Warszawa, 2.02.2024 r.

Naruszenie ochrony danych osobowych w firmie – co dalej?

Jeżeli doszło do naruszenia ochrony danych osobowych w Twojej firmie, np. dane Twoich klientów zostały upublicznione lub dostały się w nieuprawnione ręce, zginęły Ci dokumenty zawierające dane osobowe, to jesteś zobowiązany do podjęcia konkretnych działań.

Administrator czy podmiot przetwarzający?

W pierwszej kolejności powinieneś określić, czy w stosunku do danych osobowych, których dotyczy naruszenie, jesteś administratorem czy może przetwarzasz je jako procesor (podmiot przetwarzający). Gdy jesteś administratorem danych, masz obowiązek podjąć pewne czynności, a gdy przetwarzasz te dane w imieniu innego administratora jesteś zobowiązany do pomocy temu administratorowi w wywiązaniu się z tych obowiązków.

Identyfikacja

Zacznij od analizy incydentu, określ zakres oraz rodzaj danych, których potencjalnie dotyczy naruszenie, ilość dotkniętych osób oraz ewentualne skutki naruszenia.

Przygotuj raport o naruszeniu ochrony danych, który obejmuje wszystkie istotne informacje dotyczące naruszenia, takie jak:

- Data i godzina wykrycia naruszenia.
- Sposób, w jaki doszło do naruszenia.
- Rodzaj danych osobowych dotkniętych naruszeniem.
- Liczba osób, których dane zostały naruszone.
- Potencjalne skutki naruszenia dla osób dotkniętych.

Analiza

Na podstawie tych danych przeprowadź analizę, czy w przypadku tego naruszenia doszło do naruszenia praw i wolności osób, których dane dotyczą, czyli czy to zdarzenie może w jakiś negatywny sposób mieć wpływ na te osoby. Weź pod uwagę wielkość potencjalnej szkody oraz prawdopodobieństwo jej wystąpienia. Pamiętaj, żeby taką ocenę przeprowadzić wyłącznie z perspektywy osoby, której dane zostały naruszone.

Jeżeli Twoja analiza wykaże, że nie istnieje ryzyko naruszenia praw lub wolności osób fizycznych dotkniętych naruszeniem lub jest znikome to wystarczy, że odnotujesz zdarzenie w wewnętrznej ewidencji naruszeń i postarasz się, aby podobna sytuacja nie miała miejsca.

Do analizy warto wykorzystać sprawdzone narzędzie w postaci materiału stworzonego przez Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA). Znajdziesz je tutaj: https://www.enisa.europa.eu/publications/dbn-severity

Organ nadzorczy - PUODO

Jeżeli Twoja analiza wykaże, że zaistniałe zdarzenie może prowadzić do szkód materialnych, niematerialnych czy uszczerbku fizycznego osób, których dane dotyczą, np. kradzież tożsamości, dyskryminacja, naruszenie dobrego mienia, stres, nadużycie finansowe, naruszenie poufności danych osobowych chronionych tajemnicą zawodową, to należy uznać, że istnieje wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą i informacja o takim naruszeniu (potencjalne ryzyko nie

musi się wcale zmaterializować) powinna zostać zgłoszona do organu nadzorczego, tj. Prezesa Urzędu Ochrony Danych Osobowych, nie później niż 72 godziny od stwierdzenia naruszenia.

Dodatkowo, jeżeli naruszeniu uległy dane:

- zawierające informacje szczególnie chronione, np. pochodzenie rasowe, poglądy polityczne, wyznanie przynależność do związków zawodowych, dane genetyczne, dane dotyczące zdrowia lub dane dotyczące seksualności lub wyrokach skazujących,
- zawierające czynniki osobowe, np. sytuacja ekonomiczna, zdrowie, zainteresowania, lokalizacja, w celu tworzenia i wykorzystywania profili osobistych,
- osób wymagających szczególnej opieki, np. dzieci,
- dotyczące dużej ilości osób, których dane dotyczą,

to odgórnie należy uznać, że naruszenie tych danych powoduje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą.

Dodatkowo warto wziąć pod uwagę, że nasz polski organ nadzorczy jest bardzo przewrażliwiony, gdy informacją, która uległa „wyciekowi" jest PESEL. Można wówczas przyjąć – często wbrew temu co nam wyjdzie z analizy naruszenia metodologią ENISA – że takie naruszenie i tak powinieneś zgłosić.

Osoba, której dane dotyczą

Jeżeli naruszenie danych niesie za sobą wysokie ryzyko naruszenia praw i wolności osoby, której dane dotyczą informacja o naruszeniu powinna bez zbędnej zwłoki trafić również do tej osoby, tak aby umożliwić tej sobie podjęcie niezbędnych działań zapobiegawczych. Informacja taka powinna zawierać opis charakteru naruszenia ochrony danych osobowych oraz zalecenia co do minimalizacji potencjalnych niekorzystnych skutków.

Poinformowanie powinno być dokonane w sposób przejrzysty i zrozumiały.

Środki naprawcze

Wdróż odpowiednie środki naprawcze, aby zminimalizować ewentualne skutki naruszenia ochrony danych i zapobiec podobnym incydentom w przyszłości. Mogą to być zarówno środki techniczne np. wdrożenie aktualizacji oprogramowania, szyfrowanie, przeprowadzenie testów bezpieczeństwa aplikacji, jak i środki organizacyjne, np. dodatkowe szkolenia dla personelu lub aktualizacja procedur.

Naruszenia ochrony danych nie powinny w ogóle mieć miejsca, jednak niestety przytrafiają się one większości administratorów danych. Jeżeli więc w Twojej organizacji zdarzy się taka sytuacja, nie myśl długo tylko działaj! I pamiętaj, że za ukrycie takiego naruszenia (w tym nie zgłoszenie go do organu nadzorczego) mogą grozić Ci większe konsekwencje, niż te które byłyby spowodowane samym naruszeniem.

Maria Lothamer – ekspert ds. ochrony danych, Wiceprezes Zarządu w iSecure Sp. z o.o.