultacie właściwie skonstruowaną politykę bezpieczeństwa musi prowadzić zarówno międzynarodowa korporacja jak i niewielkich rozmiarów firma spedycyjna.

Wstępna analiza postanowień RODO wskazuje, że podmioty działające na mniejszą skalę (zatrudniające mniej osób), które nie są zaangażowane w przetwarzanie dużej ilości danych osobowych, nie będą musiały wdrażać rozbudowanej polityki bezpieczeństwa. W myśl bowiem art. 24 ust. 1 RODO administrator obowiązany będzie do wdrożenia odpowiednich środków technicznych i organizacyjnych uwzględniając „charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia”. W dalszej części wskazanego przepisu RODO określa, iż jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki podejmowane przez administratora obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.

### Zasada one-stop-shop

RODO reguluje problem przetwarzania danych przez grupy kapitałowe, określając tego typu podmioty jako „grupy przedsiębiorstw” i definiując je jako „przedsiębiorstwa sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane”. Ma to doniosłe znaczenie, bowiem

postanowienia RODO przewidują uproszczone procedury dotyczące transferu danych osobowych w obrębie grupy.

Warto w tym kontekście nadmienić, że wspomniane grupy przedsiębiorstw lub pojedyncze spółki oferujące usługi na terenie kilku państw UE, będą mogły wykorzystać tzw. zasadę „one-stop-shop”. Zgodnie z nią, główna jednostka organizacyjna (tu np. podmiot zarządzający grupą kapitałową), będzie uprawniona do dokonania wyboru organu ochrony danych osobowych, który stanie się właściwy w kontekście funkcjonowania całej grupy.

### **Możliwe sankcje**

Odnotowania wymaga dotkliwość sankcji jakie przewiduje RODO za naruszenia nowych reguł a do których nałożenia będzie pozostawał uprawniony każdy organ nadzorczy państwa członkowskiego (w Polsce - Generalny Inspektor Ochrony Danych Osobowych). Nie wdając się w szczegółowy opis charakterystyki konkretnych uchybień, należy mieć na uwadze możliwość zastosowania sankcji finansowych w wysokości do dziesięciu milionów EUR lub do 2 % rocznego obrotu przedsiębiorstwa. Co więcej, w przypadku naruszeń podstawowych zasad przetwarzania danych osobowych, nałożona kara może wynieść nawet 20 milionów EUR lub 4% rocznego obrotu przedsiębiorstwa. Równocześnie warto nadmienić, że wymienione sankcje będą mogły być stosowane z urzędu oraz bez uprzedniego wezwania do usunięcia uchybień (tak jak ma to miejsce w obecnie obowiązujących przepisach).

### **Precyzowanie postanowień przez państwa członkowskie**

RODO stanowi, że państwa członkowskie mogą przyjąć przepisy szczególne, tj. precyzować czy też zaostrzać postanowienia zawarte w RODO. W szczególności dotyczy to uregulowania zagadnień określających uprawnienia organów nadzorczych wobec administratorów lub podmiotów przetwarzających, którzy podlegają – na mocy prawa UE lub prawa państwa członkowskiego bądź przepisów ustanowionych przez właściwe organy krajowe – obowiązkowi zachowania tajemnicy zawodowej lub innym równoważnym obowiązkom zachowania tajemnicy, jeżeli jest to niezbędne i proporcjonalne w celu pogodzenia prawa do ochrony danych osobowych z obowiązkiem zachowania tajemnicy. Powyższe ma zastosowanie wyłącznie do danych osobowych, które administrator lub podmiot przetwarzający otrzymali lub pozyskali w wyniku lub w ramach działania objętego tym obowiązkiem zachowania tajemnicy.

### **Podsumowanie**

Przepisy RODO zaczną bezpośrednio oddziaływać na polski porządek prawny z dniem 25 maja 2018 roku. Jak zostało powyżej zasygnalizowane, przyjęte rozwiązania przewidują szereg zmian względem obecnego stanu prawnego. Z tego też względu, istotnego znaczenia nabiera ich dokładna analiza i dostosowanie obecnej polityki przetwarzania danych osobowych do nowych ram prawnych.



**Autor:**  
**Piotr Gajlewicz**



**Autor:**  
**Szymon Romanowicz**