KANCELARIA DORADCZA PARTNER SYSTEM

Właściciel kancelarii

Biegły sądowy z zakresu

ochrony informacji niejawnych i danych osobowych

przy Sądzie Okręgowym w Bydgoszczy

mgr inż. Arnold PASZTA

www.partnersystem.info

ZASADY OCHRONY DANYCH OSOBOWYCH I BEZPIECZEŃSTWA INFORMACJI

- Przestrzeganie zasad ochrony danych osobowych i reguł związanych z bezpieczeństwem informacji jest obowiązkiem każdego pracownika, który ma lub mógłby mieć do czynienie z danymi osobowymi.

- Złamanie zasad może być uznane na naruszenie obowiązków pracowniczych lub zobowiązań zawartych w umowach.

DEFINICJE

Dane osobowe stanowią wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania żyjącej osoby fizycznej. Poszczególne informacje, które w połączeniu ze sobą mogą prowadzić do zidentyfikowania tożsamości danej osoby, także stanowią dane osobowe.

DEFINICJE

Dane osobowe zwykłe (choć takiego określenia nie znajdziemy w RODO) to w zasadzie te dane, które nie zaliczają się do zamkniętego katalogu danych szczególnej kategorii, a co za tym idzie nie podlegają szczególnej ochronie. Do danych zwykłych można zaliczyć m.in. numer PESEL, imię i nazwisko czy adres zamieszkania.

DEFINICJE

W artykule 9 RODO możemy znaleźć numeratywnie wymienione szczególne kategorie danych. Są to:

- dane osobowe ujawniające pochodzenie rasowe lub etniczne,
- dane osobowe ujawniające poglądy polityczne,
- dane osobowe ujawniające przekonania religijne lub światopoglądowe,
- dane osobowe ujawniające przynależność do związków zawodowych,
- dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej,
- dane dotyczących zdrowia, seksualności lub orientacji seksualnej.

DEFINICJE

Przetwarzanie danych osobowych – operacja, lub zestaw operacji wykonywanych na danych osobowych w sposób:

- zautomatyzowany – systemy informatyczne;
- niezautomatyzowany – forma papierowa.

DEFINICJE

Przepisy o ochronie danych osobowych **nie dotyczą** czynności wykonywanych wyłącznie na użytek osobisty lub domowy, takich jak m.in.:

- porządkowanie informacji o kontaktach w prywatnym telefonie komórkowym, który nie jest wykorzystywany do celów służbowych czy prowadzonej działalności gospodarczej;
- rozpowszechnianie w sieci prywatnych informacji na swój temat;
- usuwanie ze swojego komputera plików zawierających informacje o prywatnych wynikach badań lekarskich.

OPERACJE PRZETWARZANIA
-przykłady

- zbieranie danych
- przeglądanie danych
- organizowanie danych
- niszczenie danych
- ujawnienie danych
- modyfikowanie danych

DEFINICJE

ADMINISTRATOR DANYCH - oznacza organ, jednostkę organizacyjną, podmiot lub osobę decydującą o celach i środkach przetwarzania danych osobowych.

PRZYKŁADY :

- stowarzyszenie;
- biblioteka;
- przedszkole;
- spółka z ograniczoną odpowiedzialnością;
- adwokat prowadzący własną kancelarię.

DEFINICJE

PODMIOT PRZETWARZAJĄCY (PROCESOR) - oznacza organ publiczny, osobę fizyczną lub prawną, lub każdy inny podmiot, którzy przetwarza dane osobowe w imieniu i na rzecz administratora. PRZYKŁADY :

- firmy obsługujące księgowość/kadry;
- firmy niszczące dokumenty;
- usługi zewnętrznego archiwum;
- zewnętrzne IT.

DEFINICJE

INSPEKTOR OCHORNY DANYCH (IOD)- Inspektor Ochrony Danych (IOD) to osoba dysponującą wiedzą fachową na temat prawa i praktyk w dziedzinie ochrony danych powoływana przez administratora danych osobowych lub podmiot przetwarzający w celu wspomagania wewnętrznego przestrzegania przepisów RODO.

DEFINICJE

INSPEKTOR OCHORNY DANYCH (IOD)

ZADANIA :

- monitorowanie wdrożonych systemów ochrony danych;
- informowanie pracowników o ich obowiązkach związanych z RODO;
- audyty systemu ochrony danych osobowych;
- szkolenie pracowników w zakresie ochrony danych.

DEFINICJE

IOD nie mogą jednak wykonywać zadań, za które odpowiadają wyłącznie administratorzy lub podmioty przetwarzające. W praktyce oznacza to, że IOD – z uwagi na potrzebę unikania konfliktu interesów i zapewnienia niezależności (patrz poniżej) – **nie powinni:**

- **zgłaszać** naruszeń ochrony danych osobowych Prezesowi UODO w imieniu administratorów ani podpisywać i wysyłać takich zgłoszeń;
- **zawiadamiać w imieniu administratorów osób,** których dane dotyczą, o naruszeniach ochrony danych osobowych;
- **dokumentować naruszeń** ochrony danych osobowych w imieniu administratorów (w szczególności jeśli wiązałoby się to z ustalaniem celów i sposobów przetwarzania danych osobowych albo określaniem działań zaradczych);
- **podejmować zobowiązań** dotyczących bezpieczeństwa przetwarzania w imieniu administratorów lub podmiotów przetwarzających;
- **działać na podstawie pełnomocnictwa** w sprawach dotyczących ochrony danych osobowych.

DEFINICJE

ORGAN NADZORCZY (PREZES URZĘDU OCHRONY DANYCH OSOBOWYCH – PREZES UODO)- niezależny organ publiczny odpowiedzialny za monitorowanie stosowania przepisów i ochronie danych osobowych.

ZASADY PRZETWARZANIA DANYCH

ZASADA LEGALNOŚCI ORAZ PRZEJRZYSTOŚCI – przetwarzanie danych musi odbywać się zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą. Musi istnieć podstawa prawna przetwarzania:

- zgoda osoby, której dane dotyczą;
- niezbędność przetwarzania danych do wykonywania umowy (np. podanie danych przy zatrudnianiu).

ZASADY PRZETWARZANIA DANYCH

ZASADA CELOWOŚCI – cel przetwarzania musi być z góry określony i przedstawiony osobie, której dane dotyczą. Przy przetwarzaniu musi istnieć konkretny, wyraźny i prawnie uzasadniony cel. Przetwarzanie danych niezgodne z celem jest zakazane.

