PYTANIA DO EKSPERTA

Administrator sam musi zdecydować, czy dane zdarzenie trzeba zgłosić

Czy przedsiębiorca będzie mógł zwrócić się do organu nadzorczego o pomoc w ustaleniu, czy dane zdarzenie jest naruszeniem w rozumieniu RODO?

Ogólne rozporządzenie o ochronie danych osobowych przyznaje administratorom znacznie większą samodzielność w decydowaniu o przetwarzaniu danych osobowych. Zapewnia im to większą elastyczność działania, ale wiąże się również z większą odpowiedzialnością za podejmowane decyzje. Zgodnie z tym nowym podejściem również ustalenie tego, czy dane zdarzenie należy traktować jako naruszenie ochrony danych, będzie samodzielnym zadaniem administratora. Niemniej w przepisach RODO otrzymuje on pewne wskazówki w tym zakresie. Artykuł 4 pkt 12 RODO stanowi, że naruszenie ochrony danych oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Pomocne w ocenie naruszeń mogą być także wyjaśnienia zawarte w Wytycznych Grupy Roboczej Art. 29 w sprawie powiadomień o naruszeniu ochrony danych osobowych na mocy rozporządzenia 2016/670 przyjętych 3 października 2017 r. Zatem administrator, dokonując oceny danego zdarzenia, będzie mógł się nimi posiłkować. GIODO nie jest natomiast uprawniony, by konsultować zaistniałe incydenty z administratorem.

fot. Materiały prasowe

DR EDYTA BIELAK-JOMAA

generalny inspektor ochrony danych osobowych (GIODO)

Na jaką pomoc może zatem liczyć?

Zdaję sobie sprawę, że szczególnie mniejsze przedsiębiorstwa, zwłaszcza w pierwszym okresie stosowania RODO, mogą mieć problem z oceną sytuacji, w której może pojawić się obowiązek zgłoszenia naruszenia ochrony danych. Dla nich cenną pomocą powinny być wymienione przeze mnie dokumenty, które sukcesywnie publikujemy na naszej stronie w związku z przygotowaniami do RODO. Kwestie te omawiamy także podczas szkoleń, a jeśli będzie taka potrzeba, to przygotujemy dodatkowe materiały instruktażowe.

Czy nie istnieje obawa, że administrator danych bez wsparcia konsultacyjnego GIODO nie dochowa terminu zgłoszenia?

Przepisy RODO określają, że zgłoszenie naruszenia ma nastąpić niezwłocznie, jednak nie później niż w ciągu 72 godzin od wykrycia. Ten termin jest wystarczająco długi, by w większości przypadków przeanalizować, czy faktycznie doszło do naruszenia, a jeśli tak, to jakie są lub mogą być jego skutki i jakie należy podjąć działania zaradcze. Można przecież przesłać zgłoszenie, a później – w miarę uzyskiwania dodatkowych informacji – po prostu je uzupełnić. Wyjątkowo administrator może zgłosić naruszenie po upływie 72 godzin. Jednak wówczas musi przesłać również wyjaśnienie przyczyn opóźnienia. Należy pamiętać, że działania związane z naruszeniem ochrony danych powinny być podejmowane szybko. Chodzi o to, by w jak najkrótszym czasie wdrożyć rozwiązania zabezpieczające, by możliwie szybko ograniczyć skutki np. wycieku danych, zabezpieczyć inne dane oraz podjąć odpowiednie działania naprawcze, a także wówczas, gdy to konieczne, poinformować o zaistniałej sytuacji osoby, których dane dotyczą.

Czy treść zawiadomienia do osoby, której dotyczy naruszenie, powinna być wcześniej skonsultowana z organem nadzorczym?

W sytuacji naruszenia ochrony danych osobowych czas reakcji jest bardzo istotny, a konsultacje tylko opóźniłyby podjęcie działań mających przyczynić się do ograniczenia możliwych negatywnych skutków zaistniałej sytuacji. Bardzo ważne jest, by osoby, których dane zostały np. ujawnione czy skradzione albo w inny sposób naruszone, mogły po takim powiadomieniu jak najszybciej same podjąć działania, które zabezpieczą je przed kolejnymi zagrożeniami. Przykładowo zmienią hasła do systemu informatycznego lub wymienią bądź zastrzegą dowód osobisty. Dodatkowo mogą podjąć inne kroki zalecane w danej sytuacji przez administratora.

Przepisy RODO (art. 33 i 34) określają, jak powinny wyglądać takie zawiadomienia. Przede wszystkim muszą być napisane prostym językiem. Opisywać charakter naruszenia, zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub dane innego punktu kontaktowego, gdzie można uzyskać więcej informacji. Trzeba w nich opisać możliwe konsekwencje naruszenia ochrony danych osobowych oraz zastosowane lub proponowane przez administratora środki w celu zaradzenia naruszeniu ochrony danych osobowych oraz zminimalizowania ewentualnych negatywnych skutków.

Warto zaznaczyć, że w wielu przypadkach to powołany przez administratora danych inspektor ochrony danych będzie kontaktował się w tym zakresie z osobami, których dane zostały naruszone oraz z organem nadzorczym. Do kompetencji takiej osoby będzie też należało instruowanie samego administratora danych i jego pracowników co do działań, które powinny zostać podjęte. On też będzie informował osoby poszkodowane danym naruszeniem o ich prawach i obowiązkach. Dlatego RODO nieprzypadkowo wymaga, by inspektorzy mieli odpowiednią wiedzę i umiejętności. Takie osoby powinny więc być w stanie ocenić sytuację i doradzić administratorowi, czy istnieje konieczność powiadamiania o naruszeniu zarówno GIODO, jak i osób, których dotyczy incydent. GIODO ma zaś kompetencje, by reagować np. wówczas, gdy uzna, że podjęte przez administratora działania są niewystarczające i należy wdrożyć dodatkowe środki zaradcze. ©℗

Rozmawiała **Joanna Pieńczykowska**