Rada UE

PRESS
PL

KOMUNIKAT PRASOWY
951/15
18.12.2015

Reforma ochrony danych w UE: Rada potwierdza porozumienie z Parlamentem Europejskim

18 grudnia 2015 r. Komitet Stałych Przedstawicieli (Coreper) potwierdził teksty kompromisowe w sprawie reformy ochrony danych uzgodnione z Parlamentem Europejskim. 15 grudnia osiągnięto porozumienie między Radą, Parlamentem i Komisją. Porozumienie to jest zgodne z postulatem Rady Europejskiej dotyczącym zakończenia negocjacji w sprawie reformy ochrony danych przed końcem 2015 r.

Félix BRAZ, minister sprawiedliwości Luksemburga, a zarazem przewodniczący Rady powiedział: „To niezwykle ważne porozumienie o donośnych konsekwencjach. Reforma nie tylko wzmacnia prawa obywateli, lecz także dostosowuje przepisy dotyczące przedsiębiorstw do epoki cyfrowej,a równocześnie ogranicza obciążenia administracyjne. Porozumienie dotyczy ambitnych dokumentów wybiegających w przyszłość. Możemy być całkiem spokojni co do wyników reformy."

Reforma ochrony danych ma się dokonać dzięki pakietowi legislacyjnemu zaproponowanemu przez Komisję w 2012 r., którego celem jest aktualizacja i unowocześnienie przepisów o ochronie danych. Obejmuje on dwa instrumenty: ogólne rozporządzenie o ochronie danych (które ma zastąpić dyrektywę 95/46/WE) oraz dyrektywę o ochronie danych przy ściganiu przestępstw (która ma zastąpić decyzję ramową w sprawie ochrony danych z 2008 r.).

Ochrona osób w związku z przetwarzaniem ich danych osobowych jest prawem podstawowym przewidzianym w Karcie praw podstawowych UE (art. 8) i w Traktacie o funkcjonowaniu Unii Europejskiej (art. 16).

Ogólne rozporządzenie o ochronie danych

Ogólne rozporządzenie o ochronie danych ma na celu zwiększenie poziomu ochrony osób fizycznych, których dane osobowe są przetwarzane, oraz zwiększenie możliwości biznesowych na jednolitym rynku cyfrowym, m.in. poprzez zmniejszenie obciążeń administracyjnych.

Większa ochrona danych

Zasady i przepisy dotyczące przetwarzania danych osobowych osób fizycznych muszą respektować podstawowe prawa i wolności, szczególnie prawo do ochrony danych osobowych. Wzmocnienie praw do ochrony danych daje osobom, których dane te dotyczą (czyli osobom, których dane są przetwarzane), większą kontrolę nad swoimi danymi osobowymi. Konkretnie przewidziano:

- bardziej szczegółowe przepisy dotyczące przetwarzania danych osobowych przez administratorów danych (czyli osoby odpowiedzialne za przetwarzanie danych), w tym wymóg uzyskania zgody zainteresowanego
- łatwiejszy dostęp do własnych danych osobowych
- pełniejsze informacje na temat tego, co się dzieje z danymi osobowymi, gdy zostają udostępnione. Obejmuje to informowanie obywateli o polityce ochrony prywatności w sposób jasny i łatwo zrozumiały; informacje te mogą również być przekazywane za pośrednictwem ustandaryzowanych ikon
- prawo do usunięcia danych i do „zostania zapomnianym". Pozwala to osobom, których dotyczą dane, na przykład wymagać niezwłocznego usunięcia ich danych osobowych gromadzonych lub publikowanych na portalach społecznościowych, gdy dana osoba była jeszcze dzieckiem
- jeżeli młoda osoba poniżej 16 roku życia chce korzystać z usług internetowych, usługodawca musi starać się zweryfikować, czy rodzice udzielili na to zgody. Państwa członkowskie mogą obniżyć ten limit wiekowy do 13 lat
- prawo do przenoszenia danych: łatwiej będzie przenosić swoje dane od jednego usługodawcy do innego (np. z jednej sieci społecznościowej do innej). Doprowadzi to nie tylko do wzmocnienia praw do ochrony danych, ale także zwiększy konkurencję między usługodawcami
- prawo do wniesienia sprzeciwu wobec przetwarzania danych osobowych odnoszących się do interesu publicznego lub do uzasadnionego interesu administratora danych. Prawo to obejmuje wykorzystywanie danych osobowych do celów „profilowania"
- wspólne zabezpieczenia prawne obejmujące przetwarzanie danych osobowych do celów archiwizacyjnych, jeżeli leży to w interesie publicznym, oraz w celach naukowych i historycznych, a także statystycznych.

