OCENA SKUTKÓW DLA OCHRONY DANYCH - DATA PROTECTION IMPACT ASSESSMENT

12.10.2017

Rok 2017 to okres przygotowywania organizacji na nowe przepisy dotyczące ochrony danych osobowych, jakie wprowadza od maja 2018 unijne rozporządzenie o ochronie danych osobowych (RODO).
Choć termin wydaje się wciąż odległy, jest to tylko złudzenie. Czasu jest mało, szczególnie jeśli weźmiemy pod uwagę skalę wyzwań, jakie stawiane są przed podmiotami przetwarzającymi dane osobowe.

Dokonywanie oceny skutków dla ochrony danych (Data Protection Impact Assessment, DPIA), jest jednym z nowych obowiązków ciążących na administratorze danych a wynikającym bezpośrednio z artykułu 35. RODO. Głównym celem DPIA jest zapewnienie zgodności procesów przetwarzania danych osobowych z unijnym rozporządzeniem. Ponieważ niektóre rodzaje przetwarzania mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem operacji przetwarzania danych, powinien dokonać oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Ryzyko może być zauważalne na wielu płaszczyznach, takich jak cel przetwarzania, charakter samych danych, ich zakres czy wreszcie kontekst. W dniu 4 kwietnia 2017 roku, Grupa Robocza Art.29 wydała wytyczne pozwalające podmiotom przetwarzającym dane zrozumieć, kiedy ryzyko naruszenia praw lub wolności osób fizycznych jest wysokie.

Przedstawiono między innymi następujące kryteria przesłanek do zastosowania DPIA;

- czy przetwarzane dane podlegają profilowaniu?
- czy przetwarzanie danych obejmuje automatyczne podejmowanie decyzji, które wywierają znaczący wpływ na prawa osób, których dotyczą?
- czy wykonywany jest systematyczny monitoring na dużą skalę miejsc dostępnych publicznie?
- czy przetwarzane są dane szczególnych kategorii, dane wrażliwe?
- czy dane przetwarzane są na dużą skalę?
- czy zbiory danych są łączone?
- czy dane są przetwarzane z wykorzystaniem innowacyjnych technologii lub z wykorzystaniem innowacyjnych środków organizacyjnych, użycie biometrii etc.?
- czy dane są przekazywane poza UE?

Wytyczne wskazują również, że w celu zastosowania mechanizmów wynikających z art. 35 RODO należy spełnić przynajmniej dwie z wymienionych w dokumencie przesłanek. Czasami jednak w przypadku spełnienia tylko jednej przesłanki możliwe będzie zastosowanie oceny skutków ochrony danych pod warunkiem, że będzie to wystarczająco uzasadnione. Grupa Robocza Art.29, rekomenduje, by dokonywać DIPA w procesie przetwarzania danych już w chwili obecnej, nie czekając na dzień 25 maja 2018 roku. Dokument z wytycznymi i kryteriami, Grupy Roboczej Art.29 jest dostępny na oficjalnym portalu Unii Europejskiej.

Każda instytucja przetwarzająca dane osobowe musi stworzyć sformalizowaną i udokumentowaną ocenę skutków ochrony danych osobowych. Taki dokument zawierać ma przynajmniej systematyczny i dokładny opis celów przetwarzania danych, a także wszelkich planowanych operacji z tym przetwarzaniem związanych w tym prawnie uzasadnionych interesów realizowanych przez administratora. Dokument musi zawierać informację, czy przetwarzanie danych faktycznie jest proporcjonalne i niezbędne do tego by osiągnąć zakładane cele. Dodatkowo koniecznym jest oszacowanie ryzyka naruszenia praw i wolności osób, których dane są przetwarzane. W dokumencie należy również przedstawić jakie środki są planowane w celu likwidacji podatności na naruszenia w przypadku każdego konkretnego ryzyka. Koniecznym jest dokonywanie czasowych audytów tych ryzyk, tak by w przypadku wykrycia nowego zagrożenia, zastosować niezbędne dla zapewnienia bezpieczeństwa środki. Dokument taki musi zostać stworzony przez administratora danych w konsultacji z działającym w organizacji Inspektorem Ochrony Danych, jeśli został on powołany. Przed rozpoczęciem przetwarzania danych, czasem również wymagana będzie uprzednia konsultacja z organem nadzorczym (obecnie GIODO, od maja 2018 Prezes Urzędu Ochrony Danych Osobowych). Będzie tak, jeśli ocena wskaże, że przy braku zabezpieczeń odpowiednich środków bezpieczeństwa oraz mechanizmów minimalizujących ryzyko przetwarzanie powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych i dodatkowo administrator wyraża opinię, że ryzyka tego nie da się zminimalizować środkami rozsądnymi z punktu widzenia dostępnych technologii i kosztów wdrożenia. Jeżeli w trakcie konsultacji organ nadzorczy wyrazi zdanie, że planowane przetwarzanie danych stanowi naruszenie przepisów RODO, wyda odpowiednie zalecenia dla podmiotu przetwarzającego dane.

> KAŻDA INSTYTUCJA PRZETWARZAJĄCA DANE OSOBOWE MUSI STWORZYĆ SFORMALIZOWANĄ I UDOKUMENTOWANĄ OCENĘ SKUTKÓW OCHRONY DANYCH OSOBOWYCH.

Istnieją jednak wyjątki, kiedy organizacja nie musi stosować DPIA. Obowiązek ten nie zachodzi gdy;

- operacja jest niezbędna dla wypełnienia obowiązku prawnego, który ciąży na administratorze danych,
- operacja jest niezbędna do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi i ma podstawę prawną w prawie Unii lub w prawie państwa członkowskiego, któremu podlega administrator danych.

Podsumowując należy pamiętać, że ocena skutków ochrony danych jeśli jest wykonana w fazie projektowania systemu pomaga nie tylko zidentyfikować możliwe ryzyka dla procesu przetwarzania, ale też wdrożyć najwyższe standardy prywatności i ochrony danych już we wczesnych stadiach jego realizacji, co jest korzystne dla całego systemu i w przypadku zastosowania odpowiednich środków zabezpieczających minimalizuję możliwość naruszenia danych, a w wypadku gdy takie naruszenie mimo wszystko nastąpi, pozwala uniknąć wysokich kar administracyjnych nakładanych przez organ nadzorczy (nawet 20 mln euro).

Autor: Cyprian Gutkowski

Kierownik Projektu
Fundacja Bezpieczna Cyberprzestrzeń

Śledź na:
TT: @cybsecurity_org
Facebook: **@FundacjaBezpiecznaCyberprzestrzen**