ZFODO

Związek Firm Ochrony Danych Osobowych


**Zespół odpowiedzialny za przygotowanie materiału:**
Justyna Głuchowska - Auraco Sp. z o.o.
Alicja Kaczkowska - JDS Consulting Sp. z o.o. Sp. k.
Agnieszka Duda - JDS Consulting Sp. z o.o. Sp. K.
Katarzyna Ramotowska - ODO Management Group Sp. z o.o.
Maciej Wara – Wąsowski - ODO Management Group Sp. z o.o.
Małgorzata Gudfinnsson - Lex Artsit Sp. z o.o.
Marcin Szkutnik – Lex Artist Sp. z o.o.
Uwagi i sugestie przekazała również firma ODO24 Sp. z o.o.

Warszawa, dn. 20.06.2024 r.

## 1. Pojęcie naruszenia ochrony danych osobowych.

1. Dotyczy str. 3 Poradnika. **Pytanie:** Czy w opinii Urzędu Ochrony Danych Osobowych naruszenie ochrony danych osobowych zawsze będzie skutkiem złamania zasad bezpieczeństwa danych i co UODO rozumie pod tym pojęciem? Czy w sytuacji, gdy mamy do czynienia tylko i wyłącznie z błędem ludzkim, polegającym na wpisaniu błędnego adresu na kopercie i wysłaniu dokumentu z danymi osobowymi na nieprawidłowy adres będziemy mieli do czynienia ze złamaniem zasad bezpieczeństwa danych?

2. **Sugestia:** W opinii ZFODO zasadnym byłoby wyjaśnienie co UODO rozumie pod pojęciem "złamanie zasad bezpieczeństwa danych", żeby administratorzy nie mieli wątpliwości, czy dane naruszenie (np. to przytoczone powyżej") stanowi złamanie zasad bezpieczeństwa danych. Chyba, że w opinii UODO nie stanowi, wówczas należałoby zmienić brzmienie 3 przesłanki wystąpienia naruszenia.

3. Dotyczy str. 4 Poradnika. **Sugestia:** W opinii ZFODO należałoby doprecyzować co rozumiemy pod tym pojęciem i dodać jeden z podstawowych przykładów naruszenia integralności danych, jakim jest atak ransomware (szyfrowanie danych, pozostawiając je w stanie nienadającym się do użytku) i który jest szerzej opisany w dalszej części Poradnika (str. 20).

## 2. Obowiązki podmiotów

1. Dotyczy str. 5 Poradnika. **Sugestia:** W ostatnim akapicie tego punktu Poradnika, gdzie wskazany jest najważniejszy element procesu zgłaszania naruszeń, należałoby odnieść się do tytułu tej części, a nie do samego procesu zgłaszania naruszeń, tzn. co jest najważniejszym elementem procesu obsługi naruszeń. Zdaniem ZFODO nie będzie to szybkość zawiadomienia organu nadzorczego, a bardziej szybkość podjęcia środków zaradczych i zawiadomienie osób, których dane dotyczą.

## 3. Termin zawiadomienia:

1. **Sugestia:** Zapisy w tym punkcie budzą wątpliwości interpretacyjne, polegające na tym, że nie jest jasne jak liczyć 72h od stwierdzenia naruszenia przez podmiot przetwarzający. Czy od tego momentu, czy też 72h liczymy od stwierdzenia naruszenia przez administratora? Wówczas po otrzymaniu bez zbędnej zwłoki informacji o naruszeniu od procesora, jest ono przez administratora weryfikowane i dopiero po uznaniu przez administratora, że do naruszenia w podmiocie przetwarzającym doszło i wykonaniu analizy ryzyka naruszenia praw i wolności osób fizycznych, naruszenie jest zgłaszane do UODO.
   RODO nie precyzuje tej kwestii, dlatego wskazane byłoby doprecyzowanie tego w Poradniku.

