MATERIAŁY DYDAKTYCZNE 120

Zgłaszanie naruszeń ochrony danych osobowych

KATOWICE 2024

podkom. Paweł Dobaj
podkom. Grzegorz Waleczek
Zakład Prewencji i Ruchu Drogowego

Zgłaszanie naruszeń ochrony danych osobowych

Katowice 2024

Nadzór merytoryczny:
nadkom. Michał Stępień

Redakcja, korekta, skład:
Paweł Mięsiak

Spis treści

Wstęp

Ochrona danych osobowych jest jednym z najistotniejszych elementów zapewniania prywatności i bezpieczeństwa w cyfrowym świecie. Zgodnie z rosnącą liczbą zagrożeń związanych z przetwarzaniem danych osobowych, zarówno na poziomie krajowym, jak i międzynarodowym, konieczne stało się wprowadzenie szczegółowych regulacji, które mają na celu nie tylko ochronę tych danych, ale także nakładanie odpowiednich obowiązków na administratorów danych w przypadku ich naruszenia. W obliczu rozwoju technologii, a także coraz częstszych incydentów związanych z niewłaściwym lub nielegalnym przetwarzaniem danych, systematyczne zarządzanie bezpieczeństwem informacji stało się absolutną koniecznością.

W niniejszej publikacji omawiane są kluczowe aspekty dotyczące ochrony danych osobowych w kontekście naruszeń ochrony tych danych oraz procedur, które należy podjąć, aby skutecznie reagować na takie incydenty. Przedstawione zostały zarówno definicje fundamentalnych pojęć związanych z ochroną danych osobowych, jak i szczegółowe przepisy prawne odnoszące się do zgłaszania takich naruszeń odpowiednim organom oraz zawiadamiania osób, których dane dotyczą.

Niniejszy pozycja jest skierowana do pracowników Policji, którzy mają podstawową wiedzę z zakresu ochrony danych osobowych oraz styczność z tą tematyką, w tym do administratorów danych, inspektorów ochrony danych oraz każdego, kto pragnie zrozumieć mechanizmy i obowiązki związane z przetwarzaniem danych osobowych. Zawiera ona szereg praktycznych informacji i wskazówek, które pozwolą nie tylko na spełnienie wymogów prawnych, ale także na właściwe zarządzanie ryzykiem związanym z naruszeniami ochrony danych osobowych.

W pierwszej części publikacji omówiono podstawowe definicje, które stanowią fundament rozumienia obowiązków związanych z ochroną danych osobowych. Pojęcia takie jak „naruszenie ochrony danych osobowych", „dane osobowe", „dane dotyczące zdrowia" czy „dane dotyczące karalności" są kluczowe, ponieważ pozwalają określić, jakie dane podlegają szczególnej ochronie oraz wskazują na potencjalne zagrożenia związane z ich niewłaściwym przetwarzaniem.

Kolejnym ważnym zagadnieniem, które zostało poruszone jest procedura zgłaszania naruszeń ochrony danych osobowych, zarówno w kontekście wymogów zawartych w Rozporządzeniu o Ochronie Danych Osobowych (RODO), jak i w polskim systemie prawnym, szczególnie na podstawie ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości (UDODO). Zgłoszenie

naruszenia danych organowi nadzorczemu w terminie 72 godzin oraz obowiązek powiadomienia osób, których dane dotyczą stanowią kluczowe elementy, które mają na celu zminimalizowanie skutków ewentualnych naruszeń i zapewnienie osób fizycznych o bezpieczeństwie ich danych osobowych.

Ostatnia część publikacji dotyczy procedur zgłaszania naruszeń oraz wzorów dokumentów wymaganych podczas obsługi zdarzeń. Zawiera szczegółowe informacje na temat obowiązków administratorów danych w odniesieniu do zgłaszania naruszeń Prezesowi Urzędu Ochrony Danych Osobowych, a także podkreśla znaczenie dokumentowania takich przypadków, co ma na celu zarówno spełnienie wymogów prawnych, jak i zapewnienie pełnej przejrzystości w zakresie ochrony danych osobowych.