ZASADY PRZETWARZANIA DANYCH

ZASADA INTEGRALNOŚCI I POUFNOŚCI DANYCH – postępowanie z danymi osobowymi powinno zapewniać odpowiedni poziom bezpieczeństwa, w tym ochronę przed niedozwolonym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych podjętych po analizie i uwzględnieniu ryzyka.

ZASADY PRZETWARZANIA DANYCH

ZASADA ADEKWATNOŚCI (MINIMALIZACJI DANYCH) – administrator powinien przetwarzać dane, które są niezbędne ze względu na cel ich zbierania.

ZASADA MERYTORYCZNEJ POPRAWNOŚCI – dane osobowe muszą być:

- prawdziwe,
- kompletne,
- aktualne ze względu na cel.

ZASADY PRZETWARZANIA DANYCH

ZASADA OGRANICZENIA PRZECHOWYWANIA – dane osobowe mogą byś przechowywane w formie umożliwiającej identyfikację osoby przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te zostały pozyskane (jeśli celem zbierania CV było zatrudnienie na konkretne stanowisko, nie można przechowywać CV na potrzeby przyszłych rekrutacji bez dodatkowej zgody).

ZASADY PRZETWARZANIA DANYCH

ZASADA ROZLICZALNOŚCI – administrator musi być w stanie wykazać, że jego działania są dostosowane do wymogów prawnych, np. w razie kontroli wykazać, że realizuje obowiązek informacyjny lub stosuje odpowiednie środki techniczne i organizacyjne zabezpieczające przed nieuprawnionym dostępem przez osoby trzecie.

ZASADY BEZPIECZEŃSTWA DANYCH

ZASADA CZYSTEGO BIURKA – należy przechowywać wszelkie dokumenty i nośniki danych poza zasięgiem osób postronnych, schowane i zamknięte na klucz.

ZASADA POUFNEGO DRUKU – należy odbierać dokumenty niezwłocznie po ich wydrukowaniu.

ZASADY BEZPIECZEŃSTWA DANYCH

ZASADA CZYSTEGO EKRANU – należy pamiętać o blokowaniu komputerów przed każdorazowym, nawet chwilowym opuszczeniem stanowiska pracy. Należy również uniemożliwić osobom trzecim nieupoważniony wgląd w treści wyświetlane na monitorach – odpowiednio ustawiać ekran lub stosować filtry prywatyzujące.

PROCEDURY BEZPIECZEŃSTWA DANYCH

POLITYKA OCHRONY DANYCH – dokument opisujący kluczowe kwestie wiążące się z ochroną danych osobowych. Znajdują się tam wszystkie najważniejsze informacje jak poprawnie chronić dane.

PROCEDURY BEZPIECZEŃSTWA DANYCH

PROCEDURA ZGŁASZANIA NARUSZEŃ – pracownik ma obowiązek zgłaszania wszelkiego rodzaju naruszeń ochrony danych. Pracownik musi zareagować niezwłocznie po wykryciu zagrożenia lub naruszenia danych osobowych.

Zgłoszenie naruszenia powinno nastąpić do 72h od powzięcia informacji o zdarzeniu

NARUSZENIA

Wszędzie tam, gdzie przetwarzane są dane osobowe, może dojść do naruszenia ochrony danych osobowych.

Jest nim zakłócenie bezpieczeństwa przetwarzanych danych osobowych, które może wpłynąć na ich poufność, integralność lub dostępność.

Dochodzi do niego bez względu na to, czy wystąpi:

- przez przypadek (np. w wyniku błędu, zaniedbania lub nieprzewidzianej awarii technicznej);
- na skutek celowego, bezprawnego działania (np. oszustwa, kradzieży lub włamania).

NARUSZENIA

Naruszenie ochrony danych osobowych pojawia się więc zawsze, gdy dochodzi do zdarzenia, które:

- jest incydentem bezpieczeństwa;
- dotyczy przetwarzanych danych osobowych;
- może doprowadzić do ich nieuprawnionego zniszczenia, utracenia, zmodyfikowania, ujawnienia lub dostępu do nich.

Tym samym naruszeniem ochrony danych osobowych nie jest zdarzenie, które **nie spełnia** któregoś z tych warunków.

NARUSZENIA

Art. 4 pkt 12 RODO Definicje

- *„naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;*

NARUSZENIA

Naruszeniem ochrony danych osobowych może być m.in.:

- strawienie przez pożar jedynego egzemplarza dokumentów kadrowych (**zniszczenie**);
- zagubienie pendrive'a będącego jedynym nośnikiem bazy informacji o klientach (**utracenie**);
- przekształcenie w ramach żartu nazwisk studentów w systemie informatycznym uczelni (**zmodyfikowanie**);
- wysłanie do niewłaściwego odbiorcy przesyłki pocztowej zawierającej niezabezpieczoną przed dostępem umowę o świadczenie usług (**ujawnienie**);
- przejęcie internetowego konta bankowego przez oszusta (**dostęp**).

NARUSZENIA

Naruszeniem ochrony danych osobowych **nie będzie** m.in.:

- chwilowy brak dostępu do danych osobowych związany z zaplanowaną aktualizacją systemu informatycznego (zdarzenie **nie jest** incydentem bezpieczeństwa);
- zagubienie dokumentacji niezawierającej danych osobowych, np. dokumentów zawierających dane finansowe, których nie można powiązać z osobą fizyczną (zdarzenie **nie dotyczy** danych osobowych);
- omyłkowe wysłanie e-maila zawierającego dane osobowe do niewłaściwego – ale uprawnionego – odbiorcy wewnątrz organizacji (zdarzenie **nie prowadzi** do nieuprawnionego ujawnienia danych osobowych).

NARUSZENIA

Uwaga!

Jeżeli osoba, której dane dotyczą, jest zidentyfikowana lub możliwa do zidentyfikowania, pozostałe informacje o niej **nie muszą być prawdziwe**, aby mogło dojść do naruszenia ochrony danych osobowych. Przetwarzanie (np. wykorzystywanie, przekazywanie lub rozpowszechnianie) fałszywych danych osobowych również może prowadzić do naruszenia praw lub wolności osób, których dane te dotyczą.