2. **Sugestia**: Zgodnie z Wytycznymi EROD 9/2022 możliwe jest przyjęcie, że zgłoszenia naruszenia dokonuje podmiot przetwarzający, powiadamiając jednocześnie ADO i za jego zgodą (uregulowane w umowie powierzenia) - biorąc pod uwagę czas w jakim należy powiadomić PUODO o naruszeniu (np. firmy telekomunikacyjne – 24h) i niekiedy utrudniony przepływ informacji między ADO a PP, wskazane byłoby dopuszczenie takiej możliwości poprzez zawarcie odpowiednich zapisów w Poradniku.

3. **Sugestia:** Dookreślenie terminu „stwierdzenia naruszenia" celem uniknięcia wątpliwości interpretacyjnych.

**Komentarz:** Art. 33 ust. 1 RODO należałoby 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).
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.

## 4. Zgłoszenie zawiadomienia

1. Dotyczy str. 7 poradnika. “Zgłaszanie naruszeń”. **Uwaga:** Brak informacji w poradniku na temat naruszeń transgranicznych. Przypadków w których organizacje mają oddziały w kilku krajach UE. Sugestia: Dodanie akapitu na temat zgłaszania naruszeń transgranicznych. Ścieżka postępowania w takich przypadkach. Rekomendacje na temat wyboru właściwego urzędu w przypadku naruszeń, które dotyczą spółek powiązanych, mających siedziby w kilku krajach UE

2. Dotyczy str. 8 poradnika. **Sugestia:** W opinii ZFODO należałoby dodać w Poradniku, na wzór części D Wytycznych EROD 9/2022, zapisy dotyczące warunków, w których zgłoszenie naruszenia nie jest wymagane - usprawni to pracę ADO i zmniejszy liczbę niepotrzebnych zgłoszeń do PUODO.

3. **Sugestia:** Dodatkowo wskazane byłoby doprecyzowanie pojęcia “odbiorcy zaufani” na wzór pojęcia przedstawionego w Wytycznych 9/2022 oraz zamieszczenie w Poradniku listy odbiorców zaufanych (np. administracja publiczna, gdzie udostępnienie danych niewłaściwemu urzędowi powoduje zgodnie z kpa przekazanie sprawy wg właściwości i nie powinno w naszej opinii być zgłaszane jako naruszenie).

4. Dotyczy str. 10 poradnika. **Sugestia:** W 1 akapicie w ostatnim zdaniu powinno być “zawiadomienie z opóźnieniem”, o którym mowa w części B.3 Wytycznych EROD, a nie “zawiadomienie sukcesywne”; ponadto nie zawsze zawiadomienie z opóźnieniem będzie wiązało się z zawiadomieniem sukcesywnym, ponieważ można w zawiadomieniu z opóźnieniem zawrzeć wszystkie posiadane informacje w związku ze zdarzeniem, przykładem jest tutaj tzw. “zawiadomienie pakietowe”, o którym mowa w pkt. 64 Wytycznych EROD.

5. Dotyczy str. 11 Poradnika „Najczęściej popełniane błędy podczas zgłaszania naruszeń” oraz Str. 29 Poradnika „Najczęściej popełniane błędy podczas zawiadamiania osób” **Sugestia:** Aktualizacja przez organ wskazanych wyżej części Poradnika o najnowsze doświadczenia organu.

## 5. Określanie ilości wpisów.

1. **Pytanie:** Jak w opinii PUODO należy prawidłowo określić liczbę wpisów danych osobowych, których dotyczy naruszenie? Z uwagi na rozbieżności w praktyce, rekomendujemy przyjęcie koncepcji liczenia każdego osobnego rekordu danych jako pojedynczego wpisu.

   **Komentarz:** W opinii ZFODO jako wpis należy zaliczyć każdy rekord danych z osobna, tym samym, jeżeli naruszeniu podlega dokument zawierający następujące dane: imię i nazwisko, adres zamieszkania, telefon kontaktowy, adres e-mail, należy uznać, że naruszeniem objęte zostały 4 wpisy. Przy ocenie liczby wpisów należy wziąć pod uwagę liczbę dotkniętych systemów lub baz danych. Każdy system lub baza, w której doszło do naruszenia, powinna być uwzględniona osobno przy określaniu ilości wpisów.