Celem tej publikacji jest nie tylko przedstawienie przepisów prawnych, ale także pomoc w ich praktycznym zastosowaniu, poprzez przedstawienie konkretnych rozwiązań, które można wdrożyć w organizacjach w celu skutecznego zarządzania danymi osobowymi oraz zapewnienia ich odpowiedniej ochrony przed naruszeniami. Dzięki tej publikacji czytelnicy będą w stanie lepiej zrozumieć obowiązki związane z ochroną danych osobowych oraz wdrożyć procedury, które zapewnią zgodność z obowiązującymi regulacjami, chroniąc tym samym prawa i wolności osób fizycznych.

Wykaz skrótów zastosowanych w publikacji:

- **RODO –** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 216/679 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).
- **UDODO** – ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości.
- **UODO** – Urząd Ochrony Danych Osobowych.
- **Prezes Urzędu** – Prezes Urzędu Ochrony Danych Osobowych.

Rozdział 1.
Wybrane definicje

1.1. Dane osobowe

Zgodnie z artykułem 4 pkt 1 RODO oraz artykułem 4 pkt 5 UDODO, „dane osobowe" oznaczają wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej. Osobą fizyczną możliwą do zidentyfikowania jest osoba, którą można zidentyfikować bezpośrednio lub pośrednio na podstawie takich informacji jak imię, nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy czy inne szczególne czynniki określające tożsamość fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną osoby[1].

Definicja danych osobowych wyznacza zakres ochrony prawnej w zakresie przetwarzania informacji o ludziach. Obejmuje to wszelkie informacje, które mogą zostać przypisane do konkretnej osoby fizycznej tzn. osoby, którą da się zidentyfikować, nawet pośrednio, na podstawie dostępnych danych. Kluczową kwestią w tej definicji jest rozróżnienie między informacjami, które pozwalają na pełną identyfikację danej osoby, a tymi, które tylko umożliwiają jej pośrednią identyfikację.

„Zidentyfikowana osoba fizyczna" to taka, której tożsamość jest już znana lub może być ustalona na podstawie dostępnych informacji. Z kolei „osoba możliwa do zidentyfikowania" to taka, którą można ustalić, łącząc dane osobowe z innymi informacjami. Dla lepszego zrozumienia tej definicji warto posłużyć się przykładami[2].

Przykłady danych osobowych:

- **imię i nazwisko:** najbardziej oczywisty przykład identyfikatora, umożliwiający natychmiastową identyfikację osoby. Przykład: „Anna Kowalska". Zaznaczyć należy, że od okoliczności sprawy zależy czy wskazane dane pozwalają na bezpośrednią lub pośrednią identyfikację osoby fizycznej, ponieważ wskazany przykład „Anna Kowalska" na portalu Facebook odpowiada, co najmniej kilkudziesięciu osobom,
- **numer identyfikacyjny**: może to być numer PESEL, NIP czy numer paszportu. Te numery przypisane do osoby w bazach danych publicznych lub prywatnych

[1] 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).

[2] E. Bielak-Jooma, D. Lubasz, *RODO Ogólne rozporządzenie o ochronie danych – komentarz*, str. 163-185.

stanowią unikalny identyfikator. Przykład: „PESEL 44051401512" jednoznacznie identyfikuje osobę w Polsce,
- **dane o lokalizacji**: informacje o miejscu pobytu osoby np. adres zamieszkania, mogą stanowić dane osobowe, szczególnie gdy są powiązane z innymi informacjami. Przykład: adres „ul. Powstańców Warszawy 12, Warszawa" może wskazywać na konkretną osobę, jeśli jest częścią większej bazy danych,
- **identyfikator internetowy**: to każda informacja, która pomaga zidentyfikować użytkownika w sieci. Przykłady to adresy IP, pliki cookie czy login. Na przykład, adres IP „192.168.1.1" może być powiązany z konkretnym użytkownikiem, zwłaszcza jeśli dane są zbierane przez strony internetowe i systemy śledzenia,
- **szczególne czynniki tożsamości**: to m.in. dane dotyczące zdrowia, zachowań czy preferencji, które pomagają określić tożsamość osoby. Przykład: „Osoba z grupą krwi A+, alergią na orzeszki ziemne i preferencjami do muzyki klasycznej" – te informacje pomagają nakreślić obraz osoby, chociaż sama w sobie nie są wystarczające do jednoznacznej identyfikacji.

