Kiedy wycieką dane klienta, a adresu do korespondencji brak

Posted on 2026-11-02

Zgodnie z RODO w przypadku naruszenia ochrony danych osobowych, które może generować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator ma obowiązek bez zbędnej zwłoki poinformować o tym osoby, których te dane dotyczą. „Bez zbędnej zwłoki", a więc najszybciej, jak to możliwe. Zawiadomienie to ma na celu przede wszystkim dostarczenie im szczegółowych informacji na temat działań zapobiegawczych, które powinny podjąć – im szybciej ono nastąpi, tym większe szanse uchronienia się przed negatywnymi skutkami naruszenia.

Problemy zaczynają się, gdy bezpośredni kontakt z osobą, której dane dotyczą jest niemożliwy lub wymagałby „niewspółmiernie dużego wysiłku". Może to dotyczyć sytuacji gdy administrator posiada w swej bazie jedynie imię, nazwisko oraz numer PESEL, ale nie dysponuje aktualnym adresem e-mail, nr telefonu czy adresem zamieszkania (dane zebrane jednorazowo przy dawnych projektach, w celach promocyjnych etc.) lub w wyniku naruszenia utracono dane kontaktowe osób fizycznych albo dane te nigdy nie były znane administratorowi.

Zasadą jest, że jeżeli administrator nie jest w stanie zawiadomić osoby fizycznej o naruszeniu, ponieważ przechowywane dane są niewystarczające do skontaktowania się z tą osobą, powinien ją poinformować tak szybko, jak jest to rozsądnie wykonalne (np. jeżeli

osoba fizyczna skorzysta z przewidzianego w art. 15 RODO prawa do uzyskania dostępu do swoich danych osobowych i dostarczy administratorowi dodatkowe informacje wymagane do skontaktowania się z nią)[1]. A zatem jeśli taka osoba sama zgłosi się do administratora i uwierzytelniając się poda aktualne dane kontaktowe, musi on niezwłocznie przekazać jej zaległą informację o incydencie.

Pomoc w art. 34 RODO, czyli komunikat publiczny

Jeśli natomiast skontaktowanie się z takimi osobami fizycznymi wymagałoby niewspółmiernie dużego wysiłku, zastosowanie znajdzie art. 34 ust. 3 lit. c RODO. Przepis ten zdejmuje z administratora obowiązek indywidualnego zawiadomienia każdej osoby, jeśli wymagałoby to „niewspółmiernie dużego wysiłku". W zamian nakazuje jednak zastosowanie publicznego komunikatu lub podobnego środka, dzięki któremu osoby, których dane dotyczą zostaną poinformowane w równie skuteczny sposób.

Niewspółmierność powinna być oceniana z uwzględnieniem skali ryzyka, rodzaju zagrożonych praw lub wolności podmiotu danych, a także czasu, w jakim zgodnie z przepisem art. 34 ust. 1 RODO obowiązek zawiadomienia powinien zostać zrealizowany. Jeżeli zatem administrator nie posiada danych kontaktowych osób, których dotyczy naruszenie, to wymóg ich pozyskania powinien być oceniony jako związany z niewspółmiernie dużym wysiłkiem. Podobnie, jeżeli administrator posiada jedynie numery telefonów do podmiotów danych, ale nie dysponuje zasobami, które pozwoliłyby mu sprawnie do każdego z nich zadzwonić[2].

Kiedy faktycznie występuje „niewspółmiernie duży wysiłek”?

Przepisy nie podają konkretnych liczb czy sposobu obliczania takich wartości, wymagając od administratora indywidualnej oceny tego typu przypadków. W praktyce przesłanka ta jest uznawana w sytuacji, kiedy administrator nie posiada danych kontaktowych i niemożliwe jest ich łatwe ustalenie, a koszt i czas do tego potrzebne byłyby ogromne dla organizacji administratora.

Czym „niewspółmiernie duży wysiłek” nie jest?

Przesłanka ta nie zachodzi, gdy chodzi o wysokie koszty finansowe. Warto tutaj wspomnieć o pierwszej karze nałożonej przez Prezesa Urzędu Ochrony Danych Osobowych za naruszenie obowiązków informacyjnych administratora na spółkę Bisnode (obecnie Dun & Bradstreet), w której NSA potwierdził, że pojęcie niewspółmiernie dużego wysiłku nie może być utożsamiane z wysokością kosztów, jakie administrator zmuszony będzie ponieść w związku z koniecznością dopełnienia obowiązku, który jest w pełni możliwy do realizacji, bowiem zarówno kwestie organizacyjne, jak i finansowe nie przeważają nad prawami osób fizycznych, których dane osobowe przetwarzane są przez administratora[3]. A więc sam fakt konieczności zapłacenia znacznej kwoty na wysyłkę listów (nawet dla milionów osób) nie jest

„niewspółmiernie dużym wysiłkiem”, jeśli administrator posiada aktualne adresy tych osób.

Jak powinien wyglądać publiczny komunikat?

Jeśli nie jest możliwe bezpośrednie zawiadomienie osoby, której dane dotyczą poprzez wysłanie listu, e-maila, czy sms należy upublicznić informację o naruszeniu. Komunikat taki powinien być łatwo dostępny dla potencjalnych „poszkodowanych”. Wbrew pozorom nie wystarczy jednak opublikowanie lakonicznej notki w mało widocznej zakładce na stronie internetowej. Komunikat zastępczy musi być tak samo skuteczny jak wiadomość prywatna skierowana do podmiotu danych.

Najskuteczniejsze metody to:

- Ogłoszenie na stronie internetowej: umieszczenie wyraźnego, rzucającego się w oczy komunikatu (np. w formie baneru lub specjalnej podstrony) na stronie głównej administratora.
- Media społecznościowe: publikacja informacji na oficjalnych profilach administratora (Facebook, LinkedIn itp.).
- Komunikat w lokalnej prasie lub mediach: jeśli naruszenie dotyczy osób z konkretnego regionu.
- Tablice ogłoszeń: w widocznych miejscach w fizycznej siedzibie administratora, jeśli osoby, których dane dotyczą tam bywają.
  Powiadomienie, które jest tylko częścią komunikatu prasowego lub zostało zamieszczone na blogu przedsiębiorstwa, nie byłoby skuteczną metodą zawiadomienia osób fizycznych o naruszeniu. EROD zaleca, aby administratorzy wybierali metody pozwalające zapewnić jak największą szansę właściwego przekazania informacji wszystkim osobom fizycznym, na

które to naruszenie wywiera wpływ. W niektórych okolicznościach może to oznaczać, że administrator wykorzysta szereg metod komunikacji, a nie tylko jeden kanał kontaktowy[4].

Co musi zawierać komunikat?

---

[1] Zob. EROD, Wytyczne nr 9/2022 dotyczące zgłaszania naruszenia ochrony danych osobowych na podstawie RODO, wersja 2.0, przyjęte 28 marca 2023 r., pkt 96.

[2] W. Chomiczewski [w:] RODO. Ogólne rozporządzenie o ochronie danych. Komentarz, red. E. Bielak-Jomaa, D. Lubasz, Warszawa 2018, art. 34.

[3] Zob. wyrok NSA z dnia 19 września 2023 r., III OSK 2538/21.

[4] Zob. EROD, Wytyczne nr 9/2022 dotyczące zgłaszania naruszenia ochrony danych osobowych na podstawie RODO, wersja 2.0, przyjęte 28 marca 2023 r., pkt 90.