## 6. Ocena naruszeń.

1. Dotyczy Str. 13, pkt. 9.1 Poradnika. **Sugestia:** dodanie wzmianki o tym, że pierwszym działaniem w celu stwierdzenia naruszenia powinno być uzyskanie pewności, że incydent dotyczy „danych osobowych" (a nie informacji, które nimi nie są np. informacji dotyczących osoby prawnej, danych finansowych). Sugeruje się również, dodanie informacji, że brak wiedzy na temat kategorii danych, których dotyczy naruszenie uniemożliwia dokonanie właściwej oceny ryzyka naruszenia.

   **Komentarz:** Wśród naruszeń ochrony danych osobowych są takie w których w pierwszej fazie postępowania wyjaśniającego administrator nie wie (lub nie jest pewien) jakiego zakresu danych (kategorii danych) on dotyczy. W niektórych przypadkach, może nawet nie mieć pewności czy naruszenie dotyczyło danych osobowych w rozumieniu art. 4 pkt. 12 RODO czy też innego rodzaju informacji takich jak np. informacje dotyczące osób prawnych, dane finansowe, zestawienia liczbowe. Brak wiedzy w tym zakresie w sposób istotny wpływa na możliwość stwierdzenia naruszenia, a następnie wykonania prawidłowej oceny ryzyka naruszenia praw lub wolności osób których dane dotyczą.

2. **Pytanie:** Jaki wpływ na ocenę poziomu ryzyka ma ogólna ilość informacji podlegających naruszeniu? Czy w przypadku ujawnienia bazy danych zawierającej dużą ilość rekordów lecz w przeliczeniu per osoba, do każdej osoby objętej naruszeniem można przypisać tylko jeden wpis, możliwe jest ogólne ustalenie ryzyka na poziomie niskim ze względu na małą dotkliwość naruszenia z osobna dla każdej osoby nim objętej?

3. **Sugestia:** Wskazanie czynników, które PUODO bierze pod uwagę, przy ustalaniu, że poziom ryzyka przyjęty przez administratora jest nieprawidłowy. Dotyczy to zwrócenia uwagi na główne rozbieżności w ocenach administratorów i tych dokonywanych przez organ.

   **Komentarz:** Należy rozbudować poradnik o wskazania dotyczące metodyki/analizy określenia poziomu z uwzględnieniem decyzji PUODO, w których kwestionowano adekwatność

przeprowadzonej analizy naruszenia. W dotychczasowej treści poradnika wskazane zostały w pkt. 9.2 kryteria oceny ryzyka dla osób fizycznych będącego wynikiem naruszenia. W praktyce zdarzały się sytuacji, że mimo udokumentowania przez administratorów oceny ryzyka, nie była ona podzielana przez Organ. Istotne jest, aby organizacja już na poziomie kwalifikacji naruszenia uwzględniła właściwe kryteria oraz poziomy ryzyka.

4. Dotyczy str. 13 poradnika. **Sugestia**: aktualizacja rekomendowanych metod oceny ryzyka. ENISA jest datowana na 2013 rok. Żyjemy w środowisku nowych technologii, które dynamicznie zmieniają sposoby zabezpieczeń (szczególnie informatycznych)

5. Dotyczy str. 17, pkt. 9.3 Poradnika. **Sugestia:** zmodyfikowanie fragmentu mówiącego o tym, że naruszenie polegające na zgubieniu lub wręczeniu niewłaściwej osobie dokumentu zawierającego imię, nazwisko i nr PESEL „w większości sytuacji" powoduje wysokie ryzyko poprzez wskazanie, że naruszenie dotyczące takiego zakresu danych „może powodować" takie ryzyko. Równocześnie sugeruje się dodanie nowego fragmentu mówiącego o tym, że dla oceny ryzyka naruszenia praw lub wolności osób których dane dotyczą decydujący jest całokształt okoliczności określonego stanu faktycznego, wśród których zakres danych ma duże znacznie, lecz nie jest najistotniejszy.