NARUSZENIA

Czasami trudno dokładnie określić, do jakich konsekwencji doprowadzi incydent bezpieczeństwa. W niektórych przypadkach ostatecznego wpływu zdarzenia na przetwarzane dane, a w konsekwencji na osoby, których dane dotyczą, nie da się przewidzieć nie tylko na początku, ale nawet przez cały czas jego trwania

NARUSZENIA

Przykład:

Zainfekowanie systemu informatycznego firmy złośliwym oprogramowaniem ransomware może doprowadzić do zablokowania dostępu do zgromadzonych w nim zasobów (**utracenie**).

W wyniku zdarzenia hakerzy mogą uzyskać także wgląd do danych osobowych pracowników i klientów (**dostęp**), a nawet skopiować je i sprzedać lub publicznie udostępnić w sieci (**ujawnienie**).

Jeżeli firma nie posiada kopii zapasowej bazy danych, z czasem może odzyskać dostęp jedynie do części informacji w pierwotnej lub zmienionej formie (**zmodyfikowanie**), a nawet utracić je na zawsze (**zniszczenie**).

NARUSZENIA

Do naruszenia ochrony danych osobowych dochodzi niezależnie od tego, czy niepożądane konsekwencje dla osób fizycznych **rzeczywiście** wystąpią. Ocena dotycząca tego, czy taka sytuacja może się wydarzyć i jak może być dotkliwa dla jednej lub więcej osób, stanowi jeden z kluczowych obowiązków administratorów związanych z naruszeniami ochrony danych osobowych

BEZPIECZEŃSTWO DANYCH

Przetwarzanie musi być bezpieczne12, a naruszenia ochrony danych osobowych mogą zakłócać bezpieczeństwo przetwarzania w różny sposób.

NARUSZENIA POUFNOŚCI DANYCH OSOBOWYCH

Poufność danych osobowych oznacza, że mogą się z nimi zapoznać wyłącznie osoby do tego uprawnione, czyli takie, które posiadają odpowiednie upoważnienie lub podstawę prawną do podejmowania określonych działań z użyciem danych osobowych.

NARUSZENIA POUFNOŚCI DANYCH OSOBOWYCH

Naruszenie poufności danych osobowych występuje w przypadku:

- nieuprawnionego ujawnienia danych osobowych, gdy ten, kto przetwarza dane osobowe, umożliwi zapoznanie się z nimi osobom nieuprawnionym.
- nieuprawnionego uzyskania dostępu do danych osobowych: gdy osoba nieuprawniona samodzielnie (np. bez upoważnienia) uzyska możliwość ich przetwarzania.

NARUSZENIA POUFNOŚCI DANYCH OSOBOWYCH

Naruszeniem **poufności** danych osobowych może być m.in.:

- ustne przekazanie osobom nieuprawnionym informacji będących danymi osobowymi, powziętych w związku z wykonywanym zawodem lub sprawowaną funkcją;
- omyłkowe wysłanie e-maila zawierającego dane osobowe do niewłaściwego (i nieuprawnionego) odbiorcy (chyba że administrator ma dowód niedostarczenia wiadomości);
- sprzedaż starych telefonów, komputerów lub innych nośników bez uprzedniego trwałego usunięcia danych osobowych zapisanych w ich pamięciach;

NARUSZENIA INTEGRALNOŚCI DANYCH OSOBOWYCH

Naruszenie **integralności** danych osobowych występuje w przypadku nieuprawnionego zmodyfikowania danych osobowych.

Może do niego dojść w przypadku:

- dokonania jakiejkolwiek zmiany przez osobę nieuprawnioną;
- dokonania nieprawidłowej (np. przypadkowej, błędnej, niedokładnej, niekompletnej, nieaktualnej) zmiany przez osobę uprawnioną (lub niedokonania przez nią odpowiedniej zmiany).

NARUSZENIA INTEGRALNOŚCI DANYCH OSOBOWYCH

Naruszeniem **integralności** danych osobowych może być m.in.:

- niewprowadzenie do bazy danych zmian informacji, które powinny być zaktualizowane;
- działanie złośliwego oprogramowania dokonującego zmiany w plikach zawierających dane osobowe;
- włamanie się osoby nieuprawnionej do systemu kadrowego i podmienienie numerów rachunków bankowych pracowników na inne;
- odtworzenie z kopii zapasowej danych osobowych i brak ich aktualizacji.

NARUSZENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH

Dostępność danych osobowych oznacza, że mogą być one bez przeszkód przetwarzane zgodnie z ich przeznaczeniem przez osoby do tego uprawnione.

Naruszenie dostępności danych osobowych występuje w przypadku:

- **nieuprawnionego utracenia danych** osobowych dotyczy sytuacji, w której czasowo lub trwale nie da się z nich skorzystać, choć istnieje możliwość ich odzyskania lub odtworzenia.
- **nieuprawnionego zniszczenia danych osobowych** gdy przepadają one nieodwracalnie, ponieważ administrator nie ma możliwości ich ponownego odtworzenia (np. z kopii zapasowej).

NARUSZENIA DOSTĘPNOŚCI DANYCH OSOBOWYCH

Naruszeniem **dostępności** danych osobowych może być m.in.:

- trwała lub czasowa utrata dostępu do danych osobowych z powodu awarii systemu informatycznego lub cyberataku;
- zagubienie papierowej dokumentacji lub elektronicznego nośnika (np. pendrive'a, dysku SSD, płyty CD) zawierającego dane osobowe (jedynego egzemplarza);
- utrata dostępu do danych osobowych na skutek zablokowania lub usunięcia konta użytkownika.

NARUSZENIA

Naruszenia ochrony danych osobowych mogą pojawiać się w każdej organizacji, bez względu na jej wielkość, zakres przetwarzanych danych osobowych czy środki przeznaczone na ich ochronę.

Przyczynami powstawania naruszeń ochrony danych osobowych mogą być:

- zdarzenia przypadkowe;
- celowe, bezprawne działania.

