PYTANIA DO EKSPERTA

RODO zapewnia administratorom znaczną samodzielność i elastyczność

Kiedy zostanie przekazany do publicznej wiadomości wykaz rodzajów operacji przetwarzania podlegających oraz niepodlegających wymogowi dokonania oceny skutków dla ochrony danych?

Przepisy ogólnego rozporządzenia o ochronie danych (RODO) w art. 35 ust. 4 nakładają na organ nadzorczy obowiązek ustanowienia i podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków. Dają mu też możliwość (art. 35 ust. 5) ustanowienia i podania do publicznej wiadomości wykazu rodzajów operacji przetwarzania niepodlegających wymogowi dokonania oceny skutków dla ochrony danych, lecz go do tego nie zobowiązują. Niemniej jednak generalny inspektor ochrony danych osobowych (GIODO) rozważa przygotowanie również takiej listy.

W związku z tym, że rozporządzenie będzie stosowane od 25 maja 2018 r., GIODO nie ma podstaw prawnych, by wcześniej opublikować taką listę bądź listy. Wiele pomocnych informacji pozwalających na identyfikowanie takich operacji przekazujemy jednak zarówno w przygotowanych przez Grupę Roboczą Art. 29, której GIODO jest członkiem, „Wytycznych dotyczących oceny skutków dla ochrony danych WP 248", dostępnych na stronie internetowej GIODO w zakładce „Reforma przepisów" (pod linkiem https://giodo.gov.pl/pl/1520344/10393), jak i w opracowanym przez GIODO dwuczęściowym poradniku „Jak rozumieć i stosować podejście oparte na ryzyku?" zamieszczonym na naszej stronie internetowej (pod linkiem http://giodo.gov.pl/pl/1520282/10294).

fot. Materiały prasowe

DR EDYTA BIELAK-JOMAA

generalny inspektor ochrony danych osobowych (GIODO)

Czy możliwe jest przedstawienie listy kilku przykładowych rodzajów operacji podlegających bądź niepodlegających wymogowi przeprowadzenia oceny?

Na obecnym etapie bezsprzecznie można stwierdzić, że ocena skutków dla ochrony danych jest wymagana w trzech przypadkach, wskazanych w art. 35 ust. 3 RODO. Przykładowe rodzaje operacji, które z dużym prawdopodobieństwem będą podlegać wymogowi przeprowadzenia oceny skutków, można odnaleźć we wspomnianych wytycznych Grupy Roboczej Art. 29 w tabeli zamieszczonej na stronach 13 i 14 tego dokumentu. Warto również zwrócić uwagę na dziewięć kryteriów, jakie Grupa Robocza wskazała w powołanych wytycznych (na str. 10–12), zalecając, że muszą być brane pod uwagę przy ustalaniu konieczności dokonywania oceny skutków dla ochrony danych. Mają one również pomóc organom nadzorczym przygotować wykaz operacji przetwarzania wymagających oceny skutków dla ochrony danych.

Ponadto w wytycznych można odnaleźć przypadki (str. 15), dla których według grupy roboczej nie zachodzi konieczność przeprowadzenia oceny skutków.

Czy administrator przeprowadzający wstępną ocenę skutków dla ochrony danych, stwierdzając, że w przedsięwzięciu nie będzie występować wysokie ryzyko przetwarzania, a więc nie powstaje obowiązek przeprowadzenia oceny, jest obowiązany przechować dokument wstępnej oceny? Czy podlegać to będzie kontroli?

Unijny ustawodawca w art. 35 ust. 1 RODO nie określa, jakie działania i środki organizacyjne powinien podjąć administrator, aby stwierdzić, czy jest zobowiązany do przeprowadzenia oceny skutków dla ochrony danych. Zgodnie z art. 24 RODO obowiązkiem administratora jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z rozporządzeniem i aby można było to wykazać. Ponadto środki te mają być w razie potrzeby poddawane przeglądom i uaktualniane. Wynika to również z zasady rozliczalności. RODO zapewnia administratorom danych dużą samodzielność i elastyczność działania, przy jednoczesnym nałożeniu odpowiedzialności. Wszelka dokumentacja, która będzie pozwalała administratorowi wywiązać się z obowiązku wykazania zgodności, będzie podlegała kontroli.

Czy określony w art. 35 ust. 11 RODO obowiązek dokonywania przeglądu zmieniającego się ryzyka wynikającego z operacji przetwarzania stanowi obowiązek przeprowadzenia kolejnej „zaktualizowanej" oceny skutków dla ochrony danych, czy jest to obowiązek przyjmujący inną formę?

Ustawodawca unijny nie precyzuje, jaką formę organizacyjną powinien przyjąć taki przegląd. Warto jednak podkreślić, że grupa robocza w swoich wytycznych wskazuje, że dobrą praktyką powinno być stałe przeprowadzanie przeglądu oceny skutków dla ochrony danych i regularne przeprowadzanie ponownej oceny. W związku z powyższym, nawet jeżeli 25 maja 2018 r. administrator stwierdzi, że nie wymaga się przeprowadzenia oceny skutków dla ochrony danych, to w odpowiednim momencie będzie musiał przeprowadzić taką ocenę w ramach swoich ogólnych obowiązków w zakresie rozliczalności.

Raz jeszcze zachęcam, by zapoznać się z naszym poradnikiem „Jak rozumieć i stosować podejście oparte na ryzyku?". W pierwszej części nasi eksperci wyjaśniają istotę zasady podejścia opartego na ryzyku oraz wskazują, do czego zasada ta zobowiązuje podmioty stosujące RODO. Tłumaczą też, czym jest ryzyko naruszenia praw i wolności osób, których dane dotyczą. Podkreślają przy tym, że szacowanie ryzyka to proces ciągły, realizowany przy użyciu konkretnej metody, zapewniającej stosowanie jednolitych definicji i pojęć. W drugiej części przedstawiono natomiast kolejne możliwe etapy działań podejmowanych w celu przeprowadzania ogólnej oceny ryzyka oraz oceny skutków dla ochrony danych.

Rozmawiała **Joanna Pieńczykowska**