

Warszawa, dn. 29 października 2026 r.

Jakie procedury wdrożyć na wypadek naruszenia ochrony danych osobowych?

Czy Twoja organizacja ma przygotowane procedury, które pozwolą szybko i prawidłowo zareagować na naruszenie ochrony danych osobowych? Samo wykrycie incydentu to dopiero początek. Kluczowe znaczenie mają jasno określone zasady postępowania, podział odpowiedzialności oraz sposób oceny i dokumentowania naruszenia.

W niniejszym artykule pokazuję jakie procedury warto wdrożyć, ale robię to w konkretnym stanie faktycznym, a mianowicie na przykładzie wycieku dokumentów rekrutacyjnych.

Procedura wewnętrznego zgłaszania incydentów

Pierwszym elementem jest określenie, **kto, komu i w jaki sposób powinien zgłosić podejrzenie naruszenia ochrony danych osobowych**. A zatem procedura powinna wskazywać kanał zgłoszenia, zakres przekazywanych informacji oraz osoby odpowiedzialne za przyjmowanie i dalszą obsługę incydentów. Co istotne - pracownik nie musi samodzielnie rozstrzygać, czy doszło do naruszenia w rozumieniu RODO ani czy konieczne jest zgłoszenie do UODO. Jego zadaniem jest przekazanie informacji umożliwiających dalszą analizę.

Procedura zabezpieczenia danych i ograniczania skutków naruszenia

Organizacja powinna z góry określić, **jakie działania należy podjąć niezwłocznie po otrzymaniu zgłoszenia i kto odpowiada za ich wykonanie**.

W przypadku wycieku CV mogą one obejmować cofnięcie nieuprawnionego dostępu do dokumentów, zabezpieczenie historii udostępnień, ustalenie odbiorców danych oraz podjęcie działań zmierzających do usunięcia nieuprawnionych kopii. Należy jednak pamiętać, że samo usunięcie plików lub cofnięcie dostępu nie zawsze eliminuje skutki naruszenia. Dlatego procedura powinna przewidywać również weryfikację skuteczności podjętych działań.

Procedura analizy naruszenia i oceny ryzyka

Kolejnym elementem jest określenie zasad ustalania, czy konkretne zdarzenie stanowi naruszenie ochrony danych osobowych oraz jakie może powodować konsekwencje dla osób, których dane dotyczą.

W przypadku wycieku CV szczególne znaczenie mogą mieć:

- rodzaj ujawnionych danych, np. dane kontaktowe, historia zatrudnienia, data urodzenia,
- liczba kandydatów objętych naruszeniem,
- czas, przez jaki dokumenty były dostępne osobom nieuprawnionym,
- możliwość dalszego wykorzystania lub rozpowszechnienia danych.

Ocena powinna uwzględniać zarówno prawdopodobieństwo wystąpienia negatywnych konsekwencji, jak i ich potencjalną wagę.

Procedura zgłaszania naruszeń do UODO i zawiadamiania osób

Organizacja powinna określić, **kto odpowiada za ocenę obowiązku zgłoszenia, kto przygotowuje zgłoszenie oraz w jaki sposób kontrolowane są terminy**. Warto tu wspomnieć o tym, że UODO jednoznacznie wskazuje, że zgłoszenia nie powinien dokonywać Inspektor Ochrony Danych, ponieważ może mieć to wpływ na jego niezależność.

Zgodnie z art. 33 RODO administrator zgłasza naruszenie właściwemu organowi nadzorczemu, chyba że jest mało prawdopodobne, aby skutkowało ono ryzykiem naruszenia praw lub wolności osób fizycznych.

Jeżeli zgłoszenie jest wymagane, należy go dokonać bez zbędnej zwłoki, w miarę możliwości nie później niż w ciągu 72 godzin od stwierdzenia naruszenia.

Jeżeli naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, co do zasady konieczne jest również zawiadomienie osób, których dane dotyczą, bez zbędnej zwłoki, z uwzględnieniem wyjątków określonych w art. 34 RODO.

Za realizację tych obowiązków odpowiada administrator danych. Inspektor Ochrony Danych, jeżeli został wyznaczony, może pełnić wyłącznie funkcję doradczą i wspierać kontakt z organem nadzorczym.

Procedura dokumentowania naruszeń i działań naprawczych

Każde stwierdzone naruszenie ochrony danych osobowych należy udokumentować, niezależnie od tego, czy wymaga zgłoszenia do UODO. Procedura powinna określać sposób prowadzenia dokumentacji, osoby odpowiedzialne za jej przygotowanie oraz zasady odnotowywania podjętych decyzji. Ponadto dokumentacja powinna umożliwiać odtworzenie okoliczności naruszenia, jego skutków oraz zastosowanych działań zaradczych. Należy również uwzględnić ocenę ryzyka i uzasadnienie decyzji o zgłoszeniu lub odstąpieniu od zgłoszenia.

Podsumowanie

Wskazane obszary mogą zostać uregulowane w ramach jednej procedury, która jasno określa:

- sposób zgłaszania i obsługi incydentów;
- podział zadań i odpowiedzialności;
- zasady zabezpieczania danych i oceny ryzyka;
- sposób realizacji obowiązków wobec UODO i osób, których dane dotyczą;
- zasady dokumentowania naruszeń i wdrażania działań naprawczych.

Warto również okresowo weryfikować, czy przyjęta procedura odpowiada rzeczywistym procesom w organizacji i czy pracownicy wiedzą, jak z niej korzystać.

Dobrze przygotowana procedura to nie tylko dokument – to przede wszystkim jasna instrukcja działania, która pozwala organizacji sprawnie reagować w sytuacji naruszenia ochrony danych osobowych.

Olga Skotnicka – ekspertka ds. ochrony danych osobowych w iSecure Sp. z o.o.