



Ochrona danych: Rada zatwierdza podejście ogólne

15 czerwca 2015 r. Rada wypracowała **podejście ogólne** względem **ogólnego rozporządzenia o ochronie danych**, które dostosowano do ery cyfrowej. Ma ono lepiej chronić dane osób fizycznych, a zarazem poszerzać możliwości biznesowe na jednolitym rynku cyfrowym.

Łotewski minister sprawiedliwości **Dzintars Rasnačs** powiedział: „dzisiaj **poczyniliśmy ogromny krok ku nowoczesnym, zharmonizowanym unijnym ramom ochrony danych**. Bardzo się cieszę, że po ponad 3 latach negocjacji udało nam się porozumieć w sprawie tego aktu. Nowe rozporządzenie o ochronie danych, dostosowane do potrzeb ery cyfrowej, **poszerzy prawa obywateli i zapewni wysoki standard ochrony**”.

Podejście ogólne oznacza, że Rada osiągnęła porozumienie polityczne, na podstawie którego może teraz rozpocząć negocjacje z Parlamentem Europejskim, by tym samym wypracować ogólne porozumienie w sprawie nowych unijnych przepisów o ochronie danych. **Pierwsze rozmowy trójstronne** z Parlamentem są zaplanowane na **24 czerwca 2015 r.**

„Dziękuję Parlamentowi Europejskiemu za gotowość rozpoczęcia rozmów **już w przyszłym tygodniu**. Mam nadzieję, że uda nam się szybko porozumieć, tak by nasi obywatele mogli już wkrótce cieszyć się efektami reformy” – powiedział **Dzintars Rasnačs**.

Luksemburg, obejmujący wkrótce prezydencję w Radzie, zapowiedział, że równoległe z negocjacjami nad rozporządzeniem przyspieszone zostaną prace nad dyrektywą o ochronie danych do celów egzekwowania prawa, tak by w październiku można było zatwierdzić podejście ogólne. Luksemburski minister sprawiedliwości **Félix Braz** powiedział: „ta reforma to pakiet. Jesteśmy zdecydowani zakończyć prace nad nim do końca tego roku”.

Główne punkty porozumienia

Większa ochrona danych

Dane osobowe muszą być zbierane i przetwarzane zgodnie z prawem, pod surowymi warunkami i w uzasadnionym celu. Aby móc przetwarzać dane osobowe, **administratorzy danych** (czyli osoby lub podmioty odpowiedzialne za przetwarzanie) muszą przestrzegać szczegółowych przepisów, np. wymogu uzyskania **jednoznacznej zgody od podmiotu danych** (czyli od osoby, której dane osobowe mają być przetwarzane).

Szersze **prawa ochrony danych** dadzą osobom fizycznym większą kontrolę nad własnymi danymi:

Łatwiejszy dostęp do danych

dokładniejsze informacje o tym, co dzieje się z przekazanymi przez nie danymi (administratorzy muszą przejrzystej wskazywać, co robią z danymi, np. **jasnym i prostym językiem** powiadamiać podmioty danych o realizowanej przez siebie strategii ochrony prywatności)

prawo do usunięcia danych osobowych i prawo do „bycia zapomnianym”: można np. zażądać od usługodawcy, by niezwłocznie usunął dane, jeżeli pozyskano je, gdy podmiot danych był dzieckiem

prawo do przenoszenia danych: łatwiej będzie przenosić swoje dane od jednego usługodawcy do innego (np. z jednej sieci społecznościowej do innej). To zaś zwiększy konkurencję wśród usługodawców

limitowane profilowanie: ograniczone zostanie automatyczne przetwarzanie danych służące ocenie danej osoby, np. efektów jej pracy, sytuacji ekonomicznej, zdrowia czy preferencji.

Podmiotom danych łatwiej będzie dochodzić swoich praw. Od każdej decyzji organu ochrony danych osoby takie będą się mogły odwołać do własnego sądu krajowego – bez względu na to, gdzie siedzibę ma administrator.

Szersze możliwości biznesowe na jednolitym rynku cyfrowym

Jednolity zestaw przepisów, obowiązujący w całej UE i mający zastosowanie zarówno do unijnych, jak i pozaunijnych firm oferujących swoje usługi internetowe w UE, sprawi, że transgranicznej wymiany danych nie będą zakłócać sprzeczne krajowe przepisy o ochronie danych. Ponadto intensywniejsza współpraca organów nadzorczych z państw członkowskich zapewni spójne stosowanie nowych przepisów w całej UE. To zaś będzie sprzyjać **uczciwej konkurencji** i zachęci przedsiębiorstwa, zwłaszcza małe i średnie, do jak najszerzego korzystania z **jednolitego rynku cyfrowego**.

Aby zmniejszyć koszty i zagwarantować pewność prawa, w **ważnych sprawach transgranicznych**, które dotyczą kilku krajowych organów nadzorczych, **podejmowana będzie jedna decyzja nadzorcza**. Ten **system kompleksowej obsługi**

pozwole przedsiębiorstwu mającemu oddziały w kilku państwach członkowskich ograniczyć kontakty tylko do organu ochrony danych z państwa członkowskiego, w którym ma siedzibę.

Aby zmniejszyć koszty dostosowywania się do nowych przepisów, administratorzy mogą – opierając się na ocenie zagrożeń, jakie niesie ich przetwarzanie danych osobowych – określić poziomy zagrożeń i wprowadzić środki im odpowiadające.

Liczniesze i lepsze narzędzia egzekwowania przepisów

Skuteczniejszemu egzekwowaniu nowych przepisów o ochronie danych sprzyjać będzie nałożona na administratorów większa odpowiedzialność, w tym odpowiedzialność prawna. **Administratorzy muszą wdrożyć odpowiednie środki bezpieczeństwa** i niezwłocznie informować o naruszeniu ochrony danych zarówno organ nadzorczy, jak i osoby znacznie poszkodowane w wyniku tego naruszenia. Administratorzy i podmioty przetwarzające mogą ustanowić w swojej strukturze inspektora ochrony danych. Co więcej, prawo Unii lub prawo krajowe może od nich tego wymagać.

Jeśli dojdzie do łamania przepisów o ochronie danych, podmioty danych oraz – pod pewnymi warunkami – organizacje ochrony danych mogą wnieść **skargę** do organu nadzorczego lub skierować sprawę na drogę sądową. Jeżeli zarzuty się potwierdzą, **administratorowi może grozić grzywna** w wysokości do 1 mln EUR lub 2% całkowitego rocznego obrotu.

Gwarancje w razie przekazywania danych osobowych poza UE

Ochrona danych osobowych przekazywanych do państw trzecich i organizacji międzynarodowych jest gwarantowana **decyzją stwierdzającą odpowiedni poziom ochrony**. Komisja z pomocą państw członkowskich i Parlamentu Europejskiego może zdecydować, że poziom ochrony danych przewidziany w danym państwie trzecim lub danej organizacji międzynarodowej jest odpowiedni. Jeżeli decyzja taka nie zapadnie, dane mogą być przekazywane wyłącznie wtedy, gdy istnieją odpowiednie zabezpieczenia (standardowe klauzule ochrony danych, wiążące reguły korporacyjne czy klauzule umowne).

[Ogólne rozporządzenia o ochronie danych \(podejście ogólne\)](#)

Press office - General Secretariat of the Council

Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319

press.office@consilium.europa.eu - www.consilium.europa.eu/press