

Będzie wiadomo, kiedy należy analizować ryzyko

RODO

Sławomir Wikariak
slawomir.wikariak@infor.pl

Wypuszczenie na patrol policjantów z kamerami czy wprowadzenie odcinkowego pomiaru prędkości to przykłady działań, które będą wymagały przeprowadzenia oceny skutków dla ochrony danych osobowych.

Wśród nowych obowiązków, które narzuca unijne rozporządzenie 2016/679 o ochronie danych osobowych (RODO), pojawia się konieczność przeprowadzania przez administratorów tzw. ocen skutków dla ochrony danych osobowych (ang. Data Protection Impact Assessment; dalej: DPIA). Będą one obligatoryjne wszędzie tam, gdzie pojawi się ryzyko naruszenia praw lub wolności osób.

Skąd czerpać wiedzę, czy dany sposób przetwarzania danych wymaga DPIA? Z pomocą ma przyjść wykaz przygotowywany przez generalnego inspektora ochrony danych osobowych. Wczoraj na stronie internetowej został opublikowany jego projekt.

– W ten sposób rozpoczęliśmy konsultacje społeczne. Do 30 kwietnia czekamy na uwagi wszystkich zainteresowanych. Chcielibyśmy, aby każdy mógł przedstawić swe stanowisko – powiedziała wczoraj dr Edyta Bielak-Jomaa, GIODO. Liczy ona szczególnie na udział w konsultacjach ekspertów z różnych sektorów i środowisk: prawników, informatyków, ekspertów do spraw bezpieczeństwa, socjologów czy etyków.

Wstępny wykaz zawiera 10 rodzajów przetwarzania danych, które wymagają przeprowadzenia DPIA. Dla przykładu – pierwszy z nich to profilowanie, które może wywoływać negatywne skutki prawne, fizyczne, finansowe lub inne. GIODO wskazuje tu na profilowanie osób bezrobotnych bez ich zgody, pod kątem dostępu do różnych form pomocy, ale również profilowanie użytkowników portali społecznościowych w celu wysyłania im spamu. Innym przykładem może być ocena stylu życia (np. odżywiania się, sposobu spędzania czasu) klientów firm ubezpieczeniowych, która może prowadzić do podwyższenia składki ubezpieczeniowej, czy nawet profilowanie pośrednie polegające na przypisaniu osoby do określonej grupy w celu przedstawie-

nia korzystniejszej oferty (np. ubezpieczenie dla nauczycieli). Innym rodzajem przetwarzania wymagającym przeprowadzenia oceny może być zautomatyzowane podejmowanie decyzji wywołujących skutki prawne. Tu GIODO jako przykład podaje nie tylko drogi objęte odcinkowym pomiarem prędkości, ale również te wyposażone w system elektronicznego poboru opłat viaTOLL. Przeprowadzenia DPIA będzie też wymagało zapowiadane wyposażenie policjantów w minikamery rejestrujące dokonywane czynności. Konieczna będzie chociażby ocena sposobu transmisji czy przechowywania filmów oraz dostępu do nich.

Przeprowadzenie DPIA może nie być łatwe. Powód? Niewielu jest ekspertów, którzy mogą się podjąć tego zadania. Zdecydowana większość administratorów sama zaś mu nie poddała.

– Konieczne jest przeprowadzenie analizy ryzyka, której ostateczny wynik jest w rzeczywistości iloczynem tego, z jak poważnym zagrożeniem mamy do czynienia, i tego, jak często może ono wystąpić. Zainfekowanie systemu komputerowego szpitala w wyniku głośnego ataku wirusem typu ransomware może być przykładem najpoważniejszego z możliwych zagrożeń. Nie mając dostępu do dokumentacji medycznej pacjenta, nie będzie można przeprowadzić operacji, co grozi jego śmiercią – mówi Maciej Gawroński, partner zarządzający w kancelarii Gawroński & Partners s.k.a.

Jeśli chodzi o rozwiązania stosowane przed 25 maja, kiedy to zaczną być stosowane RODO, to teoretycznie nie powinny one podlegać obowiązkowi przeprowadzania DPIA. W praktyce może się jednak okazać, że będą. Wystarczy, że zmieni się rodzaj ryzyka.

„Wymóg przeprowadzenia oceny skutków dla ochrony danych dotyczy istniejących operacji przetwarzania, które ze względu na użycie nowych technologii, zakres i kategorie przetwarzania mogą powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych oraz w przypadku których nastąpiła zmiana rodzaju ryzyka, z uwzględnieniem charakteru, zakresu, kontekstu i celów przetwarzania” – podkreśla GIODO.



Więcej na
www.gazeta-prawna.pl