WKB
WIERCIŃSKI KWIECIŃSKI BAEHR

ALERT PRAWNY

Nowe unijne rozporządzenie o ochronie danych osobowych przyjęte przez Radę i Parlament Europejski

15 kwietnia 2016 r., aktualizacja: 16 maja 2016 r.

Rozporządzenie przyjęte 14 kwietnia 2016 r. przez Parlament Europejski zacznie obowiązywać od 25 maja 2018 roku

Znamy już ostateczny kształt nowych unijnych przepisów o ochronie danych osobowych – **rozporządzenia (EU) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i swobodnym przepływem takich danych oraz uchylenia dyrektywy 95/46/WE** (zwane w skrócie **ogólnym rozporządzeniem o ochronie danych**, ang. *General Data Protection Regulation*). W kwietniu zakończył się trwający ponad 4 lata proces legislacyjny dotyczący rozporządzenia ogólnego – Komisja Europejska przedstawiła jego projekt w styczniu 2012 roku.

Tekst nowego rozporządzenia został opublikowany w Dzienniku Urzędowym UE 4 maja 2016 roku (link). **Rozporządzenie wchodzi zatem w życie 25 maja 2016 roku, a zaczyna obowiązywać od 25 maja 2018 roku.**

Poniżej przedstawiamy najważniejsze zmiany, jakie zostaną wprowadzone w nowym rozporządzeniu:

- **Dyrektywa 95/46/WE w sprawie przetwarzania danych osobowych zostanie uchylona, a w jej miejsce wejdzie właśnie rozporządzenie o ochronie danych, które jest stosowane bezpośrednio.** Co prawda rozporządzenie w kilkudziesięciu przypadkach przewiduje możliwość wprowadzenia przez państwa członkowskie pewnych wyjątków od jego przepisów, jednakże i tak dzięki nowemu rozporządzeniu dojdzie do bardzo istotnego ujednolicenia zasad przetwarzania danych osobowych w Unii Europejskiej. Będzie to z pewnością ułatwienie dla organizacji i przedsiębiorców prowadzących działalność na terenie kilku państw UE.
- Za niezgodne z prawem przetwarzanie danych osobowych będą grozić **kary finansowe w wysokości nawet do 20 mln euro albo do 4% rocznego światowego obrotu danego przedsiębiorstwa** (w zależności od tego, która liczba będzie wyższa). Tak wysokie kary będą nakładane m.in. za naruszenie podstawowych zasad przetwarzania danych osobowych, czyli na przykład za naruszenie praw osób, których dane są przetwarzane, np. prawa dostępu do treści danych, a także w przypadku niewykonania decyzji organu ochrony danych osobowych (w Polsce: GIODO). Nieco niższe kary, tj. maksymalnie do 10 mln euro albo do 2% rocznego światowego obrotu, będą grozić m.in. za niepoinformowanie organu ochrony danych o naruszeniu bezpieczeństwa danych osobowych (np. ich wycieku), za nieodpowiednie zabezpieczenie danych osobowych, a także za niewyznaczenie inspektora ochrony danych, jeżeli było to wymagane.
- **Rozporządzenie przewiduje też możliwość ubiegania się przez osobę, której dane dotyczą o odszkodowanie za szkody majątkowe lub niemajątkowe** wynikające z naruszenia przepisów rozporządzenia przez administratora danych lub podmiot przetwarzający.
- **Zniesiony będzie obowiązek zgłaszania zbiorów danych do rejestracji** organom ochrony danych osobowych – **zamiast tego administratorzy danych osobowych, a także podmioty przetwarzające dane, będą prowadzić rejestr czynności przetwarzania danych** zawierający między innymi informacje o administratorze danych, o celach przetwarzania, o odbiorcach danych osobowych (podmiotach, którym dane mogą być udostępnione), oraz ogólny opis technicznych i organizacyjnych środków bezpieczeństwa. Można się więc spodziewać, że wymogi dotyczące opisywania technicznych i organizacyjnych środków zabezpieczania danych osobowych nie będą już tak szczegółowe jak obowiązujące obecnie w Polsce przepisy o polityce bezpieczeństwa i instrukcji zarządzania systemem informatycznym służącym do przetwarzania danych osobowych (zawarte w rozporządzeniu Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i

organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych).