NARUSZENIA

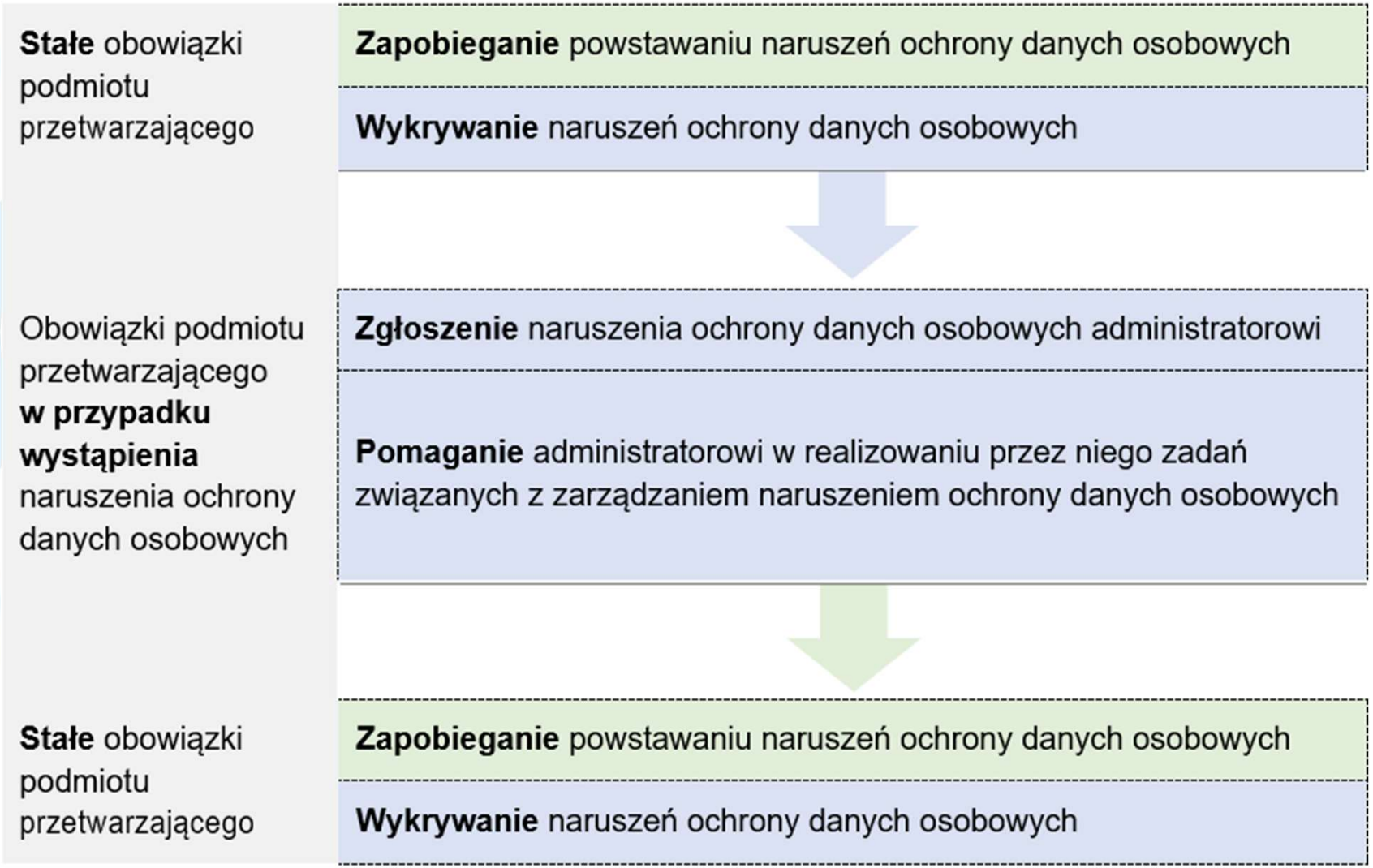
RODO **nie przewiduje** obowiązku zapobiegania **wszelkim możliwym** naruszeniom ochrony danych osobowych. Jeżeli takie zdarzenie wystąpiło **pomimo** prawidłowego realizowania obowiązków przez podmioty zobowiązane do zapewnienia bezpieczeństwa przetwarzania, nie muszą się one obawiać zastosowania wobec nich sankcji administracyjnych.

