O naruszeniu ochrony danych trzeba powiadomić organ nadzorczy

Kolejne spotkanie z ochroną danych osobowych, w pewnym zakresie kontynuując tematykę z poprzedniego artykułu, poświęcimy kwestii naruszenia ochrony danych osobowych, czyli ustalimy co jest, a co nie jest naruszeniem, co musi zrobić administrator jeżeli stwierdzi u siebie naruszenie, jakie będą konsekwencje zgłoszenia, a jakie niezgłoszenia naruszenia. Tu jeszcze krótka uwaga. Omawiać będziemy nie naruszenie przepisów ochrony danych osobowych tylko naruszenie ochrony danych osobowych. **Naruszenie przepisów** o ochronie danych, to zachowanie, w wyniku którego następuje naruszenie RODO lub innych przepisów obowiązujących w tym zakresie. Natomiast **naruszenie ochrony danych osobowych** zdefiniowane jest w art. 4 RODO: „Naruszenie ochrony danych 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". Na bazie tej definicji należy zwrócić uwagę, że naruszenie to nie tylko sytuacje, w których czyjeś dane osobowe „wyciekają" w sposób niekontrolowany, dostają się w niepowołane ręce, lecz także sytuacje, w wyniku których następuje także uszkodzenie, zniszczenie czy nieprawidłowa modyfikacja tych danych. A jakie są obowiązki administratora, w momencie w którym stwierdzi, że doszło u niego do naruszenia. Art. 33 RODO w ust.1 wskazuje jednoznacznie: „W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, **nie później niż w terminie 72 godzin po stwierdzeniu naruszenia** – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia." Stwierdzamy więc, że nastąpiło naruszenie i mamy 72 godziny żeby dokonać zgłoszenia do PUODO. Jeżeli tego nie zrobimy, a organ nadzoru uzyska o tym fakcie wiedzę, to musimy być przygotowani na konsekwencje z tego tytułu, łącznie z karą finansową. O takiej karze więcej w części drugiej artykułu. Wracając do naruszenia. W definicji pojawia się zapis, z którego wynika, że administrator nie jest zobowiązany do dokonania zgłoszenia jeżeli jest mało prawdopodobne, by to naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Już na tym etapie mamy więc problem, który analizować należy w odniesieniu do konkretnego zdarzenia, które miało miejsce u administratora, bowiem od prawidłowej analizy i w jej wyniku stwierdzenia czy mamy do czynienia z naruszeniem, które wymaga zgłoszenia bądź nie, zależą dalsze konsekwencje. W takiej sytuacji niezbędne okazują się dwie rzeczy; po pierwsze posiadanie wdrożonej dokumentacji ochrony danych z częścią dotyczącą procedur związanych z naruszeniem ochrony danych osobowych, po drugie wsparcie ze strony osób, które posiadają odpowiednią wiedzę i doświadczenie w praktycznym stosowaniu przepisów ochrony danych osobowych. Jak potrafi być skomplikowana kwestia praktycznego działania w tym zakresie, przedstawiliśmy Wam już w poprzednim artykule omawiając udział w postępowaniu prowadzonym przez PUODO. Ale często, to jaką mamy szansę wybronienia się czy nie przed konsekwencjami naruszenia ochrony danych osobowych, zależy od tego jak jesteśmy przygotowani na sytuacje kryzysowe. Czyli, między innymi, na działania związane z naruszeniem i jego zgłoszeniem. Artykuł 33 ust. 3 RODOO wskazuje szereg elementów, które powinno zawierać zgłoszenie do PUODO:

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.
Dodatkowo administrator ma obowiązek dokumentowania wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, skutki tych naruszeń. Jest także zobowiązany do udokumentowania podjętych działań zaradczych. Taka dokumentacja musi pozwolić organowi nadzorczemu na zweryfikowanie czy administrator przestrzega wymogów określonych w treści art. 33 RODO. No i nie wolno zapominać o obowiązku wynikającym z zapisu art. 34 RODO, czyli sytuacji, w której naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, bowiem w takim przypadku administrator bez zbędnej zwłoki **zawiadamia osobę, której dane dotyczą**, o takim naruszeniu. Taka informacja, zgodnie z RODO, powinna być sporządzona prostym, zrozumiałym językiem i zawierać opis charakteru naruszenia ochrony danych osobowych oraz wskazania dla tej osoby fizycznej odnoszące się do minimalizacji potencjalnych niekorzystnych skutków, tak aby umożliwić tej osobie podjęcie niezbędnych, skutecznych działań zapobiegawczych. Te informacje należy przekazać osobom, których dane dotyczą, tak szybko, jak to jest tylko możliwe. W sytuacji, w której administrator nie zrealizował swojego obowiązku w tym zakresie, może mu zostać to narzucone przez organ nadzoru. Jest oczywiście możliwość uniknięcia potrzeby zawiadomienia, ale tylko w sytuacji kiedy administrator spełnia następujące warunki:
a) wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b) zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
Sporo obowiązków i wymogów, w tym konsekwencja tego, co już stwierdziliśmy wcześniej, niby RODO nie wymaga konkretnej dokumentacji, ale jednocześnie nie mając opracowanych i wdrożonych procedur, regulaminów, polityk, nie jesteśmy w stanie udokumentować organowi nadzoru, że prawidłowo realizujemy ochronę danych osobowych. I wybronić się przed konsekwencjami z tego wynikającymi. A jeżeli już kwestia konsekwencji, to krótkie omówienie dwóch decyzji PUODO dotyczących kwestii , które omawialiśmy powyżej, czyli braku zawiadomienia organu nadzoru o naruszeniu ochrony danych osobowych.

Pierwsza decyzja dotyczy nałożenia przez Prezesa Urzędu Ochrony Danych Osobowych kary pieniężnej w wysokości 136.000 zł na spółkę ENEA S.A. za brak zgłoszenia naruszenia ochrony

danych osobowych[1]. Jak wynika z treści uzasadnienia decyzji „Do Urzędu Ochrony Danych Osobowych (UODO) wpłynęła informacja o naruszeniu ochrony danych osobowych pochodząca od osoby, która stała się nieuprawnionym adresatem danych osobowych. Naruszenie to polegało na wysłaniu e-maila z niezaszyfrowanym, niezabezpieczonym hasłem załącznikiem zawierającym dane osobowe kilkuset osób. Nadawcą maila był współpracownik ukaranego przedsiębiorstwa." Pomimo wyjaśnień ze strony spółki, że została dokonana ocena pod kątem ryzyka naruszenia praw i wolności osób fizycznych, na podstawie której spółka uznała, iż nie doszło do naruszenia skutkującego koniecznością zawiadomienia UODO, tym bardziej, że uzyskano oświadczenie nieuprawnionego adresata, że w sposób trwały zniszczył załącznik, do którego otrzymania nie był upoważniony oraz podjęto działania w wyniku, których wyeliminowano możliwość zaistnienia w przyszłości negatywnych skutków tego zdarzenia dla osób, których dane dotyczą, PUODO stwierdził, że: „W przedmiotowej sprawie doszło do wysłania do nieuprawnionego odbiorcy wiadomości e-mail wraz z załącznikiem w postaci niezaszyfrowanego pliku zawierającego dane osobowe adresata wiadomości i innych osób. Oznacza to, że doszło do naruszenia bezpieczeństwa prowadzącego do przypadkowego ujawnienia danych osobowych osobie nieuprawnionej do otrzymania tych danych, a więc do naruszenia poufności danych tych osób, co przesądza, że wystąpiło naruszenie ochrony danych osobowych." W uzasadnieniu decyzji znalazło się dodatkowo stwierdzenie, że Urząd uwzględnił również okoliczności łagodzące, mające wpływ na ostateczny wymiar kary, tj. działania podjęte przez administratora w celu zminimalizowania szkody poniesionej przez osoby, których dane dotyczą.

