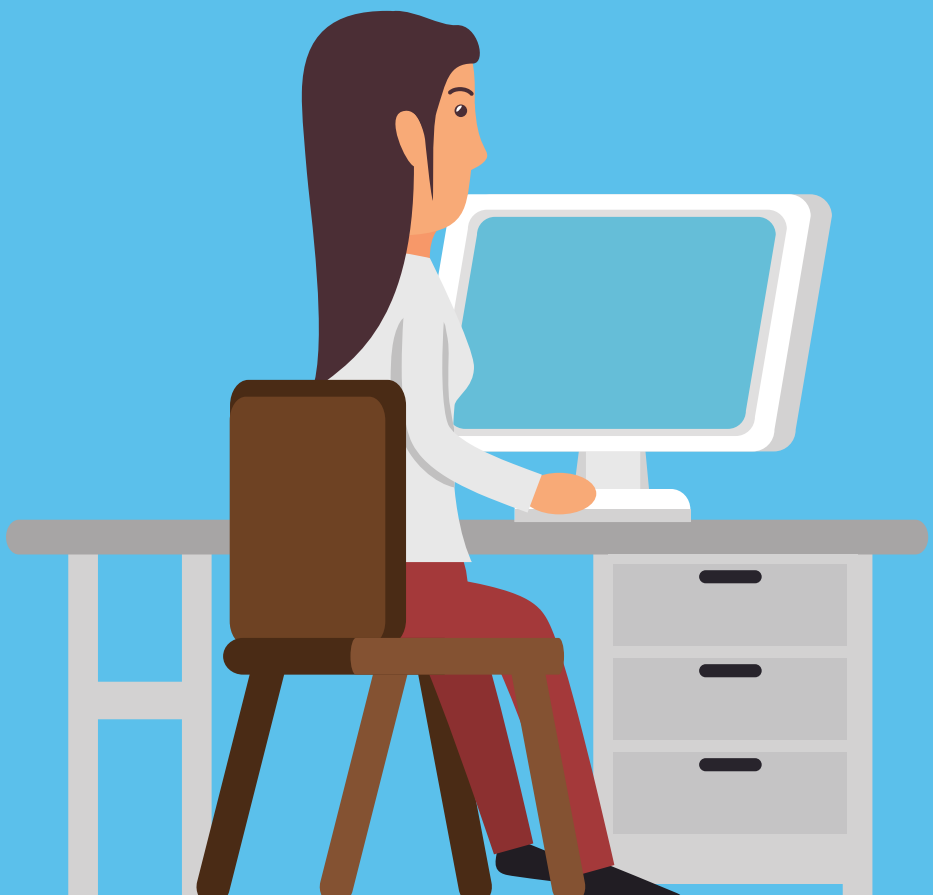
PROCEDURA POSTĘPOWANIA WOBEC

NARUSZENIA OCHRONY DANYCH OSOBOWYCH W PODMIOCIE LECZNICZYM

+ WZORY DOKUMENTÓW



INCYDENT NARUSZENIA OCHRONY DANYCH OSOBOWYCH

- co to takiego?

Czy kiedykolwiek obawiałeś się, że w ramach działalności Twojej organizacji mogło dojść do **naruszenia ochrony danych osobowych**, a nadto nie wiedziałeś, jak w związku z tym postąpić?

Obecnie niemal każdy już wie, czym są dane osobowe oraz jakie środki organizacyjne, techniczne i fizyczne należy wdrożyć, aby te dane chronić.

Dla wielu jednak niewiadomą wciąż pozostaje, czy każde naruszenie zasad ochrony danych osobowych należy kwalifikować jako tzw. „***incydent***" podlegający obowiązkowi zgłoszenia w Urzędzie Ochrony Danych Osobowych.

Te i inne aspekty wyjaśniamy w niniejszym e-booku. W szczególności dowidzą się Państwo:

- **czym jest "incydent naruszenia ochrony danych" - czy każdy trzeba zgłosić?**
- **czy kara jest nieunikniona?**
- **niezgłoszenie naruszenia organowi nadzorczemu - czy to się opłaca?**

Nadto w e-booku znajdziecie Państwo wzory dokumentów wraz z ich omówieniem.

Życzymy przyjemnej lektury.