W życiu codziennym spotykamy się z danymi osobowymi na każdym kroku – od wypełniania formularzy online, przez korzystanie z usług bankowych, po rejestrację na stronach internetowych. Każde z tych działań wiąże się z przetwarzaniem danych, które mogą dotyczyć nas osobiście. Zatem każda informacja, która może pozwolić na naszą identyfikację, stanowi dane osobowe, co stawia przed firmami i instytucjami obowiązek ich ochrony. W dobie cyfryzacji szczególną uwagę zwraca się na dane internetowe, takie jak adresy IP, cookies czy identyfikatory urządzeń, które coraz częściej są używane do śledzenia użytkowników w Internecie, tworzenia ich profili czy personalizowania reklam.

Zrozumienie definicji danych osobowych jest kluczowe dla prawidłowego stosowania przepisów ochrony prywatności. Każda informacja, która pozwala na identyfikację osoby, jest traktowana jako dane osobowe. W związku z tym, zarówno osoby fizyczne, jak i instytucje przetwarzające dane, muszą być świadome obowiązków związanych z ich ochroną. W praktyce oznacza to dbanie o bezpieczeństwo informacji, które mogą być użyte do identyfikacji osób, i stosowanie odpowiednich środków zaradczych, aby zapewnić zgodność z przepisami RODO i UDODO.

1.2. Dane szczególnej kategorii danych osobowych

Zgodnie z art. 9 ust. 1 RODO, przetwarzanie szczególnych kategorii danych osobowych jest zabronione. Do danych osobowych szczególnej kategorii zaliczają się:
- pochodzenie rasowe lub etniczne,
- poglądy polityczne,

– przekonania religijne lub światopoglądowe,
– przynależność do związków zawodowych,
– dane genetyczne,
– dane biometryczne wykorzystywane w celu jednoznacznego zidentyfikowania osoby fizycznej,
– dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby.

Katalog tych danych ma charakter zamknięty, co oznacza, że nie można go rozszerzać o inne kategorie danych, a przetwarzanie takich informacji jest obarczone szczególnymi restrykcjami.

Przetwarzanie danych szczególnych kategorii wiąże się z wyjątkową ochroną, ponieważ dotyczą one najintymniejszych i najbardziej wrażliwych aspektów życia człowieka. Informacje na temat pochodzenia rasowego, poglądów politycznych, przekonań religijnych, orientacji seksualnej czy zdrowia mogą być wykorzystywane w sposób nieuprawniony, narażając osoby na poważne konsekwencje, w tym dyskryminację, utratę prywatności czy inne formy naruszenia podstawowych praw i wolności. Z tego względu, aby zapewnić odpowiednią ochronę prywatności i bezpieczeństwa danych osobowych, przetwarzanie tych danych wymaga szczególnych podstaw prawnych i powinno odbywać się zgodnie z rygorystycznymi zasadami RODO.

Zgodnie z RODO, przetwarzanie tych danych jest generalnie zabronione, chyba że zachodzą określone wyjątki, takie jak uzyskanie zgody osoby, której dane dotyczą, lub spełnienie innych warunków określonych w artykule 9 ust. 2 RODO[3].

Dane szczególnych kategorii mogą obejmować różnorodne informacje, które mogą ujawniać wrażliwe aspekty tożsamości osoby fizycznej. Poniżej zostały wymienione informacje, które są zaliczane do danych szczególnych kategorii:

– **pochodzenie rasowe lub etniczne**: dane dotyczące rasy lub pochodzenia etnicznego mogą wskazywać na to, do jakiej grupy społecznej należy dana osoba. Ich przetwarzanie może prowadzić do dyskryminacji, dlatego wymaga spełnienia szczególnych przesłanek prawnych,
– **poglądy polityczne**: informacje o tym, do jakiej partii politycznej należy osoba lub jakie ma poglądy polityczne, są również wrażliwe. Bez odpowiednich podstaw prawnych ich przetwarzanie może prowadzić do naruszenia prywatności oraz wolności obywatelskich,
– **orientacja seksualna**: dane dotyczące orientacji seksualnej osoby są szczególnie wrażliwe, ponieważ dotyczą aspektu jej prywatnego życia, a ich ujawnienie może prowadzić do poważnych konsekwencji społecznych, w tym do dyskryminacji,

[3] E. Bielak-Jooma, M. Kuba, *RODO Ogólne rozporządzenie o ochronie danych – komentarz*, str. 437-447.

