

PYTANIA DO EKSPERTA

Prowadzona obecnie dokumentacja może być wykorzystywana

Czy polityki bezpieczeństwa i instrukcje zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, przygotowane zgodnie z dotychczas obowiązującymi przepisami, będą mogły być przez przedsiębiorców dostosowane do wymagań RODO?

Obecnie stosowana dokumentacja przetwarzania danych w bardzo szerokim zakresie może być wykorzystana również po wejściu do stosowania przepisów ogólnego rozporządzenia o ochronie danych (RODO). Przepisy te bowiem – poza wprost wskazanym obowiązkiem prowadzenia rejestru czynności przetwarzania i raportem z oceny skutków dla ochrony danych, których określono niezbędną zawartość – nie narzucają wymagań w zakresie sposobu dokumentowania stosowanych procedur czy środków bezpieczeństwa. Dlatego obecnie prowadzona dokumentacja, na którą składają się polityka bezpieczeństwa i instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych, z powodzeniem może być wykorzystana w celu stworzenia dokumentacji, której celem będzie wykazanie zgodności realizowanych procesów przetwarzania z wymaganiami RODO. Obowiązek prowadzenia takiej dokumentacji wynika z art. 24 RODO, który stanowi,



DR ANDRZEJ KACZMAREK

dyrektor departamentu informatyki
w Biurze Generalnego Inspektora Ochrony
Danych Osobowych

że administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z RODO i aby móc to wykazać. Opracowana w powyższy sposób dokumentacja powinna zatem opisywać zastosowane w powyższym celu procedury i środki techniczne.

Przepisy obecnie obowiązującej ustawy o ochronie danych osobowych oraz rozporządzenia ministra spraw wewnętrznych i administracji z 29 kwietnia 2004 r. w sprawie

dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, RODO natomiast – poza wymaganiami dotyczącymi zawartości rejestru czynności przetwarzania i raportu z oceny skutków – daje administratorom pełną swobodę. Nawet wprost nie ustanawia obowiązku prowadzenia czy posiadania dokumentacji przetwarzania danych osobowych, nie wspominając już o wymaganiach dotyczących jej zawartości. Jednak nie oznacza to, że dokumentacja przetwarzania danych osobowych po rozpoczęciu stosowania RODO nie będzie wymagana.

Jak GIODO będzie sprawdzać, czy administrator jest organizacyjnie przygotowany do spełniania wymagań RODO?

Zgodnie z RODO sprawdzenia dotyczące organizacyjnego przygotowania się administratorów danych do przetwarzania danych osobowych z uwzględnieniem zasad określonych w tym akcie prawnym będą wykonywane przez

GIODO z wykorzystaniem przysługujących mu narzędzi i w toku realizacji zadań wskazanych w art. 57 i 58 RODO. Wśród nich wymienić można m.in.:

- monitorowanie i egzekwowanie stosowania przepisów RODO,
- prowadzenie postępowań w związku z rozpatrywaniem skarg oraz informacji otrzymanych od innych organów nadzorczych,
- prowadzenie postępowań w formie audytów ochrony danych,
- dokonywanie przeglądu udzielonych certyfikacji.

Niezależnie od możliwości sprawdzenia przez GIODO organizacyjnego przygotowania się administratorów danych i podmiotów przetwarzających do wymagań RODO trzeba pamiętać, że administratorzy danych i podmioty przetwarzające będą poddawani swego rodzaju kontroli ze strony osób, których dane przetwarzają. Jeśli uznają one, że dochodzi w tym zakresie do nieprawidłowości, mają prawo, zgodnie z art. 79 RODO, wniesienia sprawy do sądu. Ponadto jeżeli osoba, której dane są przetwarzane, w wyniku naruszenia zasad przetwarzania poniosła szkodę majątkową lub niemajątkową, ma prawo do żądania z tego tytułu odszkodowania od administratora lub podmiotu przetwarzającego.



Oprac. Joanna Pieńczykowska