Edyta Wasilewska
KANCELARIA ADWOKACKA

POSTĘPOWANIE W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

CHECK LISTA

- Zgłoszenie przypadku naruszenia danych osobowych bezpośredniemu przełożonemu,
- Ustalenie okoliczności zdarzenia,
- Zabezpieczenie dowodów,
- Przygotowanie raportu z naruszenia,
- Uzupełnienie wewnętrznego rejestru naruszeń ochrony danych osobowych,
- Ocena ryzyka naruszenia praw lub wolności osób fizycznych,
- Decyzja o zawiadomieniu Prezesa Urzędu Ochrony Danych Osobowych (PUODO),
- Decyzja o poinformowaniu osoby, której dane zostały naruszone,
- Zawiadomienie PUODO,
- Zawiadomienie o naruszeniu osoby, której dane dotyczą.

JAKIE DANE OSOBOWE PRZETWARZANE SĄ W PODMIOCIE LECZNICZYM?

DANE OSOBOWE "ZWYKŁE"

czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (m.in imię i nazwisko, numer telefonu, adres zamieszkania, PESEL, NIP, REGON, KRS, adres e-mail, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej).

DANE DOTYCZĄCE ZDROWIA

dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia.

DANE GENETYCZNE

w zależności od rodzaju podmiotu leczniczego i świadczonych w jego ramach usług, możliwe jest również przetwarzanie danych osobowych dotyczących odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej.

DANE BIOMETRYCZNE

nie często, ale może zdarzyć się, że konieczne będzie przetwarzanie również danych osobowych, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne.

BEZPIECZEŃSTWO DANYCH OSOBOWYCH

Przetwarzanie danych osobowych powinno odbywać się w sposób, który zapewni ich:

- **poufność,**
- **integralność,**
- **dostępność.**

Jednocześnie przepisy prawa nie precyzują, jakie środki techniczne, organizacyjne lub fizyczne należy w tym celu zastosować.

Stosowane zabezpieczenia powinny być jednak proporcjonalne do istniejących w organizacji podatności i zagrożeń. Zabezpieczenia to wszystko, co zmniejsza prawdopodobieństwo wystąpienia zdarzenia naruszającego ochronę danych osobowych. **Oznacza to, że nie zawsze konieczne jest stosowanie najwyższego poziomu zabezpieczeń**, jeśli byłoby to nadmierne w stosunku do charakteru przetwarzania danych osobowych. Wnioski w tym zakresie powinna każdorazowo poprzedzać rzetelna analiza polegająca na identyfikacji realnych podatności, czyli istniejących słabości lub braków albo błędów w stosowanych zabezpieczeniach, które mogą prowadzić do urzeczywistnienia się naruszenia ochrony danych osobowych.

W jaki sposób może zostać naruszona **poufność, integralność** lub **dostęponość** danych osobowych?

Następuje to poprzez przypadkowe lub niezgodne z prawem:

- *zniszczenie,*
- *utracenie,*
- *zmodyfikowanie,*
- *ujawnienie lub dostęp do danych osobowych*

przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Zatem **NARUSZENIE OCHRONY DANYCH OSOBOWYCH** to:

- ***zniszczenie****, np. oryginału dokumentacji medycznej pacjenta;*
- ***utracenie****, np. poprzez usunięcie jedynego egzemplarza elektronicznej dokumentacji medycznej pacjenta i nieposiadanie kopii zapasowej;*
- ***zmodyfikowanie****, np. zmiana danych w dokumentacji medycznej dotyczących zdrowia pacjenta*
- ***ujawnienie lub dostęp do danych osobowych****, np. przesłanie e-maila z dokumentacją medyczną innemu pacjentowi, czy pozostawienie dokumentacji medycznej w miejscu dostępnym dla osób nieupoważnionych.*

CO TO OZNACZA ?

NIE KAŻDY INCYDENT NARUSZENIA BEZPIECZEŃSTWA BĘDZIE JEDNOCZEŚNIE NARUSZENIEM OCHRONY DANYCH OSOBOWYCH

- ***zniszczenie*** *egzemplarza, który nie jest oryginałem dokumentacji medycznej pacjenta, a jedynie jej kopią, nie spowoduje utraty danych, a tym samym naruszenia zasad ich ochrony;*
- *nie ma mowy o zupełnym* ***utraceniu*** *danych poprzez usunięcie dokumentacji medycznej pacjenta w formie elektronicznej, co do której istnieje kopia zapasowa (tzw. backup) albo dodatkowy egzemplarz papierowy (o ile taka forma była dopuszczalna);*
- ***zmodyfikowanie****, np. zmiana danych w dokumentacji medycznej dotyczących zdrowia pacjenta, którą można cofnąć, zanim zostanie utrwalona, również nie będzie naruszeniem ochrony danych osobowych;*
- *nie dojdzie do* ***ujawnienia lub dostępu do danych osobowych****, jeśli załączona do e-maila dokumentacja medyczna przesłana do innego pacjenta będzie zaszyfrowana np. numerem PESEL właściwego pacjenta, a z treści samej wiadomości nie będzie możliwe zidentyfikować, do kogo wiadomość miała być kierowana.*