   **Komentarz:** Dla oceny skutków naruszenia ochrony danych, w tym w szczególności oceny ryzyka naruszenia praw lub wolności osób których dane dotyczą, zawsze istotne będą okoliczności określonego stanu faktycznego w którym doszło do naruszenia ochrony danych. W związku z tym, Poradnik, powinien przede wszystkim to akcentować. Nie powinien natomiast sugerować wyniku oceny ryzyka naruszenia w odniesieniu do określonych kategorii danych, nawet jeśli informacja na ten temat jest nieco złagodzona przez użycie określenia „w większości sytuacji". Istnieje bowiem wiele sytuacji, w których naruszenie obejmujące zestaw danych: imię, nazwisko i nr PESEL, w sposób obiektywny takiego ryzyka nie będzie powodowało np. gdy naruszenie dotyczy osoby której taki zakres danych jest już ujawniony w rejestrach KRS, naruszenie polega na wręczeniu dokumentu osobie nieuprawnionej, która po jego otrzymaniu natychmiast zauważyła, że zawiera on dane innej osoby i natychmiast go zwróciła.
   Proponowana zmiana ma na celu ograniczenie zbyt pochopnego przyjmowania wysokiego ryzyka dla naruszeń obejmujących dane w zakresie imię, nazwisko i nr PESEL w sytuacjach, gdy obiektywne okoliczności stanu faktycznego mogą tego nie uzasadniać.

## 7. Środki zaradcze.

1. **Sugestia:** Przedstawienie katalogu środków w celu zaradzenia naruszeniu ochrony danych osobowych, które powinien podjąć administrator danych, z uwzględnieniem dotychczasowych decyzji organu.

   **Komentarz:** W celu zapewnienia właściwej ochrony danych osobowych, niezbędne jest opracowanie kompleksowego katalogu środków zaradczych, które mogą być podjęte przez administratora w przypadku naruszenia ochrony danych osobowych. Z uwagi na liczne postępowania i doświadczenia UODO w tej materii rekomendowane jest przedstawienie katalogu działań i najlepszych praktyk, które z uwzględnieniem doświadczeń Urzędu powinny być powszechnie stosowane.

2. **Sugestia:** Przedstawienie w poradniku katalogu środków proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych lub w celu zminimalizowania jego ewentualnych negatywnych skutków, które może zastosować osoba zawiadomiona o naruszeniu jej danych osobowych. Rekomendacja dotyczy wskazania najczęściej powoływanych w postępowaniach organu środków, które należy uzupełnić zawiadamiając osobę.

   **Komentarz:** Prośba dotyczy przedstawienia przez UODO katalog środków, które osoby te mogą zastosować, aby chronić swoje dane i zminimalizować potencjalne negatywne konsekwencje naruszenia. Rekomendacja ma na celu wyjście naprzeciw oczekiwaniom Urzędu oraz najlepszym praktykom w zakresie niesienia pomocy i wsparcia osobom, których prawa zostały naruszone.

3. **Sugestia:** Podniesienie roli oświadczenia o niewykorzystaniu przekazanych omyłkowo informacji do celów prywatnych i/lub niezgodnych z prawem. Zachęcenie administratorów do odbierania takich oświadczeń w ramach prowadzonych działań po naruszeniu. Oświadczenie takie nie będzie miało wpływu na poziom ryzyka lecz może mieć realny wpływ na kwestie ewentualnego odszkodowania za szkodę niemajątkową na podstawie RODO.

   **Komentarz:** Trybunał Sprawiedliwości UE w wyroku w sprawie C-340/21, który dotyczył kwestii warunków odszkodowania za szkodę niemajątkową, uznał, że jeśli osoba nieuprawniona nie zapoznała się z danymi osobowymi, nad którymi administrator utracił kontrolę, to sama obawa o ich bezprawne wykorzystanie nie może być podstawą roszczenia odszkodowawczego. Odebrane przez administratora danych oświadczenie o niewykorzystaniu przekazanych omyłkowo informacji do celów prywatnych i/lub niezgodnych z prawem będzie miało zatem praktyczne znaczenie w kontekście skutków naruszenia oraz ewentualnych roszczeń osoby, której dane dotyczą.

