Czy jesteś gotowy na RODO?

GIODO
Generalny Inspektor Ochrony Danych Osobowych

9. Privacy by design i Privacy by default

Zawsze, gdy decydujesz się przetwarzać dane osobowe, dobrą praktyką powinno być podejście oparte na poszanowaniu prywatności osób, których te dane dotyczą. Zakłada ono, że ochrona prywatności powinna być brana pod uwagę i stosowana w praktyce przy prowadzeniu wszelkich projektów i działań, tak w sferze publicznej, jak i prywatnej. Tak rozumiana koncepcja privacy by design – jako część każdego podejmowanego projektu, niezależnie od jego charakteru i celu– została sformułowana wiele lat temu przez Ann Cavoukian – b. rzeczniczkę ds. informacji i prywatności kanadyjskiej prowincji Ontario – jako wynik wieloletnich prac nad wprzęgnięciem zasad ochrony prywatności do nowych projektów infrastrukturalnych realizowanych w Kanadzie.

Ogólne rozporządzenie o ochronie danych czyni tę koncepcję prawnie wiążącym obowiązkiem, wprowadzając do porządku prawnego uwzględnianie ochrony danych w fazie projektowania oraz – jako pewnego rodzaju jeden z szerszych postulatów privacy by design – zasadę domyślnej ochrony danych.

Uwzględnianie ochrony danych w fazie projektowania ma z zasady umożliwić włączanie ochrony prywatności w samo tworzenie projektu, działanie jego składników oraz w zarządzanie technologiami informacyjnymi i systemami przez cały cykl życia informacji. To proaktywne podejście wyrażone przez zasadę privacy by design zakłada, że ochrona prywatności powinna być wbudowana w każdy nowy projekt – co oznacza, że prywatność będzie chroniona nie poprzez dodatki do systemu lub nakładki przygotowane na już istniejące rozwiązania, lecz jest wbudowana w jego konstrukcję tak, że jest po prostu składową projektu. W przypadku systemów teleinformatycznych oznacza to wbudowanie ochrony prywatności zarówno w architekturę systemu, jak i w procesy biznesowe, które system obsługuje – np. poprzez jak najszybszą pseudonimizację danych czy też umożliwienie osobie, której dane dotyczą, monitorowania przetwarzania danych.

Uwzględnianie ochrony danych w fazie projektowania może być dużym wyzwaniem w sektorze publicznym. Wskazane byłoby wbudowanie ochrony prywatności w konstrukcje instrukcji kancelaryjnych. Co więcej, rozporządzenie wprost wskazuje również, że „zasadę uwzględniania ochrony danych w fazie projektowania i zasadę domyślnej ochrony danych należy też brać pod uwagę w przetargach publicznych". Innym wyzwaniem będzie też realizacja tej zasady w procesie legislacyjnym. Dobrym rozwiązaniem wydaje być wbudowanie privacy by design poprzez włączenie oceny skutków projektowanego aktu prawnego dla ochrony danych do przygotowywanej w procesie legislacyjnym oceny skutków regulacji (OSR).

Zasadę domyślnej ochrony danych należy natomiast rozumieć jako postulat uwzględnienia jak najdalej posuniętych zabezpieczeń prywatności w ustawieniach początkowych każdego systemu. Domyślnie, czyli bez konieczności jakiejkolwiek aktywności osób, których dane dotyczą – i to w kluczowym dla użytkownika momencie przyłączenia się do danego systemu. Co więcej, domyślnie powinny być przetwarzane tylko te dane, które są niezbędne do osiągnięcia celu, dla którego zostały zebrane (minimalizacja danych).

Warto więc już teraz dokonać przeglądu używanych systemów i narzędzi przetwarzania danych pod kątem realizacji ww. zasad, by mieć pewność, że 25 maja 2018 r. będziesz w stanie wykazać zgodność wszystkich działań na danych osobowych z wymogami ogólnego rozporządzenia.