Jak zatem odróżnić zwykły incydent od zdarzenia naruszającego bezpieczeństwo danych osobowych?

Nie wszystkie incydenty bezpieczeństwa muszą wiązać się z naruszeniem ochrony danych osobowych. Nie każde zatem zdarzenie w postaci przykładowo zniszczenia czy modyfikacji danych spowoduje naruszenie przepisów RODO.

Najpierw musi wystąpić któreś z poniższych zdarzeń:

- *zniszczenie,*
- *utracenie,*
- *zmodyfikowanie,*
- *ujawnienie lub dostęp do danych osobowych*

Nadto zdarzenie to musi prowadzić do naruszenia którejkolwiek z poniższych zasad:

- *poufności*
- *integralności*
- *dostępności danych*

Dopiero wówczas zachodzi:

naruszenie ochrony danych osobowych

Naruszenia można podzielić na następujące kategorie:

1) **naruszenie dotyczące poufności danych** – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego ujawnienia lub nieuprawnionego dostępu do danych osobowych;

2) **naruszenie dotyczące integralności danych** – naruszenie, w rezultacie którego dochodzi do nieuprawnionego lub przypadkowego zmodyfikowania danych osobowych;

3) **naruszenie dotyczące dostępności danych** – naruszenie, w rezultacie którego dochodzi do przypadkowego lub nieuprawnionego dostępu do danych osobowych lub zniszczenia danych osobowych.

Postępowanie w związku z naruszeniem bezpieczeństwa ochrony danych osobowych jest dość osobliwe. Administrator bowiem sam zadecyduje, czy podejmie kroki zmierzające do wszczcia przeciwko niemu postępowania Prezesa Urzędu Ochrony Danych Osobowych poprzez zawiadomienie go o popełnionym naruszeniu.

WAŻNE!

NIE KAŻDE NARUSZENIE PODLEGA OBOWIĄZKOWI ZGŁOSZENIA W URZĘDZIE OCHRONY DANYCH OSOBOWYCH.

Brak obowiązku zgłoszenia naruszenia - kiedy?

Zgodnie z zasadami administrator zgłasza organowi nadzorczemu (Prezesowi Urzędu Ochrony Danych Osobowych) naruszenie ochrony danych osobowych, chyba że jest **mało prawdopodobne,** by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych (art. 33 ust. 1 RODO).

Obowiązkowi zgłoszenia do PUODO nie podlegają zatem takie przypadki naruszenia ochrony danych osobowych, które skutkują **niskim ryzykiem naruszenia praw osób fizycznych** (**lub inaczej – gdy naruszenie najprawdopodobniej nie będzie wiązało się z ryzykiem naruszenia praw i wolności osób fizycznych**). W tym wypadku może to być chociażby prawo do prywatności, czy obowiązek zachowania w tajemnicy informacji dotyczących pacjenta.

W RODO nie ma definicji pojęcia "ryzyko". Nie zostało zatem wyjaśnione również, czym jest małe prawdopodobieństwo wystąpienia określonego ryzyka. **W praktyce przyjmuje się, że obowiązkowi zgłoszenia do PUODO podlegają wszystkie przypadki naruszenia, które skutkują prawdopodobieństwem wystąpienia ryzyka wyższym niż małym (niskim).**

Badanie prawdopodobieństwa wystąpienia skutku w postaci ryzyka naruszenia praw i wolności osoby, której dane dotyczą.

Oceny z jakim typem ryzyka mamy w danym wypadku do czynienia, każdorazowo dokonuje sam administrator. Na tej podstawie administrator następnie podejmuje decyzję o zgłoszeniu danego naruszenia do PUODO. Wskazane jest w tym zakresie posiłkować się konsultacją ze specjalistami, np. inspektorem ochrony danych (o ile taki został w organizacji powołany) lub kancelarią zewnętrzną.

