Warszawa, 19.01.2022 r.

Brak zgłoszenia naruszenia oraz niepowiadomienie osób o incydencie
- przegląd kar Prezesa Urzędu Ochrony Danych Osobowych

Obowiązek zgłoszenia naruszenia do organu nadzorczego wynika wprost z art. 33 RODO. Zgodnie z przywołanym przepisem, 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 (…)[1].

Zdecydowanie istotną rolę w cytowanym przepisie odgrywa czas. Ustawodawca wskazuje konkretny termin, w czasie którego należy dokonać zgłoszenia naruszenia organowi nadzorczemu. Element istotności czasu w odniesieniu do obowiązku zgłoszenia incydentu Prezesowi UODO został również przez ustawodawcę unijnego podniesiony w motywie 85 RODO. Zgodnie z nim brak odpowiedniej i szybkiej reakcji na określone zdarzenie kwalifikowane jako naruszenie może skutkować powstaniem:

- ✓ uszczerbku fizycznego,
- ✓ szkód majątkowych lub niemajątkowych u osób fizycznych, takich jak utrata kontroli nad własnymi danymi osobowymi lub ograniczenie praw, dyskryminacja, kradzież lub sfałszowanie tożsamości, strata finansowa, nieuprawnione odwrócenie pseudonimizacji, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową lub wszelkie inne znaczne szkody gospodarcze lub społeczne.

Biorąc pod uwagę powyższe, natychmiast po stwierdzeniu naruszenia ochrony danych osobowych, administrator powinien zgłosić je organowi nadzorczemu bez zbędnej zwłoki (nie później niż w terminie 72 godzin po stwierdzeniu naruszenia), chyba że administrator jest w stanie wykazać zgodnie z zasadą rozliczalności, że jest mało prawdopodobne, by naruszenie to mogło powodować ryzyko naruszenia praw lub wolności osób fizycznych.

Jeżeli administrator ustali, iż naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych, to poza ciążącym na nim obowiązku zgłoszenia tego faktu organowi nadzorczemu, powinien również dokonać zawiadomienia o takim naruszeniu osób, których dane dotyczą.

[1] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Dlaczego zatem administratorzy nie decydują się na zgłoszenie naruszenia do organu nadzorczego oraz powiadomienie podmiotów danych o incydencie, a po analizie zdarzenia Urząd nakłada na nich karę pieniężną?

Brak zgłoszenia naruszenia organowi nadzorczemu wynika głównie z błędnego (w ocenie Urzędu) założenia, iż analizowane przez administratorów incydenty nie będą skutkowały wysokim ryzykiem naruszenia praw i wolności osób fizycznych. Używane w tym celu algorytmy oraz formularze, choć stanowią dużą pomoc i wsparcie przy analizie konkretnych zdarzeń, nie powinny stanowić ostatecznego wyznacznika w przedmiocie decyzji o przyjęciu wysokiego lub niskiego ryzyka naruszenia praw i wolności osób fizycznych, a co za tym idzie, nie powinny determinować faktu zgłoszeniu naruszenia organowi nadzorczemu. Z kolei brak zgłoszenia naruszenia do organu nadzorczego przekłada się bezpośrednio na decyzję o braku konieczności zawiadomienia osób, których dane dotyczą o naruszeniu ochrony danych osobowych.

Przegląd kar

I. Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra

Fundacja Promocji Mediacji i Edukacji Prawnej Lex Nostra została ukarana administracyjną karą pieniężną w wysokości ponad 13 tys. zł za niezgłoszenie organowi nadzorczemu naruszenia ochrony danych osobowych bez zbędnej zwłoki, oraz niezawiadomieniu o incydencie osób, których dane dotyczą.
Na początku 2020 r. Fundacja zidentyfikowała naruszenie polegające na utracie danych osobowych wielu osób, na skutek kradzieży teczek zawierających dane osobowe beneficjentów. Fundacja nie zdecydowała się na zgłoszenie incydentu do UODO, gdyż dokonana przez nią analiza naruszenia dała ocenę jego wagi na poziomie niskim.
Jesienią 2020 r. do Urzędu Ochrony Danych Osobowych wpłynęło zawiadomienie o podejrzeniu naruszenia zasad przestrzegania przepisów o ochronie danych osobowych przez Fundację Promocji Mediacji i Edukacji Prawnej LEX NOSTRA. W związku z tym, w ocenie Urzędu, zaistniała obawa czy Fundacja w sposób należyty zabezpieczyła dokumenty przed ich utratą oraz administrowała danymi osobowymi w nich zawartymi zgodnie z wymogami wynikającymi z RODO[2].
Po otrzymaniu zawiadomienia UODO zwrócił się do Fundacji o wskazanie, czy w związku z utratą danych osobowych wielu osób na skutek kradzieży teczek zawierających dane osobowe beneficjentów, naruszenie zostało zgłoszone organowi nadzorczemu. W toku dalszych czynności podjętych przez UODO ustalono, że naruszenie dotyczyło 96 osób, a utracona dokumentacja

