



Ile mam czasu na zgłoszenie RODO naruszenia?

Opinia ZFODO

Termin 72 h na zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu zaczyna biec od momentu „stwierdzenia naruszenia” (art. 33 ust. 1 RODO). Stwierdzenie naruszenia nie zawsze wystąpi w tym samym momencie, w którym doszło do naruszenia. W związku, z wątpliwościami w tym zakresie postanowiliśmy wypracować wspólne stanowisko, jako Związek Firm Ochrony Danych Osobowych.

Czas płynie... ale względnie

Jeśli wykryłeś naruszenie, to na pewno odczuwasz presję czasu - 72 godzin, o których mowa w art. 33 ust. 1 RODO. Pamiętaj jednak o tym, że w sytuacjach związanych z naruszeniami, czas płynie nieco inaczej.

A przynajmniej nie zawsze będzie liczony od tego samego momentu.

W ocenie ZFODO powoływany wyżej przepis RODO należy interpretować w ten sposób, że **po wykryciu prawdopodobieństwa wystąpienia naruszenia, administrator niezwłocznie podejmuje działania, aby dokonać stwierdzenia, czy do naruszenia rzeczywiście doszło** i jaki ewentualnie wpływ na prawa lub wolności podmiotów danych może ono mieć.

Poniżej dwa proste przykłady obrazujące powyższe:

Naruszenie:	Moment wykrycia:	Moment stwierdzenia naruszenia:	Podsumowanie:
20 marca 2020 r. lekarz udostępnił dokumentację medyczną pacjenta innemu pacjentowi.	20 marca 2020 <i>(udostępnienie dokumentacji)</i>	20 marca 2020	Naruszenie ma oczywisty charakter. Lekarz poinformował administratora o swoim błędzie niezwłocznie po wydaniu dokumentacji. Administrator bez zbędnej zwłoki przeprowadził postępowanie wyjaśniające i jeszcze tego samego dnia spisany został protokół naruszenia oraz oszacowane zostało ryzyko naruszenia praw i wolności pacjenta, którego dane zostały bezprawnie ujawnione. Moment wykrycia naruszenia pokrywa się zatem z momentem jego stwierdzenia.





<p>20 marca 2020 r. pracownik Działu IT zauważa, że na ogólnie dostępnym serwerze dostępny jest plik z wykazem urlopów każdego z pracowników administratora.</p> <p>Plik został zamieszczony ok. tydzień temu tj. 12 marca 2020 r.</p>	<p>12 marca 2020</p> <p><i>(pojawienie się pliku na ogólnodostępnym serwerze)</i></p>	<p>22 marca 2020</p>	<p>Pracownik Działu IT zgłasza administratorowi naruszenie tego samego dnia, w którym odkrył nieprawidłowość tj. 20 marca 2020 r.</p> <p>Administrator niezwłocznie podejmuje działania wyjaśniające. Ustala kto zamieścił plik, kontaktuje się z Działem IT celem określenia, czy i przez kogo plik był przeglądany, czy też kopiowany, pobierany lub w inny sposób zapisywany, etc. Postępowanie wyjaśniające trwa 2 dni tj. do 22 marca 2020 r. Do tego czasu administrator ustalił jak plik znalazł się na dysku, czy ktokolwiek go zapisał oraz jaki wpływ na prawa i wolności osób, których dane zostały ujawnione miało to naruszenie.</p> <p>Termin zaczyna biec po stwierdzeniu naruszenia tj. 22 marca 2020 r.</p>
--	--	-----------------------------	--



Zminimalizuj ryzyko naruszenia RODO w Twojej organizacji – przeszkól zespół.

Zależy Ci na tym aby Twoi pracownicy otrzymali certyfikat i poznali praktyczną wiedzę z zakresu RODO zamiast nużących reguł?

Sprawdź nasze interaktywne szkolenia e-learningowe.

SPRAWDŹ

Inne interpretacje oraz stanowisko ZFODO

Powyższa interpretacja znajduje oparcie w wytycznych Grupy Roboczej Art. 29WP250rev.01 (ostatnio zmienionych i przyjętych w dniu 6 lutego 2018 r.)W swojej opinii GR Art. 29 przyjęła, że należy uznać, że administrator **stwierdził** wystąpienie naruszenia w momencie, w którym uzyskał **wystarczającą dozę pewności** co do tego, że doszło do wystąpienia incydentu bezpieczeństwa, który doprowadził do ujawnienia danych osobowych.





Jestem świadom, że funkcjonują obecnie również inne podejścia i stanowiska. Na przykład takie, które termin 72 godzin każą liczyć od momentu wykrycia naruszenia (wykrycie=stwierdzenie).

W gronie profesjonalnych firm zrzeszonych w ramach ZFODO, przeanalizowaliśmy wszystkie argumenty za oraz przeciw obecnie funkcjonującym poglądom w tym temacie.

Za najtrafniejsze i najbardziej zdroworozsądkowe, uznaliśmy stanowisko prezentowane w niniejszym artykule.

Całe stanowisko dostępne jest na [stronie Związku Firm Ochrony Danych Osobowych](#).

Zapraszam do zapoznania się i stosowania w praktyce!

Autor artykułu:

Przemysław Zegarek, Prezes Zarządu

Źródła:

- 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)
- praktyczne doświadczenie budowania systemów ochrony danych osobowych od 2008 roku (jako ABI) i po 2018 roku (jako IOD)