Badanie prawdopodobieństwa wystąpienia skutku w postaci ryzyka naruszenia praw i wolności osoby, której dane dotyczą, powinno być dokonywane na moment ujawnienia (dowiedzenia się o fakcie) naruszenia ochrony danych i powinno uwzględniać wszelkie okoliczności naruszenia znane na ten moment administratorowi. W szczególności ocena taka nie powinna być dokonywana w oparciu o hipotetyczne scenariusze odnoszące się do prawdopodobieństwa wystąpienia takiego skutku naruszenia ochrony danych.

PRZYKŁAD Z PRAKTYKI

W jednym z postępowań wszczętych wobec naszego Klienta, PUODO pisemnie poinformował, że naruszenie poufności danych, takich jak nr PESEL wraz z imieniem i nazwiskiem, powoduje **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych, w szczególności ryzyko uzyskania przez osoby trzecie kredytów w instytucjach pozabankowych.

JAKIE OKOLICZNOŚCI MOGĄ WSKAZYWAĆ, ŻE DOSZŁO DO NARUSZENIA OCHRONY DANYCH?

m.in.:

- nieuprawniony dostęp lub próba dostępu do pomieszczeń, w których następuje proces przetwarzania danych (widoczne uszkodzenia bądź naruszenia zabezpieczeń),
- naruszenie lub próba naruszenia zbioru danych oraz integralności systemu,
- nieautoryzowane zniszczenie lub próba zniszczenia danych zgromadzonych w zbiorach papierowych oraz w systemie,
- zmiana lub utrata danych zapisanych na kopiach zapasowych lub archiwalnych dokonana w sposób nieautoryzowany,
- nieuprawniony dostęp do systemu (sygnał o nielegalnym logowaniu lub inny objaw wskazujący na próbę lub działanie związane z nielegalnym dostępem do systemu),
- inny stan systemu lub pomieszczeń niż pozostawiony przez użytkownika po zakończeniu lub po przerwie w pracy z systemem,
- wysyłka danych do osoby nieuprawnionej,
- kradzież danych/sprzętu,
- wyciek informacji,
- ujawnienie danych osobom nieupoważnionym,
- świadome zniszczenie dokumentów/danych,
- działanie wirusów i innego szkodliwego oprogramowania poprzez samowolne instalowanie niedozwolonego oprogramowania na służbowym sprzęcie.

PESEL to nie dane osobowe?

Z drugiej jednak strony warto podkreślić, że w zeszłym roku pojawiły się orzeczenia przyjmujące, że wyciek PESEL – np. poprzez wysłania maila na nieprawidłowy adres – nie stanowi naruszenia zasad ochrony danych i nie wymaga poinformowania właściciela numeru PESEL o tym fakcie. Tak uznał WSA w Warszawie w wyroku z 19 kwietnia 2022 r., sygn. akt II SA/Wa 3024/21. Orzeczenie to nie jest prawomocne, a sprawą najprawdopodobniej zajmie się Naczelny Sąd Administracyjny. Gdyby jednak NSA podzielił stanowisko warszawskiego WSA pod wieloma względami byłaby do rewolucja w rozumieniu zasad ochrony danych osobowych. Zwłaszcza, że wyciek PESEL to jedno z najczęściej zdarzających się naruszeń RODO – przede wszystkim w działalności biznesowej.

Zgubienie przesyłki z danymi osobowymi trzeba zgłosić

Z praktycznego punktu widzenia bardzo duże znaczenie ma wyrok WSA w Warszawie z 1 lipca 2022 r., sygn. akt II SA/Wa 4143/21. Sprawa rozstrzygnięta tym wyrokiem dotyczyła problemu zagubienia przesyłki nadanej przez bank przez firmę kurierską. Kto w takiej sytuacji powinien podjąć odpowiednie działania, zmierzające do zabezpieczenia danych zawartych w zgubionej przesyłce czy też naprawy skutków dostania się ich w niepowołane ręce?
Wojewódzki Sąd Administracyjny uznał, że w przypadku nieprawidłowości w dostarczaniu przesyłki obowiązek ochrony interesów podmiotu danych z punktu widzenia ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, ciąży na nadawcy przesyłki, który znając zawartość utraconej korespondencji, jest w stanie ocenić zagrożenia wynikające dla osoby, której dane dotyczą. Tym samym to na nadawcy, zdaniem sądu, spoczywa obowiązek poinformowania o zgubieniu przesyłek wszystkich osób, których danie dotyczą. Natomiast firma kurierska jest administratorem danych tylko w tym zakresie, w jakim są one dla niej dostępne. Chodzi tu więc tylko o dane widoczne np. na kopercie