NARUSZENIA – OBOWIĄZKI ADMINITRATORA

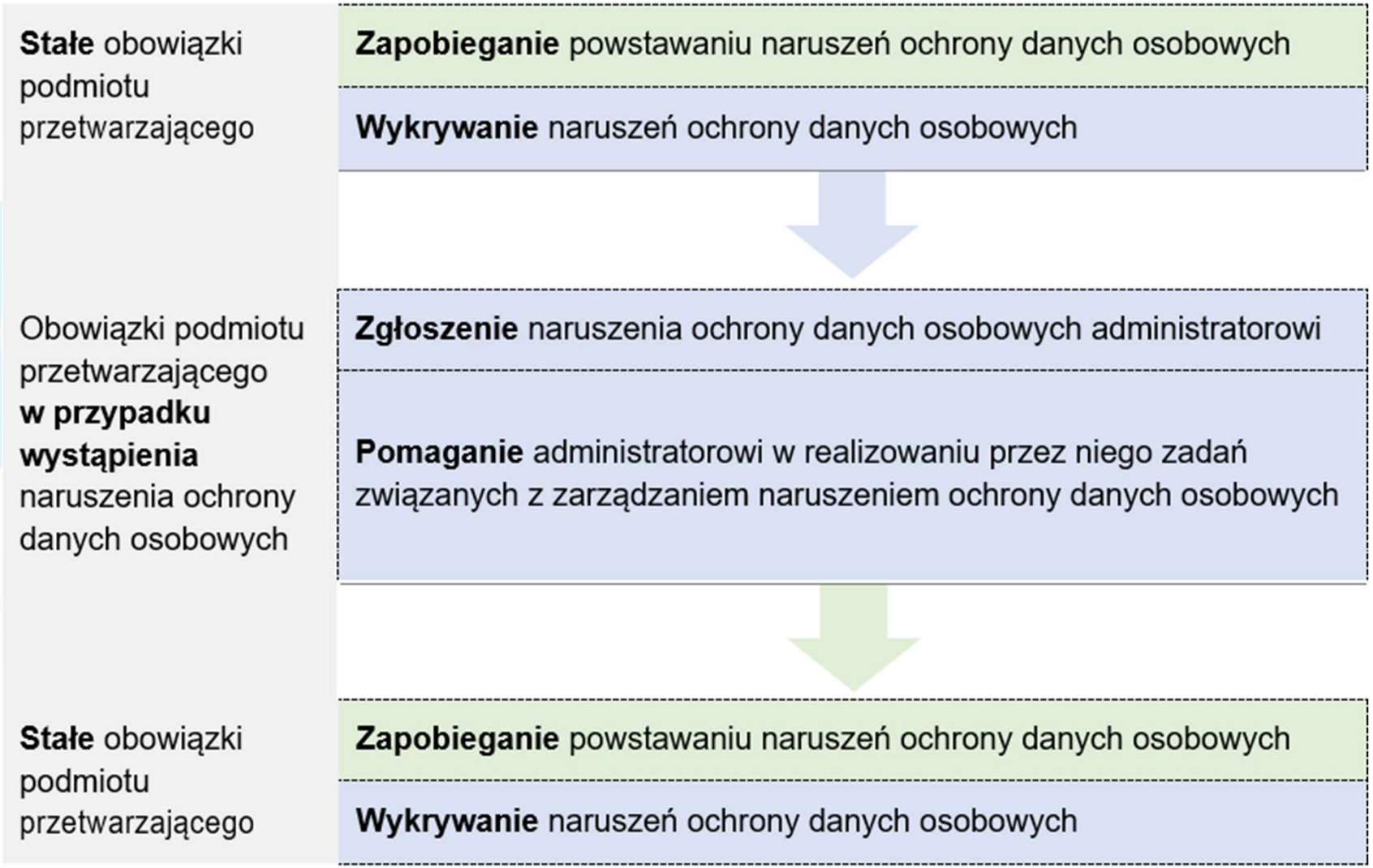
<table>
<tr><td rowspan="2">**Stałe** obowiązki administratora</td><td colspan="2">**Zapobieganie** powstawaniu naruszeń ochrony danych osobowych</td></tr>
<tr><td colspan="2">**Wykrywanie** i „stwierdzanie” naruszeń ochrony danych osobowych</td></tr>
<tr><td rowspan="4">Obowiązki administratora **w przypadku wystąpienia** naruszenia ochrony danych osobowych</td><td colspan="2">**Zaradzenie** naruszeniu ochrony danych osobowych i jego ewentualnym negatywnym skutkom</td></tr>
<tr><td colspan="2">**Ocenienie ryzyka** naruszenia praw lub wolności osób fizycznych w związku z naruszeniem ochrony danych osobowych</td></tr>
<tr><td>**Ryzyko**</td><td>**Wysokie ryzyko**</td></tr>
<tr><td>**Zgłoszenie** naruszenia ochrony danych osobowych Prezesowi UODO</td><td>**Zgłoszenie** naruszenia ochrony danych osobowych Prezesowi UODO

Zawiadomienie osób, których dane dotyczą, o naruszeniu ochrony ich danych osobowych</td></tr>
<tr><td></td><td colspan="2">**Dokumentowanie** naruszenia ochrony danych osobowych</td></tr>
<tr><td rowspan="2">**Stałe** obowiązki administratora</td><td colspan="2">**Zapobieganie** powstawaniu naruszeń ochrony danych osobowych</td></tr>
<tr><td colspan="2">**Wykrywanie** i „stwierdzanie” naruszeń ochrony danych osobowych</td></tr>
</table>

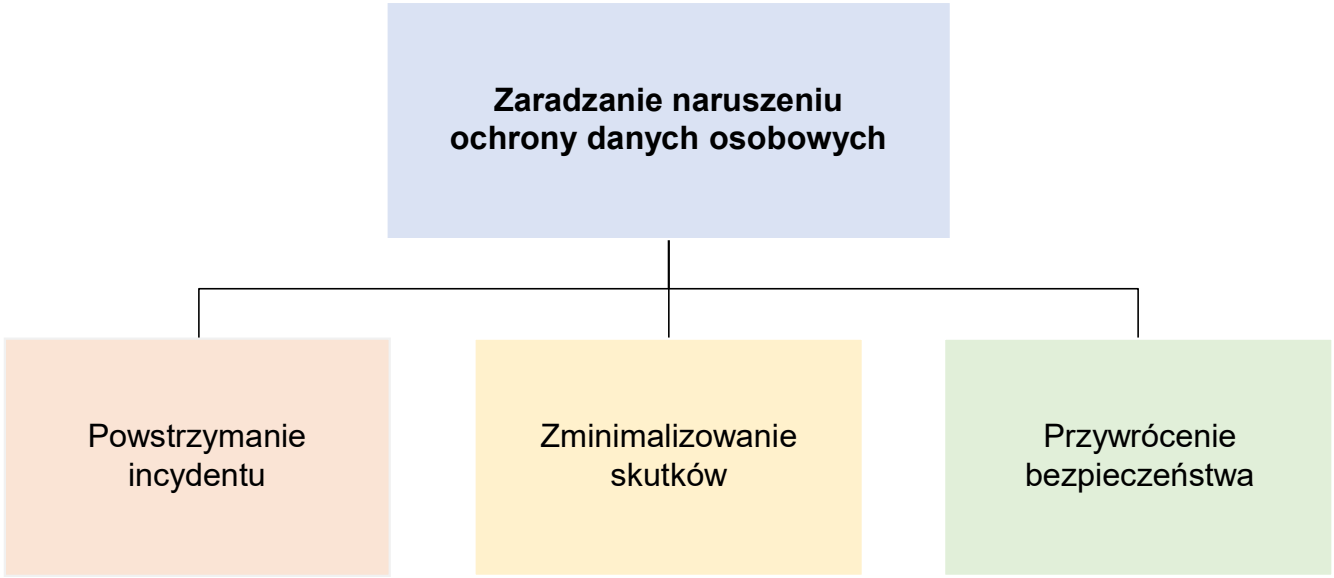
NARUSZENIE - OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO



NARUSZENIE - OBOWIĄZKI PODMIOTU PRZETWARZAJĄCEGO



ZARZĄDZANIE NARUSZENIEM



ZAPOBIEGANIE ZAGROŻENIOM

Administratorzy i podmioty przetwarzające są zobowiązani do zapewnienia bezpieczeństwa przetwarzania danych osobowych poprzez wdrożenie odpowiednich środków **technicznych i organizacyjnych**.

Właściwy dobór tych środków ma kluczowe znaczenie dla skutecznej ochrony danych i powinien uwzględniać stan wiedzy technicznej, koszt wdrażania, a także charakter, zakres, kontekst i cele przetwarzania oraz związane z nim ryzyko.