- **przekonania religijne lub światopoglądowe**: informacje dotyczące religii, wyznania lub przekonań światopoglądowych mogą mieć znaczący wpływ na życie osoby, a ich ujawnienie bez zgody osoby, której dotyczą, może prowadzić do naruszenia jej prywatności i ochrony wolności sumienia,
- **przynależność do związków zawodowych**: informacje o przynależności do związków zawodowych mogą być wrażliwe, ponieważ dotyczą działalności zawodowej i zaangażowania osoby w organizacje reprezentujące jej interesy, co może stanowić podstawę do jej ewentualnego dyskryminowania w pracy.

W każdym z tych przypadków przetwarzanie danych musi opierać się na odpowiednich podstawach prawnych, takich jak zgoda osoby, której dane dotyczą, wykonanie umowy, ochrona interesów publicznych itp. Zasadniczo, bez tych podstaw przetwarzanie takich danych jest nielegalne, co podkreśla konieczność zachowania najwyższych standardów ochrony prywatności i danych osobowych.

Przykłady przetwarzanie danych szczególnej kategorii:

- **sektor medyczny**: w szpitalach, klinikach czy ośrodkach zdrowia przetwarzanie danych dotyczących zdrowia pacjentów jest niezbędne do świadczenia odpowiedniej opieki zdrowotnej. Zgoda pacjenta, a także obowiązek prawny wynikający z przepisów zdrowotnych stanowią podstawę przetwarzania takich danych. Jednak bez tych przesłanek przetwarzanie danych zdrowotnych, np. przez pracodawcę lub osobę trzecią byłoby nielegalne,
- **sektor zatrudnienia**: pracodawcy mogą zbierać dane dotyczące przynależności do związków zawodowych pracowników tylko w specyficznych przypadkach, np. w celu przestrzegania przepisów prawa pracy lub zbiorowych umów o pracę. Jednak zbieranie takich informacji bez zgody pracownika jest niezgodne z RODO,
- **marketing**: firmy zajmujące się marketingiem muszą unikać zbierania danych wrażliwych, takich jak orientacja seksualna, poglądy polityczne czy przekonania religijne. Ich przetwarzanie może prowadzić do naruszenia prywatności i skutkować poważnymi sankcjami.

Dane szczególnych kategorii zwane także danymi wrażliwymi, są objęte szczególnymi zasadami ochrony w ramach RODO. Ich przetwarzanie może odbywać się tylko w określonych sytuacjach, takich jak uzyskanie zgody osoby, której dane dotyczą, wykonanie umowy, ochrona interesów publicznych czy spełnienie innych przesłanek prawnych. W każdym przypadku przetwarzanie danych wrażliwych powinno odbywać się zgodnie z zasadą minimalizacji danych oraz w sposób zapewniający pełną ochronę praw i wolności osób, których dane dotyczą. Bez odpowiednich podstaw prawnych, przetwarzanie danych takich jak pochodzenie rasowe, poglądy polityczne,

orientacja seksualna czy przynależność do związków zawodowych jest nielegalne, a każda próba ich wykorzystania wiąże się z poważnymi konsekwencjami prawnymi.

1.3. Dane dotyczące zdrowia

Zgodnie z artykułem 4 pkt 15 RODO oraz artykułem 4 pkt 3 UDODO, dane dotyczące zdrowia to dane osobowe dotyczące zdrowia fizycznego lub psychicznego osoby fizycznej, w tym dane o korzystaniu z usług opieki zdrowotnej, które ujawniają informacje o stanie jej zdrowia[4].