PRZYKŁADOWY REGULAMIN WEWNĘTRZNY POSTĘPOWANIA W PRZYPADKU STWIERDZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek zgłosić przypadek naruszenia danych bezpośredniemu przełożonemu oraz podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony, zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia. Bezpośredni przełożony niezwłocznie informuje o zaistniałej sytuacji Administratora, bądź inną osobę upoważnioną przez Administratora. Do czasu przybycia Administratora, bądź innej osoby upoważnionej przez Administratora, pracownik:

a) zabezpiecza dostęp do miejsca lub urządzenia,

b) wstrzymuje pracę na komputerze, na którym zaistniało naruszenie ochrony oraz nie uruchamia bez koniecznej potrzeby komputerów i innych urządzeń, które w związku z naruszeniem ochrony zostały wstrzymane,

c) podejmuje, stosownie do zaistniałej sytuacji inne, niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych,

d) jest zobowiązany zaniechać wszelkich innych działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia,

e) nie opuszcza bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Administratora, bądź innej osoby upoważnionej przez Administratora.

2. Dokonywanie zmian w miejscu naruszenia ochrony danych, o których mowa w pkt 1, bez uzyskania zgody jest dopuszczalne, jeżeli zachodzi konieczność ratowania osób lub mienia albo zapobieżenia grożącemu niebezpieczeństwu.

3. Zgodę na ponowne uruchomienie komputerów i innych urządzeń oraz kontynuowanie pracy przy pomocy sprzętu IT wyraża Administrator, bądź inna osoba upoważniona przez Administratora.

4. Pracownik jest zobowiązany do informowania Administratora, bądź innej osoba upoważnionej przez Administratora o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

5. Bezpośredni przełożony pracownika, który wykrył lub został poinformowany o nieprawidłowościach przy przetwarzaniu danych osobowych powinien niezwłocznie zidentyfikować problem i przedsięwziąć wszelkie niezbędne kroki, aby uniknąć w przyszłości podobnych zdarzeń.

6. W przypadku stwierdzenia wystąpienia naruszenia/incydentu Administrator, bądź inna osoba upoważniona przez Administratora prowadzi postępowanie wyjaśniające w toku, którego:

a) ustala czas zdarzenia będącego incydentem,

b) ustala zakres i przyczyny naruszenia/incydentu oraz jego ewentualne skutki,

c) zabezpiecza dowody,

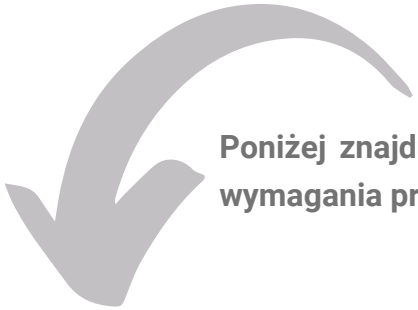
d) ustala osoby odpowiedzialne za naruszenie,

e) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu i niezwłocznie zapewnia przywrócenie prawidłowego stanu działania systemu, a w przypadku uszkodzenia baz danych, odtwarza je z ostatnich kopii awaryjnych z zachowaniem należytych środków ostrożności; sprawdza jakość komunikacji w systemie informatycznym; dokonuje analizy stanu systemu wraz z oszacowaniem rozmiaru szkód powstałych wskutek naruszenia oraz poddaje analizie metody pracy osób upoważnionych do przetwarzania danych osobowych;

