ZFODO

Warszawa, dnia 05/02/2020

STANOWISKO ZWIĄZKU FIRM OCHRONY DANYCH OSOBOWYCH („ZFODO") DOTYCZĄCE USTALENIA BIEGU TERMINU NA ZGŁOSZENIE PREZESOWI UODO NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Zgodnie z art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Analizując wspomniany przepis pojawia się pytanie, kiedy administrator „stwierdza naruszenie"? W opinii Grupy Roboczej Art. 29 administrator „stwierdził" wystąpienie naruszenia w momencie, w którym uzyskał wystarczający stopień pewności co do tego, że miało miejsce zdarzenie zagrażające bezpieczeństwu, które doprowadziło do naruszenia ochrony danych[1]. Analogiczne stanowisko zajął Prezes Urzędu Ochrony Danych Osobowych, który w wydanym poradniku dotyczącym obowiązków administratorów związanych z naruszeniami ochrony danych osobowych powołał się na wskazane stanowisko Grupy Roboczej Art. 29.[2]

ZFODO zgadza się ze stanowiskiem organów oraz doktryny. Nie ulega bowiem wątpliwości, iż celem ustawodawcy unijnego było wprowadzenie takich przepisów, które zobowiązują administratora do szybkiego reagowania w przypadku wystąpienia zdarzenia, które może stanowić naruszenie ochrony danych osobowych.

W kontekście ustalenia biegu terminu na zgłoszenie Prezesowi UODO naruszenia ochrony danych osobowych nadal pojawiają się jednak pewne wątpliwości interpretacyjne. Administrator jest zobowiązany do zgłaszania

[1] Wytyczne Grupy Roboczej art. 29 dotyczące zgłaszania naruszeń ochrony danych osobowych zgodnie z rozporządzeniem 2016/679 (WP250), str. 12, https://uodo.gov.pl/pl/10/12, dostęp 24/01/2020.

[2] Poradnik UODO „Obowiązki administratorów związane z naruszeniami ochrony danych osobowych"; wersja 1.0, czerwiec 2019, str. 10, https://www.uodo.gov.pl/pl/134/1029, dostęp 24/01/2020.

Związek Firm Ochrony Danych Osobowych, zarejestrowany w Rejestrze Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000752344, REGON: 381540557, NIP: 7010875519.

ZFODO

Prezesowi UODO naruszenia ochrony danych osobowych, gdy **naruszenie stwarza prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych**.

W związku z powyższym w ocenie ZFODO niniejszy przepis 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.

Po przeprowadzeniu czynności sprawdzających, administrator powinien opracować protokół, w którym:

1) stwierdza się wystąpienie naruszenia lub wskazuje, że do naruszenia nie doszło,
2) określa się kwalifikację naruszenia, tj. czy powoduje ryzyko naruszenia praw i wolności osób fizycznych, a jeżeli tak to w jakim stopniu (niskim / średnim / wysokim).

Kwalifikacja stopnia ryzyka jest o tyle istotna, że zgodnie z art. 34 ust. 1 RODO jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator zobowiązany jest powiadomić o nim nie tylko organ nadzoru, ale również osobę, której dane dotyczą.

Poszczególne etapy postępowania w tym zakresie obrazuje grafika stanowiąca załącznik do niniejszego stanowiska.

Czynności sprawdzające powinny być przeprowadzane przez administratora bez zbędnej zwłoki, tak, aby ewentualne stwierdzenie naruszenia i kwalifikacja ryzyka naruszenia praw i wolności osób fizycznych odbyły się możliwie w jak najkrótszym czasie. Takie postępowanie uzasadnia motyw 85 preambuły do RODO, w którym ustawodawca unijny wskazał, że brak odpowiedniej i szybkiej reakcji na naruszenia ochrony danych osobowych zwiększa ryzyko związanej z nimi szkody po stronie podmiotów danych.

Zarząd Związku Firm Ochrony Danych Osobowych:

Związek Firm Ochrony Danych Osobowych, zarejestrowany w Rejestrze Stowarzyszeń, Innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej Krajowego Rejestru Sądowego przez Sąd Rejonowy dla m. st. Warszawy w Warszawie, XII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS: 0000752344, REGON: 381540557, NIP: 7010875519.

Załącznik do stanowiska ZFODO