Ponieważ okoliczności te zmieniają się w czasie, organizacje powinny regularnie oceniać i doskonalić stosowane rozwiązania.

ZAPOBIEGANIE ZAGROŻENIOM

Środkami **organizacyjnymi** służącymi zapobieganiu naruszeniom ochrony danych osobowych są m.in.

- wdrożenie **procedur dotyczących ochrony danych osobowych** oraz ich bezpiecznego przetwarzania;
- wdrożenie **procedur reagowania na incydenty bezpieczeństwa**, w tym planów odzyskiwania danych osobowych i przywracania ich ochrony w sytuacjach nadzwyczajnych;
- przyjęcie **zasad bezpiecznego korzystania z haseł**, w tym szczegółowych wymagań dotyczących ich tworzenia, przechowywania i regularnej weryfikacji ich bezpieczeństwa;
- przeprowadzanie regularnych audytów bezpieczeństwa informatycznego i testów penetracyjnych, aby identyfikować luki w systemach, wskazywać obszary wymagające poprawy oraz podnosić świadomość użytkowników na temat zagrożeń.

ZAPOBIEGANIE ZAGROŻENIOM

Środkami **technicznymi** służącymi zapobieganiu naruszeniom ochrony danych osobowych są m.in.:

Uwierzytelnianie

- korzystanie z **bezpiecznych danych logowania;**
- wdrażanie **uwierzytelniania wieloskładnikowego**, szczególnie w przypadku dostępu do wrażliwych informacji, systemów zdalnych lub uprawnień użytkowników o podwyższonym ryzyku;
- regularne **weryfikowanie ważności danych uwierzytelniających** i ich cykliczna aktualizacja w celu zapobiegania przejęciu kont.

Infrastruktura i systemy

- regularne **aktualizowanie systemów operacyjnych, aplikacji oraz urządzeń sieciowych**, w tym przeglądarek i wtyczek;
- **izolacja procesów przetwarzania danych** oraz **segmentowanie systemów i sieci informatycznych** w celu minimalizowania ryzyka rozprzestrzeniania się zagrożeń;
- zwiększanie bezpieczeństwa serwerów i stacji roboczych, w tym blokowanie dostępu do stron stanowiących potencjalne źródło zagrożeń; blokowanie złośliwego oprogramowania i podejrzanych aplikacji; monitorowanie użytkowania oprogramowania oraz prowadzenie dzienników zdarzeń (logów).

ZAPOBIEGANIE ZAGROŻENIOM

Środkami **technicznymi** służącymi zapobieganiu naruszeniom ochrony danych osobowych są m.in.:

Poczta elektroniczna

- wyraźne określenie **polityk i procedur dotyczących wysyłania wiadomości e-mail** z danymi osobowymi, w tym: korzystanie z pola „**UDW**”; szyfrowanie e-maili i załączników za pomocą unikalnych haseł dostępnych jedynie dla odbiorcy

Ochrona przed złośliwym oprogramowaniem

- stosowanie **rozwiązań antywirusowych i antyransomware**, które umożliwiają skanowanie i wykrywanie zagrożeń w czasie rzeczywistym;
- tworzenie bezpiecznych **systemów kopii zapasowych**;

Wykorzystywanie urządzeń zewnętrznych

- przechowywanie danych w systemach wewnętrznych z zabezpieczeniem zdalnego dostępu poprzez **VPN**;
- **szyfrowanie danych** na urządzeniach zewnętrznych oraz stosowanie funkcji „zdalne czyszczenie” w razie utraty sprzętu;
- **blokowanie kont użytkowników** po kilku nieudanych próbach logowania;

OCENA RYZYKA

Aby prawidłowo ocenić ryzyko, administratorzy powinni oszacować wagę potencjalnych konsekwencji oraz prawdopodobieństwo ich wystąpienia; uwzględniając następujące okoliczności zdarzenia:

- rodzaj naruszenia ochrony danych osobowych;
- charakter, wrażliwość i zakres danych osobowych;
- łatwość identyfikacji osób, których dane dotyczą;
- dotkliwość konsekwencji dla osób, których dane dotyczą;
- cechy szczególne osób, których dane dotyczą;
- cechy szczególne administratora;
- liczbę osób, których dane dotyczą.

OCENA RYZYKA

Administratorzy muszą ustalić, czy naruszenie ochrony danych osobowych może wiązać się z:

- brakiem ryzyka;
- ryzykiem, co wymaga zgłoszenia go Prezesowi UODO;
- lub wysokim ryzykiem, co oznacza obowiązek zgłoszenia go Prezesowi UODO oraz zawiadomienia osób, których dane dotyczą

OCENA RYZYKA

Brak ryzyka

Choć co do zasady naruszenia ochrony danych osobowych stwarzają pewne ryzyko naruszenia praw lub wolności osób fizycznych, zdarzają się sytuacje, w których można jednoznacznie stwierdzić, że takie ryzyko prawdopodobnie nie wystąpi.

Są to przede wszystkim przypadki dotyczące:

- ujawnienia danych, które są już publicznie dostępne;
- ujawnienia lub utracenia danych zaszyfrowanych w sposób zapewniający ich nieczytelność dla osób nieupoważnionych (jeżeli są one zabezpieczone kluczem, który nie został naruszony, a administrator ma dostęp do ich kopii zapasowej);
- incydentów, którym administratorzy definitywnie **zaradzili**

OCENA RYZYKA

Brak ryzyka - Przykład

Pracownik firmy budowlanej wyrzucił dokumenty kadrowe i finansowe (zawierające m.in. imiona, nazwiska, numery PESEL i informacje o wynagrodzeniach) do kontenera na odpady znajdującego się na zamkniętym, monitorowanym terenie firmy. Po upływie około godziny pracownik zdał sobie sprawę z błędu, a administrator podjął natychmiastowe działania, odzyskując i zabezpieczając dokumenty. Mimo że początkowo zdarzenie mogło doprowadzić do poważnych konsekwencji, nagrania potwierdziły brak dostępu osób nieuprawnionych oraz skuteczne zaradzenie incydentowi. W takim przypadku można było jednoznacznie stwierdzić brak ryzyka naruszenia praw lub wolności osób, których dane dotyczą.

