

Zarządzanie ryzykiem zminimalizuje groźbę kar

DANE OSOBOWE

Sławomir Wikariak
slawomir.wikariak@infor.pl

Jak na gruncie nowego unijnego rozporządzenia ochrony danych osobowych (RODO) rozumieć podejście oparte na ryzyku? Kiedy ocena ryzyka jest dobrowolna, a kiedy trzeba przeprowadzić obowiązkową ocenę skutków dla ochrony danych? Odpowiedzi na te pytania przedsiębiorcy mogą szukać w opublikowanym wczoraj przez generalnego inspektora ochrony danych osobowych darmowym poradniku.

Do 25 maja 2018 r., kiedy to zacznie być stosowane RODO, pozostało mało czasu. Tak naprawdę przedsiębiorcy powinni już prowadzić zaawansowane

przygotowania. Tym bardziej, że nie chodzi tylko o wdrożenie obowiązków formalnych, wprost płynących z unijnych przepisów, ale też, a może nawet przede wszystkim, zidentyfikowanie zagrożeń związanych z przetwarzaniem danych. RODO kładzie bowiem duży nacisk właśnie na podejście oparte na ryzyku.

„Takie podejście umożliwia skoncentrowanie się na sytuacjach najwyższego ryzyka, przy jednoczesnym zachowaniu odpowiedniego poziomu ochrony, gdy to ryzyko jest niskie i nie wymaga całego instrumentarium środków przewidzianych przez rozporządzenie ogólne o ochronie danych. Przykładowo zatem inne środki ochrony

powinny być podjęte w przypadku przetwarzania danych przez sklep prowadzący sprzedaż internetową, a inne przez sklep prowadzący sprzedaż wyłącznie w lokalu, który nie przetwarza danych swoich klientów przy użyciu systemów teleinformatycznych wykorzystujących sieć internet” – można przeczytać w poradniku opublikowanym przez GODO.

Szacując ryzyko, trzeba z jednej strony wziąć pod uwagę, jakie jest prawdopodobieństwo naruszenia praw lub wolności osoby, której dane dotyczą, a z drugiej – powagę naruszenia, czyli wielkość szkody, jaką może to wyrządzić. Do obliczenia wysokości ryzyka można używać różnej metodologii. Na

końcu zaś należy dostosować podejmowane środki do potencjalnych zagrożeń. Oczywiście głównym celem tych działań jest zapobieganie zagrożeniom, ale przedsiębiorcy powinni to robić także w swoim dobrze pojmowanym interesie. Jeśli bowiem mimo wszystko dojdzie do naruszenia (np. wycieku danych), to organ wymierzający karę finansową będzie brał pod uwagę, czy firma podjęła kroki, by zapobiec takiej sytuacji, a jeśli tak, to czy działania te były adekwatne do zagrożeń. Przypomnijmy zaś, że kary przewidziane przez RODO mogą sięgnąć nawet 20 mln euro.

Jak podkreślono w podręczniku, RODO nie wskazuje jed-

nej określonej metody prowadzenia procesu zarządzania ryzykiem. Można stosować różne, byleby pozwalały na obiektywną ocenę. Co istotne, taka ocena nie może być dokonana jednokrotnie – szacowanie ryzyka powinno być traktowane jako proces ciągły.

W niektórych sytuacjach (np. przy danych przetwarzanych na masową skalę) RODO wprost zobowiązuje do przeprowadzania oceny skutków dla ochrony danych. Tu przedsiębiorcy nie mają już wyboru – muszą przeprowadzić taką ocenę i musi być ona pogłębiona, najczęściej też nie obejdzie się pomocy ekspertów.

Poradnik został udostępniony na stronie internetowej GODO: www.godo.gov.pl. ©