Aby zagwarantować geograficzną bliskość podczas dochodzenia swoich praw, osobom, których dotyczą dane, przysługuje prawo do odwoływania się od decyzji organu ochrony danych do własnego sądu krajowego – bez względu na to, gdzie siedzibę ma administrator danych.

Szersze możliwości biznesowe w ramach jednolitego rynku cyfrowego

W rozporządzeniu przewiduje się jednolity zbiór przepisów obowiązujący w całej UE i mający zastosowanie zarówno do europejskich, jak i pozaeuropejskich przedsiębiorstw oferujących usługi on-line w UE. Pozwala to uniknąć sytuacji, w których sprzeczne krajowe przepisy dotyczące ochrony danych mogłyby zakłócać transgraniczną wymianę danych. Rozporządzenie przewiduje również ściślejszą współpracę między państwami członkowskimi, aby zapewnić spójne stosowanie przepisów o ochronie danych w całej UE. To zaś będzie sprzyjać uczciwej konkurencji i zachęci przedsiębiorstwa, zwłaszcza małe i średnie, do jak najszerszego 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 **mechanizm kompleksowej obsługi** pozwoli przedsiębiorstwu, które prowadzi działalność w kilku państwach członkowskich, kontaktować się wyłącznie z organem ochrony danych w państwie członkowskim swojej podstawowej siedziby. Mechanizm ten przewiduje również w przypadku sporów jedną decyzję mającą zastosowanie do całego terytorium UE.

Mając na celu zmniejszenie kosztów administracyjnych, w rozporządzeniu zastosowano podejście oparte na ryzyku: administratorzy danych mogą stosować środki uzależnione od ryzyka związanego z operacjami przetwarzania danych, jakie przeprowadzają. Różne przedsiębiorstwa prowadzą różne rodzaje działalności i zagrożenia pod względem ochrony prywatności związane z ich działalnością mogą się różnić. Rozporządzenie nie zapewnia jednolitego rozwiązania dla wszystkich: przeciwnie, im większe zagrożenie dla ochrony danych osobowych stwarza dana działalność, tym bardziej restrykcyjne dotyczą jej zobowiązania.

Liczniejsze i lepsze narzędzia egzekwowania przepisów dotyczących ochrony danych

Rozporządzenie zawiera szereg środków mających na celu zwiększenie odpowiedzialności i rozliczalności administratorów danych, by zapewnić pełną zgodność z nowymi przepisami o ochronie danych. Administratorzy danych muszą wdrożyć pewne środki bezpieczeństwa, w tym dostosować się do wymogu powiadamiania w określonych przypadkach o naruszeniu ochrony danych osobowych. Aby nadać rozporządzeniu dalekosiężny charakter, została wprowadzona zasada ochrony danych już w fazie projektowania oraz jako zasada domyślnej ochrony danych. Organy publiczne i przedsiębiorstwa, które wykonują niektóre ryzykowne operacje przetwarzania danych, muszą wyznaczyć **inspektora ochrony danych**, aby zapewnić zgodność z przepisami.

Jeśli dojdzie do naruszenia przepisów o ochronie danych, osoby, których dotyczą dane, oraz – pod pewnymi warunkami – organizacje ochrony danych mogą wnieść skargę do organu nadzorczego lub skierować sprawę na drogę sądową. Administratorzy danych mogą zostać ukarani grzywną do wysokości 20 mln EUR lub 4% ich całkowitego rocznego obrotu.

Gwarancje w razie przekazywania danych osobowych poza UE

Rozporządzenie ustanawia przepisy dotyczące przekazywania danych osobowych do państw trzecich i organizacji międzynarodowych. Przekazywanie może mieć miejsce, o ile spełnionych zostanie szereg warunków i gwarancji, a w szczególności jeżeli Komisja podjęła decyzję stwierdzającą, że zapewniono odpowiedni poziom ochrony. Nowe decyzje stwierdzające odpowiedni poziom ochrony danych będą musiały zostać poddane przeglądowi przynajmniej raz na 4 lata. Obowiązujące decyzje i zezwolenia stwierdzające odpowiedni poziom ochrony danych pozostają w mocy do czasu ich zmiany, zastąpienia lub uchylenia.