OCENA RYZYKA

Wysokie ryzyko

Administratorzy mogą stwierdzić, że z naruszeniem ochrony danych osobowych wiąże się wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Oznacza to, że potencjalne konsekwencje incydentu mogą mieć:

- znaczną wagę;
- i/lub duże prawdopodobieństwo wystąpienia.

OCENA RYZYKA

Wysokie ryzyko

O wysokim ryzyku mogą świadczyć określone okoliczności zdarzenia, w tym m.in.:

- objęcie incydentem wrażliwych danych osobowych (szczególne tj: o pochodzeniu, poglądach polityczne, religijnych lub światopoglądowe, genetycznych, orientacji seksualnej, wyroków skazujących, czynów zabronionych), a także informacje powszechnie wykorzystywane do potwierdzania tożsamości lub zawierania umów, takie jak seria i numer dowodu osobistego oraz numer PESEL;
- szeroki zakres danych osobowych objętych incydentem (im szerszy, tym wyższe ryzyko);

OCENA RYZYKA

Wysokie ryzyko

O wysokim ryzyku mogą świadczyć określone okoliczności zdarzenia, w tym m.in.:

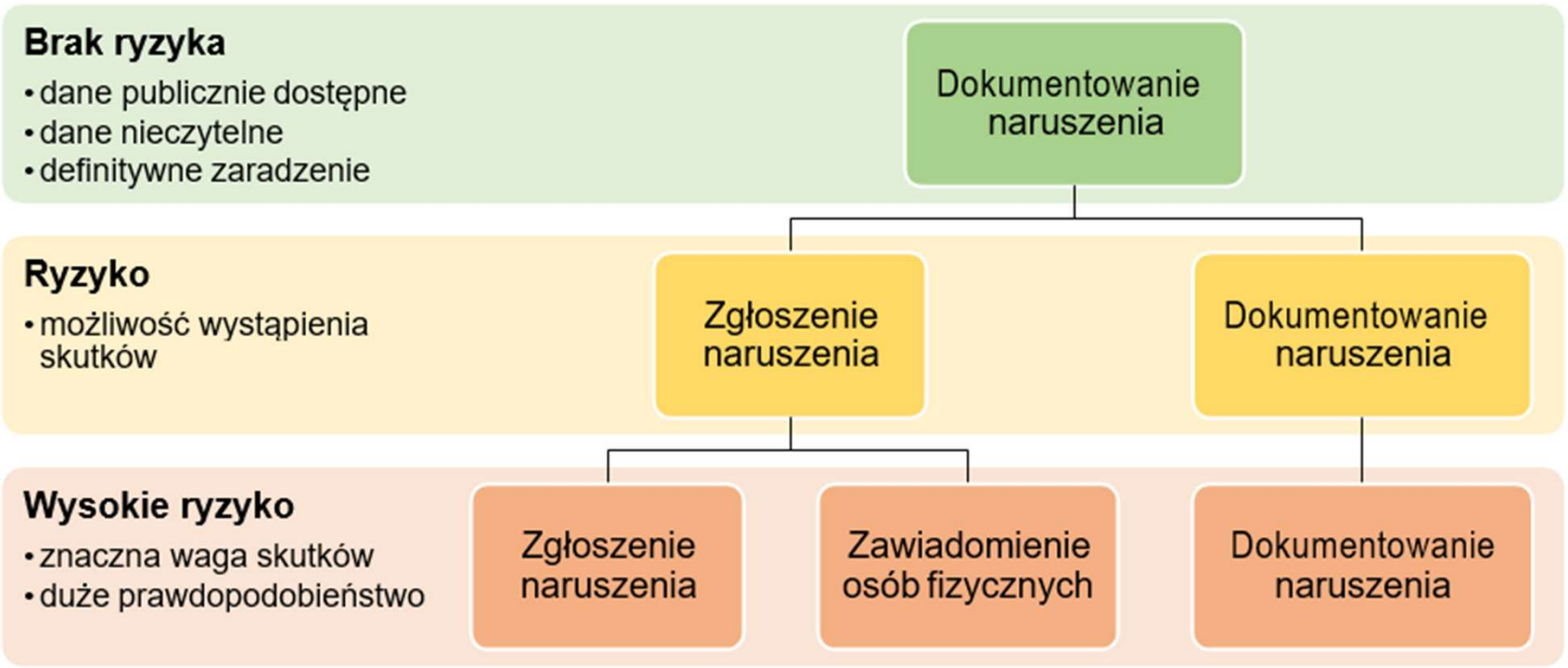
- szczególna dotkliwość możliwych skutków incydentu (takich jak kradzież tożsamości, oszustwa finansowe, straty finansowe, problemy zawodowe,
- uszczerbek na zdrowiu, silny stres, lęk i obniżone poczucie bezpieczeństwa);
- szczególny charakter osób objętych incydentem (takich jak dzieci, osoby starsze i osoby potrzebujące lub znajdujące się w trudnej sytuacji życiowej);
- duża liczba osób objętych incydentem (im większa, tym wyższe prawdopodobieństwo wystąpienia negatywnego skutku).

OCENA RYZYKA

Wysokie ryzyko - Przykład

Błąd systemowy w szpitalu spowodował błędne zaktualizowanie danych medycznych pacjentów, w tym informacji o alergiach i przyjmowanych lekach. Błędy te przez dłuższy czas pozostały niewykryte, co stanowiło poważne zagrożenie dla zdrowia i życia pacjentów. W przypadku kolejnej hospitalizacji lub nagłego zabiegu mogliby oni otrzymać niewłaściwe leki lub przejść nieodpowiednie procedury medyczne, co mogłoby prowadzić do poważnych reakcji alergicznych, niebezpiecznych interakcji leków, a nawet śmiertelnych powikłań. W takiej sytuacji naruszenie integralności może skutkować bezpośrednim uszczerbkiem na zdrowiu i znacznym obniżeniem bezpieczeństwa pacjentów, którzy ufają, że dokumentacja medyczna odzwierciedla ich rzeczywisty stan zdrowia. Z uwagi na poważne zagrożenie zdrowia administrator uznał, że incydent stworzył **wysokie ryzyko** naruszenia praw lub wolności osób fizycznych.

