

COMPLIANCE INSIGHTS

Vol. 106

Pracownik wystąpił
dane do
niewłaściwego
odbiorcy. Co
powinna zrobić
firma?



1. Jedno kliknięcie za wcześnie

Piątek, 16:40. Pracownik wpisuje trzy litery nazwiska, odpowiedź podstawia nie tego Kowalskiego, załącznik z danymi kadrowymi idzie w świat. Za minutę ktoś zauważa pomyłkę. I wtedy pada pytanie, na które firma ma dosłownie godziny: zgłaszamy do UODO czy nie? Odpowiedź nie brzmi ani „zawsze”, ani „nigdy”.

Pokazujemy, jak podjąć decyzję, jak ocenić ryzyko i czego nie wolno odkładać na poniedziałek rano.



2. Tak, to już jest naruszenie

Po takim zdarzeniu często pada zdanie: „to przecież tylko e-mail”. Intuicja podpowiada, że sprawa jest zamknięta. Art. 4 pkt 12 RODO mówi inaczej: **naruszeniem jest każde nieuprawnione ujawnienie danych, także przypadkowe.**

Wysłanie pliku pod zły adres tę definicję spełnia. Ale uwaga – naruszenie nie jest tym samym, co obowiązek zgłoszenia. Wiadomość do sąsiedniego działu i lista płac u zewnętrznego kontrahenta to dwie zupełnie różne historie, mimo identycznego błędu.



3. Najgorsze co może zrobić pracownik? Zamilknąć

Im później zdarzenie trafi do właściwych osób, tym mniej czasu pozostaje na ocenę ryzyka i działania naprawcze.

Tymczasem pracownicy milczą, obawiając się konsekwencji, albo nie wiedzą, do kogo pójść. Informacja musi trafić do IOD lub Compliance, nie utknąć w zespole. Sprawna ścieżka zgłaszania to nie dobra wola zespołu, lecz element środków bezpieczeństwa wymaganych przez art. 24 ust. 1 i art. 32 ust. 1 RODO.



4. Zanim zdecydujesz „zgłaszamy”, odpowiedz na pięć pytań

Jakie dane wyciekły? Ilu osób dotyczą? Kto je otrzymał i czy można mu ufać? Czy na ich podstawie da się zidentyfikować konkretną osobę? Co realnie może ją spotkać?

Pięć pytań, jedna notatka – i decyzja przestaje być intuicyjna. Ten sposób myślenia porządkują wytyczne EROD nr 9/2022 dotyczące zgłaszania naruszeń. Warto również sprawdzić dwie kwestie techniczne: czy plik był zaszyfrowany i czy hasło zostało wysłane zupełnie innym kanałem.



5. Ten sam błąd, dwa różne scenariusze

Scenariusz pierwszy: zaszyfrowany plik trafia do stałego kontrahenta związanego umową o poufności, który usuwa go w 15 minut i potwierdza to e-mailem. Ryzyko niskie, art. 34 ust. 3 lit. a RODO w tle.

Scenariusz drugi: zestawienie z numerami PESEL i danymi o zdrowiu (art. 9 ust. 1 RODO) trafia do nieznanego adresata, który nie odbiera telefonu i nie odpowiada na e-maile. W tym przypadku ocena ryzyka zwykle prowadzi do wniosku o konieczności zgłoszenia naruszenia oraz poinformowania osób, których dane dotyczą.



6. Od kiedy liczy się 72 godziny?

72 godziny to nie termin od zakończenia analizy. Zegar rusza w chwili, gdy firma z wystarczającą pewnością wie, że coś się stało – czyli zwykle wtedy, gdy pracownik mówi o pomyłce położonemu. Przepis wymaga zgłoszenia bez zbędnej zwłoki, w miarę możliwości w ciągu 72 godzin (art. 33 ust. 1 RODO). Jeśli nie są znane jeszcze wszystkie okoliczności, lepiej zgłosić w powyższym terminie to, co już znane, a pozostałe informacje uzupełnić w późniejszym terminie (art. 33 ust. 4 RODO).



7. Kiedy trzeba zawiadomić osoby, których dane dotyczą?

Gdy naruszenie może powodować wysokie ryzyko dla osób, których dane dotyczą, trzeba zawiadomić je bez zbędnej zwłoki (art. 34 ust. 1 RODO). Komunikat ma być napisany jasnym i prostym językiem oraz zawierać opis charakteru naruszenia, możliwe konsekwencje, zastosowane środki i dane punktu kontaktowego lub inspektora ochrony danych (art. 34 ust. 2 w zw. z art. 33 ust. 3 lit. b-d RODO). Dokumentacja wysyłki jest tu równie ważna jak sama treść.



8. Jakie są działania ograniczające skutki incydentu?

Równolegle należy ograniczać skutki zdarzenia: wycofać wiadomość, jeśli system pocztowy na to pozwala, poprosić odbiorcę o trwałe usunięcie pliku i uzyskać pisemne potwierdzenie, zablokować dostęp do dokumentu w chmurze. Skuteczne działania podjęte po naruszeniu mogą wyeliminować wysokie ryzyko i zwolnić administratora z obowiązku zawiadamiania osób na podstawie art. 34 ust. 3 RODO.



9. Wewnętrzna ścieżka postępowania

Procedurę warto przygotować zawczasu, a nie po wystąpieniu incydentu. Składają się na nią: jasna ścieżka zgłaszania, wskazanie osób decyzyjnych, formularz oceny ryzyka oraz szablony zawiadomień dla organu i dla osób. Uzupełnieniem są szkolenia i rozwiązania techniczne, jak opóźniona wysyłka czy ostrzeżenie o adresacie zewnętrznym (art. 32 RODO).



Compliance Insight



Mariusz Purgał

Partner

mariusz.purgal@kwkr.pl
+48 797 927 960



Natalia Kangier

Associate

natalia.kangier@kwkr.pl
+48 516 574 037

Zapraszamy do kontaktu

KWKR.

Behind Your **Growth**