4. Dotyczy str.20, pkt. 11, ppkt 2 Poradnika ("Jakie działania należy podejmować w celu ograniczenia występowania najczęstszych typów naruszeń ochrony danych osobowych?") **Sugestia:** wskazanie przykładowych środków technicznych, które mogą zapobiegać naruszeniom polegającym na wysyłaniu pocztą email danych do nieuprawnionego adresata. Przykładowe środki to np. szyfrowanie przesyłanych plików, aktywowanie określonych funkcjonalności w koncie poczty email takich jak: ostrzeganie nadawcy wiadomości przed wysłaniem jej do adresata spoza jego organizacji, opóźnienie wysyłki wiadomości, wysyłanie wiadomości testowej w celu weryfikacji prawidłowości adresu email Sugeruje się także, aby Poradnik rekomendował inne metody przekazywania dokumentów drogą elektroniczną takie jak zamieszczanie dokumentów w dedykowanych aplikacjach do których dostęp jest możliwy wyłącznie po uwierzytelnieniu użytkownika np. zalogowaniu za pomocą loginu i hasła.

   **Komentarz:** wskazanie konkretnych rozwiązań może być pomocne dla administratorów, szczególnie tych którzy nie dysponują odpowiednimi zasobami technicznymi i organizacyjnymi. Podanie przykładów rekomendowanych środków technicznych może w konsekwencji przyczynić się do zmniejszenia ilości tego rodzaju naruszeń. Jak wynika z informacji publikowanych przez Prezesa UODO naruszenia polegające na nieprawidłowym zaadresowaniu korespondencji tradycyjnej i elektronicznej są od lat jednym z najczęściej zgłaszanych przez administratorów naruszeń ochrony danych (Źródło: Sprawozdanie z działalności Prezesa Urzędu Ochrony Danych Osobowych w roku 2022).

## 8. Zawiadomienie osoby

1. **Sugestia:** Należy dodać zastrzeżenie nr PESEL jako jedną z form zabezpieczenia danych (środki minimalizujące negatywne skutki naruszenia w zawiadomieniu do osoby, której dane dotyczą).

2. **Sugestia:** Większość informacji zawartych w części Poradnika "Najczęściej popełniane błędy podczas zawiadamiania osób" została przedstawiona już w pierwszej części rozdziału 13 Poradnika, poprzez wskazanie formy niewystarczającej treści w każdym z obowiązkowych punktów zawiadomienia - powtarzanie tych zapisów powoduje, że dokument jest zbyt obszerny, a tym samym może być mniej czytelny.

## 9. Rejestr naruszeń.

1. **Uwaga:** W treści poradnika nie zostały zawarte szczegółowi informacje i wskazówki co do treści rejestru naruszeń. Warto wskazać przykład prawidłowo prowadzonego rejestru naruszeń.

## 10. Udział IOD

1. **Sugestia:** Określenie dozwolonej roli IOD w zakresie obsługi i zgłaszania naruszeń ochrony danych, w tym określenie stanowiska organu w zakresie kwestii związanych z możliwością wsparcia w przygotowaniu treści zgłoszenia, takich jak wprowadzanie merytorycznych zmian w treści zgłoszenia lub pomoc w przygotowaniu wstępnej wersji zgłoszenia. Dodatkowo warto rozważyć możliwość umocowania IOD do zgłaszania naruszeń do organu nadzorczego.

   **Komentarz:** W opinii ZFODO należy pozwolić IOD na wsparcie Administratora w obsłudze naruszenia, nie ograniczając jego roli jedynie do formy konsultacyjnej. Rekomendowane jest zezwolenie na dokonywanie czynności technicznych oraz redakcyjnych.

## 11. Kontakt z PUODO

1. **Sugestia:** Proponowane jest bieżące informowanie podmiotów dokonujących zgłoszenia o aktualnym statusie postępowania przed PUODO. Informowanie powinno obejmować przewidywane terminy procedowania i zamknięcia zgłoszenia. Możliwe byłoby wdrożenie odpowiedniego systemu rejestracji sprawy, gdzie podmiot zgłaszający mógł na bieżąco być informowany o zmianach w statusie sprawy.