f) podejmuje działania zapobiegawcze zmierzające do eliminacji podobnych naruszeń/incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia,
g) podejmuje decyzję o toku dalszego postępowania, stosownie do zakresu naruszenia lub zasadności podejrzenia naruszenia ochrony danych osobowych,
h) proponuje ewentualne działania dyscyplinarne.
6. Administrator, bądź osoba wyznaczona przez Administratora dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport w **Rejestrze naruszeń i incydentów** wg wzoru stanowiącego Załącznik nr 1 do niniejszej Polityki postępowania z incydentami, który następnie niezwłocznie przekazuje Administratorowi, bądź innej osobie upoważnionej przez Administratora. Raport podpisuje również pracownik, który zgłosił naruszenie oraz bezpośredni przełożony pracownika.
7. Jeżeli przyczyną naruszenia były wadliwe metody pracy, błędy i zaniedbania osób zatrudnionych przy przetwarzaniu danych osobowych, jak również w przypadku pojawiających się nieprawidłowości przy przetwarzaniu danych osobowych Administrator przeprowadza dodatkowe szkolenie uzupełniające dotyczące zasad ochrony danych osobowych w strukturze Administratora.
8. Administrator, bądź osoba wyznaczona przez Administratora dokumentuje naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze w **rejestrze naruszeń i incydentów**.

WEWNĘTRZNY REJESTR NARUSZEŃ I INCYDENTÓW - czy trzeba go prowadzić?

Tak, trzeba taki rejestr prowadzić. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na weryfikowanie przestrzegania przepisów dotyczących zasad zgłaszania naruszeń.



Poniżej znajduje się wzór rejestru naruszeń i incydentów spełniający wymagania przepisów RODO:

Wzór rejestru naruszeń i incydentów
spełniający wymagania przepisów RODO:

Opis okoliczności naruszenia/incydentu: _____
Kategoria oraz ilość osób dotknięta naruszeniem/incydentem: _____
Skutki i konsekwencje naruszenia/incydentu: _____
Działania zaradcze: _____
Data rozpoczęcia wdrożenia działań: _____
Data zakończenia wdrażania działań: _____
Osoba odpowiedzialna za wdrożenie działań: _____
Czy naruszenie skutkuje ryzykiem naruszenia praw lub wolności osób fizycznych: _____
Decyzja o niezgłoszeniu naruszenia - należy podać przyczynę, dla której administrator uznaje ryzyko naruszenia praw i wolności osób fizycznych za mało prawdopodobne: _____

Pamiętaj:

administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je PUODO.

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.

ZGŁASZAĆ CZY NIE ZGŁASZAĆ?

Niezgłoszenie naruszenia organowi nadzorczemu - czy to się opłaca?

Jak już była o tym mowa, administrator sam podejmuje decyzję, czy zgłosi organowi nadzorczemu, że w jego organizacji doszło do naruszenia bezpieczeństwa danych osobowych. Niezgłoszenie tego faktu pomimo, iż w danym przypadku taki obowiązek istniał, skutkuje ryzykiem, że PUODO zostanie powiadomiony o tym naruszeniu przez osobę trzecią. Może to wówczas prowadzić do poniesienia przez administratora odpowiedzialności związanej nie tylko z naruszeniem ochrony danych osobowych, ale również z samym niedokonaniem zgłoszenia.

RODO przewiduje odpowiedzialność administracyjną nie tylko za brak zgłoszenia naruszenia, ale nawet za nieprawidłowe zgłoszenie naruszenia, czy również brak wypełniania obowiązków administratora w zakresie prowadzenia wewnętrznej dokumentacji z naruszenia. W takich sytuacjach PUODO ma możliwość nałożenia administracyjnej kary pieniężnej, o której mowa w art. 83 ust. 4 lit. a RODO, w wysokości do **10 000 000 euro,** a w przypadku przedsiębiorstwa – w wysokości do 2% jego całkowitego rocznego światowego obrotu z poprzedniego roku obrotowego.

Tymczasem z naszej praktyki wynika, że PUODO, w zależności od rodzaju i okoliczności dotyczących naruszenia, bardzo często poprzestaje na tzw. **wystąpieniu, jeżli naruszenie było niewielkiej skali,** w którym jedynie wzywa administratora do wdrożenia odpowiednich procedur oraz podjęcia określonych działań naprawczych i na tym kończy podjętą procedurę.

Edyta Wasilewska
KANCELARIA ADWOKACKA

Mamy nadzieję, że niniejsze opracowanie spełniło Państwa oczekiwania.

W razie jakichkolwiek pytań, zapraszamy do kontaktu!

Z wyrazami szacunku,

dr Edyta Wasilewska
Adwokat

Kancelaria Adwokacka dr Edyta Wasilewska

ul. Grzybowska 87, 00-844 Warszawa

tel. +48 534 974 902

e.wasilewska@kancelaria-wasilewska.pl

www.kancelaria-wasilewska.pl

NIP: 7393654333
REGON: 360635403