[2] www.uodo.gov.pl/aktualności

iSecure Sp. z o.o. | www isecure.pl | fax +48 22 378 26 34 | Sąd Rejonowy dla m. st. Warszawy w Warszawie
ul. Sienna 72A lok. 214 | e-mail kontakt@isecure.pl | NIP 525-247-17-82 | XII Wydział Gospodarczy
00-833 Warszawa | tel +48 22 126 58 54 | REGON 14-22-29-729 | KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

zawierała kategorie danych jak m.in. imię, nazwisko, adres do korespondencji, numer telefonu. W przypadku 3-4 osób prawdopodobnie utracono także numer PESEL.
Biorąc pod uwagę powyższe, wobec braku zgłoszenia naruszenia ochrony danych osobowych do UODO oraz braku zawiadomienia o naruszeniu ochrony danych osobowych osób, których dotyczyło naruszenie, organ nadzorczy wszczął wobec Fundacji postępowanie administracyjne, które zakończyło się nałożeniem administracyjnej kary pieniężnej w wysokości ponad 13 tys. zł. Jak podkreślił UODO, Fundacja **podejmując decyzję o niezawiadomieniu o naruszeniu organu nadzorczego, jak i osób, których dane dotyczą, w praktyce pozbawiła te osoby możliwości przeciwdziałania potencjalnym szkodom. Zawiadamiając bez zbędnej zwłoki podmiot danych, administrator umożliwia osobie podjęcie niezbędnych działań zapobiegawczych w celu ochrony praw lub wolności przed negatywnymi skutkami naruszenia**[3].

II. Bank Millennium

W tym przypadku, UODO o naruszeniu ochrony danych dowiedział się ze skargi, jaka wpłynęła na Bank. Wynikało z niej, że doszło do zgubienia przez firmę kurierską korespondencji z danymi osobowymi, takimi jak: imię, nazwisko, nr PESEL, adres zameldowania, numery rachunków bankowych, numer identyfikacyjny nadawany klientom banku. Co prawda skarżący zostali o tym fakcie powiadomieni przez Bank, ale informacje na ten temat nie były wystarczające – nie spełniały wymagań określonych w RODO. Bank bowiem uznał, że ryzyko negatywnych konsekwencji dla osób dotkniętych naruszeniem jest średnie, dlatego nie zgłosił tego naruszenia organowi nadzorczemu oraz nie zrealizował w pełni obowiązku związanego z powiadomieniem osób, których dane dotyczą.

UODO podkreślił, że gdyby Bank zdecydował się powiadomić organ nadzorczy o zdarzeniu to otrzymałby wówczas wskazówki w jaki sposób należy powiadomić osoby, których dane zostały dotknięte przedmiotowym naruszeniem. Organ wskazał także, iż **z punktu widzenia przepisów o ochronie danych osobowych, biorąc pod uwagę możliwość szkodliwego wpływu na prawa lub wolności osób, nie jest istotne czy nieuprawniony odbiorca w istocie wszedł w posiadanie danych i się z nimi zapoznał, ale sam fakt, że wystąpiło takie ryzyko. Obowiązek zawiadomienia osoby fizycznej o naruszeniu ochrony danych osobowych nie jest uzależniony od zaistnienia negatywnych konsekwencji dla takiej osoby, ale od samej możliwości ich wystąpienia** – podkreślił organ nadzorczy w decyzji nakładającej na Bank Millennium S.A karę w wysokości ponad 363 tys. zł[4].

[3] www.uodo.gov.pl/aktualności
[4] www.uodo.gov.pl/aktualności

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł

Podsumowanie

Brak zgłoszenia naruszenia oraz odstąpienie od powiadomienia osób, których dane dotyczą o naruszeniu może prowadzić do wszczęcia kontroli organu nadzorczego oraz nałożenia administracyjnej kary pieniężnej. Bardzo istotnym z punktu widzenia podmiotów, które stwierdziły wystąpienia określonego zdarzenia niepożądanego/incydentu jest niezwłoczna jego analiza pod kątem tego, czy może ono powodować wysokie ryzyko naruszenia praw i wolności osób fizycznych. Kluczowym jest zatem posługiwanie się odpowiednimi narzędziami, które mogą pomóc w analizie przypadku, nie mniej jednak, nie powinny one stanowić ostatecznego kryterium w przedmiocie decyzji o przyjęciu wysokiego lub niskiego ryzyka naruszenia praw i wolności osób fizycznych, a co za tym idzie, nie powinny przesądzać o tym, czy naruszenie podlega lub nie zgłoszeniu do organu nadzorczego. Prawidłowa analiza zdarzenia powinna zatem opierać się na szczegółowym zbadaniu przypadku, którego dokonywać powinna osoba posiadająca odpowiednie doświadczenie oraz wiedzę na temat możliwych ryzyk i potencjalnych zagrożeń wynikających z naruszenia ochrony danych osobowych.

Karolina Żebrowska, specjalista ds. ochrony danych osobowych iSecure Sp. z o.o.

iSecure Sp. z o.o.
ul. Sienna 72A lok. 214
00-833 Warszawa
www isecure.pl
e-mail kontakt@isecure.pl
tel +48 22 126 58 54
fax +48 22 378 26 34
NIP 525-247-17-82
REGON 14-22-29-729
Sąd Rejonowy dla m. st. Warszawy w Warszawie
XII Wydział Gospodarczy
KRS: 0000346686
Kapitał zakładowy opłacony w całości: 50 000,00 zł