- W nowym rozporządzeniu o ochronie danych wprowadzony został **obowiązek informowania** organów ochrony danych osobowych **o naruszeniach ochrony danych osobowych**, czyli np. o ich przypadkowym ujawnieniu lub zniszczeniu. W szczególnych okolicznościach konieczne będzie także informowanie o tym osób, których dane dotyczą. Wówczas osobom tym powinny być przekazane m.in. informacje o możliwych konsekwencjach naruszenia ochrony danych oraz o podjętych lub sugerowanych przez administratora lub podmiot przetwarzający dane środkach mających na celu minimalizację negatywnych skutków naruszenia.
- **W niektórych sytuacjach obowiązkowe będzie wyznaczenie tzw. inspektora ochrony danych** (w polskim prawodawstwie zwanym dziś "**administratorem bezpieczeństwa informacji**") – **wymóg ten będzie dotyczył administracji publicznej** (z wyjątkiem sądów w zakresie orzekania), **a także niektórych podmiotów sektora prywatnego**: podmiotów przetwarzających dane wrażliwe na dużą skalę oraz podmiotów, których główna działalność związana jest z systematycznym monitorowaniem osób, których danych dotyczą na dużą skalę. Jeszcze w tym roku Grupa Robocza Artykułu 29 (organ doradczy składający się z organów ochrony danych z całej UE) ma wydać wskazówki dotyczące obowiązku powołania inspektora ochrony danych. Można się więc spodziewać wyjaśnień dotyczących nieco nieprecyzyjnych przesłanek powołania inspektora ochrony danych przez podmioty prywatne.
- Ponadto, **w szczególnych przypadkach obowiązkowe będzie przeprowadzenie tzw. oceny skutków dla ochrony danych** (ang. *data protection impact assessment*). Ocena skutków będzie przeprowadzana przed rozpoczęciem przetwarzania danych, jeżeli takie przetwarzanie może, ze względu na swój zakres, kontekst lub cele, potencjalnie zagrażać prywatności osób fizycznych. W rozporządzeniu jako przykłady takich okoliczności wskazane są: przetwarzanie na dużą skalę danych wrażliwych, systematyczne i kompleksowe profilowanie, które jest podstawą decyzji wywołujących skutki prawne wobec osób fizycznych oraz systematyczne monitorowanie na dużą skalę miejsc dostępnych publicznie. Wskazówki co do przesłanek i sposobu przeprowadzania oceny skutków ma w tym roku przedstawić wspomniana wyżej Grupa Robocza Artykułu 29.
- Pewnemu **rozszerzeniu ulegnie też obowiązek informacyjny wobec osób, których dane dotyczą** – oprócz informacji o celu przetwarzania danych, o odbiorcach danych i prawach dotyczących przetwarzania danych, administrator będzie musiał wskazać miedzy innymi: prawną podstawę przetwarzania danych, dane kontaktowe inspektora ochrony danych (o ile został powołany), kategorie przetwarzanych danych, przewidywany termin przechowywania danych osobowych.
- **Rozporządzenie wprowadza też nowy rodzaj uprawnienia osób, których dane są przetwarzane – prawo do przenoszenia danych** (ang. *data portability*). Oznacza to, że osoba, której dane dotyczą będzie mogła otrzymać swoje dane osobowe w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego. Następnie osoba ta będzie miała prawo przesłać swoje dane osobowe innemu administratorowi (np. innemu usługodawcy internetowemu). Dotyczy to sytuacji, w których przetwarzanie danych odbywa się w sposób zautomatyzowany, a podstawą prawną przetwarzania jest zgoda osoby, której dane dotyczą lub niezbędność przetwarzania danych do zawarcia lub wykonywania umowy.
- **Rozporządzenie nakłada obowiązki nie tylko na administratorów danych, ale także – w pewnych przypadkach – na podmioty przetwarzające** (tzw. procesorów, z ang. *processor*). Dotyczy to na przykład obowiązku prowadzenia rejestru czynności przetwarzania czy też powołania inspektora ochrony danych.
- **Zakres terytorialny nowego rozporządzenia o ochronie danych będzie szerszy niż w przypadku dyrektywy 95/46/WE.** Rozporządzenie znajdzie zastosowanie nie tylko wówczas, gdy przetwarzanie będzie miało związek z działalnością mieszczącej się na terytorium UE jednostki organizacyjnej administratora lub podmiotu przetwarzającego, ale także w odniesieniu do działalności organizacji spoza UE, o ile przetwarzanie danych osobowych będzie wiązało z oferowaniem towarów lub usług przebywającym na terytorium Unii osobom, których dane dotyczą lub z monitorowaniem ich zachowania, o ile do zachowania tego dochodzi w Unii. Oznacza to, że przepisów nowego rozporządzenia w pewnych przypadkach będą musiały przestrzegać podmioty