ZAGROŻENIA


Brak ryzyka
• dane publicznie dostępne
• dane nieczytelne
• definitywne zaradzenie
Dokumentowanie naruszenia
Ryzyko
• możliwość wystąpienia skutków
Zgłoszenie naruszenia
Dokumentowanie naruszenia
Wysokie ryzyko
• znaczna waga skutków
• duże prawdopodobieństwo
Zgłoszenie naruszenia
Zawiadomienie osób fizycznych
Dokumentowanie naruszenia

Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

Informowanie osób fizycznych o zdarzeniach, które nie stwarzają wysokiego ryzyka nie jest zalecane. Nadmiar komunikatów w tym zakresie może skutkować niepotrzebnym stresem lub przeciążeniem informacyjnym, prowadzącym do ignorowania przez odbiorców podobnych wiadomości, co w konsekwencji mogłoby osłabić znaczenie zawiadomień

Uwaga!

Jeżeli naruszenie ochrony danych osobowych wywołuje wysokie ryzyko wobec tylko niektórych osób nim objętych, administratorzy powinni zawiadomić wyłącznie te osoby.

Zawiadamianie osób, których dane dotyczą, o naruszeniach ochrony danych osobowych

„Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych” to oficjalne poinformowanie osoby fizycznej o naruszeniu, które może wpłynąć na poufność, integralność lub dostępność jej danych osobowych.

Administratorzy mają obowiązek zawiadamiać o naruszeniach ochrony danych osobowych, które mogą powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

Celem zawiadomienia jest ograniczenie potencjalnych szkód dla osób, których dane dotyczą, poprzez przekazanie im istotnych informacji o zdarzeniu oraz rekomendowanych środkach ostrożności.

KARY

Fortum Marketing and Sales Polska S.A. (2023) – 4 911 732 PLN

Najwyższa kara nałożona przez polski organ nadzorczy dotyczyła spółki z branży energetycznej – Fortum Marketing and Sales Polska S.A. Naruszenie miało miejsce podczas wprowadzania zmian w systemie przechowywania dokumentów zawierających dane klientów. W trakcie tych prac doszło do skopiowania bazy danych przez nieuprawniony podmiot, co wskazywało na niewystarczający nadzór nad procesorem danych.

Morele.net (2019) 2 830 410 PLN.

Naruszenie polegało na niewystarczających zabezpieczeniach technicznych i organizacyjnych, co doprowadziło do nieuprawnionego dostępu do danych osobowych około 2,2 miliona klientów. Atakujący uzyskali dostęp do takich informacji jak imiona, nazwiska, adresy e-mail oraz numery telefonów klientów. Brak odpowiednich środków bezpieczeństwa, takich jak mechanizmy uwierzytelniania i monitorowania, przyczynił się do tego incydentu

KARY

Virgin Mobile Polska Sp. z o.o. (2020) – 1 968 524 PLN

Operator telekomunikacyjny Virgin Mobile Polska Sp. z o.o. został ukarany kwotą 1 968 524 PLN za naruszenie RODO polegające na braku wdrożenia odpowiednich środków technicznych i organizacyjnych, co skutkowało nieuprawnionym dostępem do danych osobowych klientów. Incydent ten ujawnił niedociągnięcia w systemach bezpieczeństwa oraz brak skutecznego monitorowania i reagowania na zagrożenia.

ClickQuickNow Sp. z o.o. (2019) – 201 000 PLN

Spółka została ukarana za przetwarzanie danych osobowych w celach marketingowych bez zgody osób, których dane dotyczyły, co stanowiło naruszenie zasad legalności przetwarzania danych. Firma wysyłała niezamówione informacje handlowe do osób, które nie wyraziły na to zgody, co jest sprzeczne z przepisami RODO dotyczącymi zgody na przetwarzanie danych w celach marketingowych.

KARY

Samodzielny Publiczny Szpital dla Nerwowo i Psychicznie Chorych w Międzyrzeczu

W tej placówce stwierdzono brak zawarcia dwóch umów powierzenia przetwarzania danych, w których szpital powinien wystąpić jako administrator danych. Niedopełnienie tego obowiązku mogło prowadzić do niekontrolowanego przetwarzania danych pacjentów przez podmioty trzecie, co stanowiło naruszenie przepisów o ochronie danych

Potencjalne naruszenie ochrony danych osobowych związane z Unijnym Certyfikatem COVID

W październiku 2021 roku Ministerstwo Zdrowia poinformowało o potencjalnym naruszeniu ochrony danych osobowych. Na jednym z portali społecznościowych zamieszczono poprawnie walidujący kod QR Unijnego Certyfikatu COVID wystawiony na postać historyczną. Incydent ten wskazywał na możliwość nieuprawnionego dostępu do systemu generującego certyfikaty, co mogło prowadzić do fałszowania dokumentów potwierdzających szczepienie

KARY

W lipcu 2023 roku w **Centrum Medycznym Ujastek w Krakowie** doszło do poważnego naruszenia ochrony danych osobowych. Na oddziale neonatologii, w dwóch salach, zainstalowano kamery monitoringu, które rejestrowały zarówno noworodki, jak i ich matki podczas czynności takich jak pielęgnacja czy karmienie. Co istotne, ani pacjentki, ani personel medyczny nie zostali poinformowani o istnieniu tego monitoringu. Prezes Urzędu Ochrony Danych Osobowych (UODO) nałożył na placówkę kary w łącznej wysokości ponad **1,1 mln złotych**.

KARY

Centrum Medycznym Ujastek w Krakowie

Decyzja ta wynikała z faktu, że szpital nie spełnił podstawowych wymogów dotyczących legalności monitoringu, takich jak brak poinformowania osób nagrywanych oraz brak odpowiedniego uzasadnienia dla stosowania takiego rozwiązania. Dodatkowo, UODO zwrócił uwagę na niewłaściwe zabezpieczenie przechowywanych nagrań. Nośniki z zarejestrowanym materiałem były przechowywane w sposób umożliwiający dostęp do nich osobom nieuprawnionym, co stanowiło dodatkowe naruszenie przepisów o ochronie danych osobowych.

*kamery monitoringu zostały zamontowane w sposób niejawny. Według dostępnych informacji, urządzenia te były ukryte w zegarach ściennych, co umożliwiało rejestrowanie obrazu bez wiedzy pacjentek, noworodków oraz personelu medycznego.

ZGŁASZANIE NARUSZEŃ

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą.

W przypadku zgłaszania naruszeń IOD pełni funkcję doradczą.

Dziękuję za uwagę i zachęcam do zadawania pytań

Arnold.partner@gmail.com

Tlf. 602 551 851