Druga decyzja dotyczy sytuacji, w której Prezes UODO nałożył 25.000 zł kary na Śląski Uniwersytet Medyczny, gdyż na uczelni doszło do naruszenia ochrony danych, o którym administrator powinien powiadomić nie tylko organ nadzoru, ale i osoby, których dotyczył ten incydent[2]. Oprócz nałożonej kary, PUODO nakazał uczelni dokonanie powiadomienia osób, których dotyczyło naruszenie, do jakiego doszło w związku z egzaminami przeprowadzanymi w formie wideokonferencji na specjalnej do tego platformie e-learningowej. Z treści uzasadnienia decyzji wynika, że „ podczas egzaminów odbywających się pod koniec maja 2020 r. w formie wideokonferencji, miała miejsce identyfikacja studentów. Po zakończonym egzaminie nagrania z nich były dostępne nie tylko dla osób egzaminowanych, ale i innych osób mających dostęp do systemu. Ponadto wykorzystując bezpośredni link każda osoba postronna mogła mieć dostęp do nagrań z egzaminów i przedstawionych podczas identyfikacji danych egzaminowanych studentów." Uczelnia w wyjaśnieniach utrzymywała, że w tym przypadku nie było konieczności zawiadamiania Urzędu, ponieważ w jej ocenie ryzyko dla praw lub wolności osób, których dotyczył incydent było niskie. Jednocześnie uczelnia wskazała, że po tym zdarzeniu system został zmodyfikowany, by nie dochodziło do omyłkowego udostępniania plików z zarejestrowanym przebiegiem egzaminów. Administrator wskazał też,

[1] https://www.uodo.gov.pl/decyzje/DKN.5131.7.2020

[2] https://uodo.gov.pl/decyzje/DKN.5131.6.2020.

że zidentyfikował osoby, które pobrały plik z egzaminem i powiadomił je o odpowiedzialności za posługiwanie się tymi danymi. Pomimo pisma z organu nadzoru Uczelnia nie tylko nie zgłosiła naruszenia ochrony danych, lecz też i nie powiadomiła osób dotkniętych tym zdarzeniem. Kolejne pismo UODO nie spowodowało zmiany stanowiska uczelni. W tej sytuacji organ nadzoru wszczął postępowanie administracyjne, w którego toku ustalono, że do naruszenia doszło ponieważ jeden z pracowników, po zakończonym egzaminie na platformie e-learningowej nie zamknął dostępu do wirtualnego pokoju, w którym odbywał się sprawdzian. Przez to można było pobrać nagrania z przebiegu egzaminu. W związku z tym, że studenci przed przystąpieniem do egzaminu byli identyfikowani na podstawie dowodów osobistych lub legitymacji studenckich, na nagraniach zarejestrowany był szereg ich danych. W zależności od tego jakim wzorem dowodu osobistego lub legitymacji studenckiej się posługiwali inny był zakres danych w przypadku poszczególnych osób dotkniętych naruszeniem. W części przypadków były to jednak m.in. wizerunek, nr PESEL, nr dokumentu tożsamości czy albumu, imię i nazwisko, adres zamieszkania. Ponadto w wyniku naruszenia osoby nieuprawnione mogły zapoznać się z innymi danymi jak: rok studiów, grupa, kierunek studiów, informacje o zdawanym przedmiocie czy udzielonych odpowiedziach podczas egzaminu. PUODO uznał, że w tej sytuacji administrator niewłaściwie więc ocenił zaistniałe ryzyko.

Co wynika z tych dwu decyzji PUODO? Po pierwsze, to czy coś stanowi naruszenie ochrony danych osobowych czy nie, często jest inaczej interpretowane przez administratora, a inaczej przez PUODO. Drugie, że błędna interpretacja administratora może być dla niego kosztowna finansowo. Trzecie, że przyczyna naruszenia to często zdarzenia , które mają miejsce w praktyce codziennego funkcjonowania wielu firm. No i tym samym po czwarte, to że administrator uważa, że nie ma potrzeby zgłaszać naruszenia, nie ma szczególnego znaczenia, bo zawsze może znaleźć się chętny, który zrobi to za niego.

etaxar

Janusz Dębowski
Ochrona Danych Osobowych
tel. 502 434 909
biuro@etaxar.pl

mp
Magdalena Piekuś
OCHRONA DANYCH OSOBOWYCH