Załącznik nr 2 do uchwały Zarządu Głównego PTTK
nr 169/XIX/2020 z dnia 4 lipca 2020 r.

PROCEDURA ZGŁASZANIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

PREZESOWI URZĘDU OCHRONY DANYCH OSOBOWYCH

W POLSKIM TOWARZYSTWIE TURYSTYCZNO-KRAJOZNAWCZYM

Zgłaszanie naruszenia ochrony danych osobowych Prezesowi Urzędu Ochrony Danych Osobowych

Obowiązek zgłaszania naruszeń ochrony danych do Prezesa UODO stanowi nowe rozwiązanie wprowadzone do ogólnych przepisów o ochronie danych na mocy art. 33 unijnego rozporządzenia o ochronie danych. Prawodawca unijny zdefiniował pojęcie naruszenia ochrony danych osobowych, nałożył obowiązek zgłoszenia naruszenia, określił termin na dopełnienie tego obowiązku, wskazał minimalne wymogi co do treści zgłoszenia oraz nałożył na administratora obowiązek dokumentowania naruszeń. Niedopełnienie obowiązku zgłoszeniowego może pociągnąć za sobą odpowiedzialność w postaci nałożenia na administratora przez Urząd Ochrony Danych Osobowych administracyjnej kary pieniężnej, o której mowa w art. 83 ust. 4 RODO.

Uzyskanie informacji o naruszeniu przepisów o ochronie danych osobowych

Administrator może uzyskać informacje o naruszeniu przepisów o ochronie danych z różnych źródeł. Najbardziej typowe przypadki uzyskania tego rodzaju informacji, to poinformowanie o tym przez osobę zatrudnioną przy przetwarzaniu danych oraz uzyskanie informacji od podmiotu przetwarzającego dane, który na mocy art. 33 ust. 2 RODO ma obowiązek bez zbędnej zwłoki zgłosić naruszenie administratorowi.

Ocena, czy naruszenie przepisów stanowi naruszenie ochrony danych osobowych w rozumieniu RODO

Po uzyskaniu informacji o naruszeniu przepisów o ochronie danych administrator powinien ocenić, czy naruszenie to stanowi naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt 12 RODO, a więc czy jest to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych. Prawodawca unijny zawęził pojęcie naruszenia ochrony danych osobowych jedynie do tych przypadków, w których występuje tzw. incydent bezpieczeństwa pociągający za sobą skutki wskazane w przepisach. Oznacza to, że w przypadku innego rodzaju naruszeń przepisów o ochronie danych (np. naruszenia zasad, obowiązków informacyjnych itp.) administrator nie ma obowiązku zawiadamiania o tym organu nadzorczego.

Brak obowiązku zgłoszenia naruszenia Prezesowi Urzędu Ochrony Danych

Jeżeli naruszenie przepisów o ochronie danych nie stanowi naruszenia ochrony danych osobowych w rozumieniu, jakie temu pojęciu nadał prawodawca unijny w art. 4 pkt 12 RODO, to na administratorze nie ciąży obowiązek zgłoszenia tego faktu Prezesowi UODO.
Również w sytuacji, gdy stwierdzono zaistnienie naruszenia ochrony danych, jednak jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych, administrator nie ma obowiązku zgłaszać naruszenia do Prezesa UODO.

Ocena, czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw osoby

Stwierdzenie, że nastąpiło naruszenie ochrony danych (incydent bezpieczeństwa pociągający za sobą skutek w postaci zniszczenia, utraty, nieuprawnionego zmodyfikowania, ujawnienia lub dostępu do danych), nie oznacza jeszcze konieczności dokonania zgłoszenia do Prezesa UODO, gdyż przepis art. 33 ust. 1 RODO nakazuje administratorowi dokonanie oceny prawdopodobieństwa czy naruszenie ochrony danych skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych. Jeżeli prawdopodobieństwo to jest małe, to administrator może odstąpić od zgłoszenia. Uznanie, że naruszenie praw osoby jest prawdopodobne, pociąga za sobą konieczność dokonania zgłoszenia.

Zgłoszenia naruszenia ochrony danych Prezesowi Urzędu Ochrony Danych

Przepis art. 33 ust. 3 RODO określa wymagania minimalne dotyczące zawartości zgłoszenia naruszenia ochrony danych Prezesowi UODO. Zgodnie ze wskazanym przepisem, zgłoszenie powinno co najmniej:

a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b) zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Prawodawca unijny określił również termin na dokonanie zgłoszenia: administrator powinien zgłosić naruszenie bez zbędnej zwłoki, w miarę możliwości nie później niż w terminie 72 godzin

po stwierdzeniu naruszenia. Termin ten jest krótki i w praktyce może się okazać trudny do zachowania, zwłaszcza w przypadku, gdy naruszenie ma poważny charakter i administrator koncentruje się najpierw na ograniczeniu skutków naruszenia, a w dalszej kolejności stara się spełnić pozostałe obowiązki. W takiej sytuacji dopuszczalne jest późniejsze zawiadomienie, po upływie 72-godzinnego terminu, jednak należy wówczas wyjaśnić przyczyny opóźnienia. Prawodawca unijny dopuszcza także możliwość zgłoszenia częściowego (informacji, które są znane administratorowi w chwili dokonania zgłoszenia przed upływem 72 godzin), w przypadku, gdy całościowe zgłoszenie nie jest możliwe z zachowaniem wskazanego terminu, a następnie sukcesywnego uzupełniania zgłoszenia, zgodnie z art. 33 ust. 4 RODO.

Ocena, czy wymagane jest zawiadomienie osoby, której dane dotyczą o naruszeniu

Administrator powinien dokonać oceny czy przepisy wymagają od niego również zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych. Taka ocena powinna być dokonana na podstawie przepisu art. 34 RODO.

Udokumentowanie naruszenia

Oprócz obowiązków informacyjnych związanych z naruszeniem ochrony danych (zgłoszeniem naruszenia Prezesowi UODO i zawiadomieniem osoby, której dane dotyczą, o naruszeniu) unijne rozporządzenie nakłada na administratora wymóg dokumentowania wszelkich naruszeń ochrony danych osobowych. Zgodnie z art. 33 ust. 5 RODO administrator powinien dokumentować wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. W praktyce oznacza to konieczność prowadzenia dokumentacji naruszeń, w której powinny się znaleźć informacje o stwierdzonych przez administratora naruszeniach i podjętych działaniach. Dokumentacja ta - zgodnie z wymogiem określonym we wskazanym powyżej

przepisie - powinna pozwolić UODO weryfikowanie przestrzegania wymogów określonych w art. 33 RODO.