Czy jesteś gotowy na RODO?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

10. Ocena skutków dla ochrony danych

Nowa, przyjęta w ogólnym rozporządzeniu o ochronie danych, filozofia ochrony danych osobowych zakłada odejście od konieczności zgłaszania i rejestracji zbiorów. Zastępuje ją natomiast obowiązkiem przeprowadzenia oceny skutków dla ochrony danych. Ocena ta powinna obejmować przede wszystkim planowane operacje i cele przetwarzania, zabezpieczenia i mechanizmy mające minimalizować ryzyko. Ten istotny dla rozliczalności proces ma prowadzić do opisania przetwarzania danych, oceny jego niezbędności i proporcjonalności, a także pomóc we właściwym zarządzaniu (przeciwdziałaniu) ryzykami wynikającymi z przetwarzania danych.

Przeprowadzenie takiej oceny będzie wymagane, jeśli operacje przetwarzania danych mogą powodować wysokie ryzyko naruszenia prywatności osób, których dane dotyczą, np. w sytuacji:

- kiedy działania na danych dokonywane są przy użyciu nowych technologii,
- użycia zautomatyzowanych procesów przetwarzania danych, w tym profilowania,
- przetwarzania na dużą skalę szczególnych kategorii danych (danych wrażliwych, takich jak dane biometryczne czy dane na temat stanu zdrowia).

W przypadku gdy administrator danych nie może w wystarczającym stopniu zniwelować zidentyfikowanego ryzyka (znaleźć wystarczających środków) lub mimo zastosowania środków, ryzyko nadal jest wysokie, konieczna będzie konsultacja z GIODO. Jest więc oczywiste, że tego typu ocena musi pojawić się na etapie projektowania – jej wynik prowadzi bowiem do decyzji, czy przetwarzanie danych w zakładany sposób wymagać będzie uprzedniej konsultacji z GIODO. Pamiętać jednak należy, że ocena skutków jest procesem ciągłym, wymagającym aktualizacji.

Co ciekawe, rozporządzenie przewiduje, że w określonych przypadkach konieczne może być konsultowanie zamiaru przetwarzania danych osobowych z osobami, których dane dotyczą lub ich przedstawicielami – np. poprzez formalne pytanie do przedstawicieli pracowników czy też badanie przesłane klientom.

A co z już prowadzonymi operacjami przetwarzania danych? Ocena skutków dla ochrony danych niezbędna będzie dopiero dla operacji rozpoczętych po 25 maja 2018 r. lub dotychczasowych operacji znacząco zmienionych po tej dacie - na przykład ponieważ została wprowadzona do użytku nowa technologia lub ponieważ dane osobowe są wykorzystywane w innym celu. GIODO zdecydowanie zaleca jednak dokonanie oceny skutków dla wszystkich trwających już operacji przetwarzania danych spełniających kryteria wskazane w art. 35 rozporządzenia. Warto więc już teraz zacząć analizować okoliczności, w których prowadzone przez Ciebie operacje będą wymagały dokonania takiej oceny. Zastanów się, kto w Twojej organizacji jej dokona oraz kto powinien być w ten proces zaangażowany (zasięganie opinii niezależnych ekspertów).

Rozporządzenie identyfikuje także problem oceny skutków dla ochrony danych dla operacji prowadzonych przez podmioty sektora publicznego, w sytuacji kiedy podstawą przetwarzania danych osobowych jest przepis prawa lub interes publiczny. W tej sytuacji ocena skutków powinna zostać przeprowadzona w ramach oceny skutków regulacji (OSR) dla aktu prawnego stanowiącego podstawę dla takiego przetwarzania.

Ocena skutków musi być realną oceną ryzyk, umożliwiającą administratorom podejmowanie działań mających na celu ich rozwiązanie. Ogólne rozporządzenie zapewnia administratorom danych elastyczność w wykorzystaniu różnych narzędzi służących do przeprowadzenia tej oceny. Więcej praktycznych informacji na ten temat znajdziesz w przygotowanych przez GIODO i Grupę Roboczą Art. 29 Wytycznych WP 248 dotyczących oceny skutków dla ochrony danych (DPIA) dostępnych na stronie internetowej GIODO w zakładce „Reforma przepisów".