niemające oddziału lub przedstawicielstwa na terenie Unii – jeżeli przetwarzanie danych będzie dotyczyło osób przebywających na terytorium Unii Europejskiej.

Organizacje przetwarzające dane osobowe mają dwa lata na dostosowanie się do wymogów nowego rozporządzenia. Jednakże z uwagi na to, że zmiany są bardzo daleko idące, **już w najbliższym czasie warto podjąć pewne kroki w celu przygotowania się do nowych ram prawnych**, na przykład:

- **Sprawdzenie, czyje i jakie kategorie danych osobowych są przetwarzane przez organizację, w jakim celu, jakie są źródła danych i komu dane są przekazywane**. Warto także ustalić **podstawę prawną przetwarzania danych**. Zebranie tych informacji przyda się zarówno w przy redagowaniu nowego brzmienia klauzuli informacyjnej, jak i przy wdrażaniu wymogu prowadzenia rejestru operacji przetwarzania.
- Przygotowanie **nowej wersji klauzuli informacyjnej** przekazywanej osobom, których dane są przetwarzane, przy okazji zbierania lub pozyskiwania danych.
- Przygotowanie **wewnętrznej procedury dotyczącej zgłaszania** do organu nadzoru **naruszeń bezpieczeństwa danych osobowych** (np. nieuprawnionego ujawnienia lub przypadkowego usunięcia), a także informowania o tym osób, których dane dotyczą. W tym kontekście warto też zastanowić się nad procedurą monitorowania bezpieczeństwa danych osobowych i wykrywania naruszeń.
- Przygotowanie **wewnętrznych procedur dotyczących realizacji uprawnień osób, których dane są przetwarzane** – na wypadek wniosku o udostępnienie treści danych osobowych, żądania poprawienia lub usunięcia danych, czy też żądania otrzymania danych w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego (prawo do przenoszenia danych).
- Ustalenie, **czy w danej organizacji konieczne będzie wyznaczenie inspektora ochrony danych lub przeprowadzenie oceny skutków dla ochrony danych** (*data protection impact assessment*).

W przypadku jakichkolwiek dodatkowych pytań lub wątpliwości, pozostajemy do Państwa dyspozycji:

Agnieszka Wiercińska-Krużewska, Senior Partner
Prawo własności intelektualnej & TMT
Agnieszka.Wiercinska@wkb.com.pl

Katarzyna Syska, Associate
Prawo własności intelektualnej & TMT
Katarzyna.Syska@wkb.com.pl

Paulina Komorowska, Associate
Prawo własności intelektualnej & TMT
Paulina.Komorowska@wkb.com.pl