Dyrektywa o ochronie danych przy ściganiu przestępstw

Dyrektywa ma chronić dane osobowe przetwarzane do celów zapobiegania przestępstwom, prowadzenia dochodzeń w ich sprawie, ich wykrywania, i ścigania, wykonywania sankcji karnych, a także do celów ochrony przed zagrożeniami dla bezpieczeństwa publicznego i zapobiegania takim zagrożeniom.

Należy zapewnić wysoki i spójny poziom ochrony danych osobowych osób fizycznych przy jednoczesnym ułatwieniu wymiany danych osobowych między organami egzekwowania prawa w poszczególnych państwach członkowskich.

Szerszy zakres stosowania

Oprócz działań zmierzających do zapobiegania przestępstwom, ich wykrywania, prowadzenia dochodzeń w ich sprawie oraz ścigania tych przestępstw, zakres stosowania nowej dyrektywy został rozszerzony na ochronę i zapobieganie zagrożeniom dla bezpieczeństwa publicznego.

Nowa dyrektywa stosowałaby się do transgranicznego przetwarzania danych osobowych oraz do ich przetwarzania przez policję i organy sądowe na szczeblu wyłącznie krajowym. Decyzja ramowa, którą ma zastąpić, dotyczyła wyłącznie transgranicznej wymiany danych.

Prawa osób, których dotyczą dane

Nowe przepisy zachowują równowagę między prawem do prywatności a koniecznością nieujawniania przez policję informacji o przetwarzaniu danych na wczesnym etapie dochodzenia. Niemniej dokument zawiera wykaz informacji, do których otrzymania

osoba, której dane te dotyczą, jest zawsze uprawniona, aby mogla ona chronić swoje prawa, jeżeli obawia się, że miało miejsce naruszenie.

Nowe przepisy nadal obejmowałyby przekazywanie danych osobowych państwom trzecim i organizacjom międzynarodowym.

Przestrzeganie przepisów

Nowa dyrektywa przewiduje mianowanie **inspektora ochrony danych** , który ma wspomagać właściwe organy w zapewnianiu przestrzegania przepisów o ochronie danych.

Innym narzędziem zapewnienia zgodności z przepisami jest ocena wpływu. Jeżeli przetwarzanie danych może stwarzać wysokie zagrożenie dla praw i wolności poszczególnych osób, właściwe organy muszą przeprowadzić ocenę potencjalnego wpływu danego przetwarzania, w szczególności przy wykorzystaniu nowych technologii.

Monitorowanie i odszkodowania

Tekst dyrektywy został dostosowany do tekstu powiązanego rozporządzenia w celu dopilnowania, by generalnie miały zastosowanie te same zasady ogólne. Ponadto przepisy dotyczące organu nadzorczego są w dużym stopniu podobne, ponieważ organ nadzoru ustanowiony w ogólnym rozporządzeniu o ochronie danych może również zajmować się sprawami wchodzącymi w zakres dyrektywy. Nowa dyrektywa przyznawałaby również osobom, których dane są przetwarzane, prawo do odszkodowania, gdyby osoby te doznały szkody na skutek przetwarzania danych niezgodnego z przepisami.

DALSZE DZIAŁANIA

17 grudnia podczas nadzwyczajnego posiedzenia Komisja Parlamentu Europejskiego ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE) zatwierdziła teksty uzgodnione w trakcie rozmów trójstronnych. Poparcie to pozwoliło dziś Coreperowi potwierdzić ostateczne kompromisowe brzmienie rozporządzenia i dyrektywy. Po weryfikacji prawno-językowej teksty aktów zostaną przedłożone do przyjęcia przez Radę, a w następnej kolejności – przez Parlament. Rozporządzenie i dyrektywa prawdopodobnie wejdą w życie wiosną 2018 roku.

Press office - General Secretariat of the Council of the EU
Rue de la Loi 175 - B-1048 BRUSSELS - Tel.: +32 (0)2 281 6319
press@consilium.europa.eu - www.consilium.europa.eu/press