Dane dotyczące zdrowia są jedną z najbardziej wrażliwych kategorii danych osobowych, ponieważ bezpośrednio odnoszą się do prywatności i intymności osoby. Rozporządzenie RODO oraz ustawa UDODO nadaje tym danym szczególną ochronę, uznając je za dane szczególnej kategorii, które wymagają wyższych standardów bezpieczeństwa podczas przetwarzania. Z tego powodu dane dotyczące zdrowia mogą obejmować informacje o chorobach, diagnozach, leczeniu czy stanie fizycznym lub psychicznym danej osoby. Takie dane są zbierane przez placówki medyczne, ale także przez pracodawców, w sytuacjach związanych z usprawiedliwieniem nieobecności pracownika z powodu choroby[5].

Przykłady naruszeń ochrony danych dotyczących zdrowia

- **informacja o nieobecności pracownika poprzez umieszczanie zapisu o jego zwolnieniu lekarskim w publicznych dokumentach** – przykładem naruszenia ochrony danych osobowych o zdrowiu jest wpisywanie informacji o zwolnieniu lekarskim w liście obecności w firmie, oznaczając go skrótem „CH" lub „L4". Tego typu oznaczenie ujawnia stan zdrowia pracownika, co może naruszać jego prywatność. Zgodnie z RODO, administrator powinien zachować poufność informacji o zdrowiu pracowników i nie publikować takich danych bez ich zgody, a zwolnienie lekarskie powinno być traktowane jako dokument medyczny, a nie informacja powszechnie dostępna,
- **publikowanie informacji o leczeniu się osoby w Internecie** – kolejnym przykładem nieuprawnionego ujawnienia danych osobowych o zdrowiu jest sytuacja, która miała miejsce, gdy minister zdrowia opublikował wpis na platformie X, w którym zdradził szczegóły dotyczące zdrowia pewnego lekarza, który wystawiał sobie recepty. Tego typu publiczne ujawnienie informacji o zdrowiu osoby, szczególnie bez jej zgody, stanowi poważne naruszenie przepisów o ochronie danych osobowych.

[4] Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, dalej UDODO.

[5] E. Bielak-Jooma, M. Kuba, tamże, str. 277-281.

Informacje o leczeniu, podobnie jak inne dane medyczne, mogą być udostępniane tylko w ściśle określonych sytuacjach opartych o przepis prawa lub za zgodą osoby, której te dane dotyczą.

Dane dotyczące zdrowia wymagają szczególnej ochrony, ponieważ dotyczą najbardziej osobistej sfery życia człowieka. Wszelkie działania, które prowadzą do nieuprawnionego ujawnienia takich informacji, mogą prowadzić do poważnych konsekwencji prawnych. Dlatego tak ważne jest, aby każda organizacja, instytucja czy osoba odpowiedzialna za przetwarzanie danych medycznych stosowała się do zasad RODO i UDODO, zapewniając odpowiednie zabezpieczenia tych informacji[6].

1.4. Dane dotyczące wyroków skazujących i czynów zabronionych

Zgodnie z artykułem 10 RODO, przetwarzanie danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa jest dozwolone wyłącznie pod nadzorem władz publicznych lub jeśli przetwarzanie jest dozwolone prawem Unii lub państwa członkowskiego, które przewidują odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. W szczególności, wszelkie kompletne rejestry wyroków skazujących mają być prowadzone wyłącznie pod nadzorem władz publicznych.

Dane dotyczące karalności to szczególna kategoria danych osobowych, które obejmują informacje o wyrokach skazujących, naruszeniach prawa oraz związanych z nimi środkach bezpieczeństwa. Są to dane, które mogą ujawniać przestępstwa, za które dana osoba została skazana, oraz środki, które zostały jej nałożone (np. kara pozbawienia wolności, grzywna czy środek zabezpieczający). Ze względu na charakter tych danych, które odnoszą się do wrażliwych informacji o osobie, ich przetwarzanie wiąże się z dużym ryzykiem naruszenia praw i wolności osoby, której dotyczą.

Przetwarzanie takich danych jest ściśle regulowane przez prawo, w tym przepisy RODO i może odbywać się tylko w określonych przypadkach. Zgodnie z art. 10 RODO, dane dotyczące karalności można przetwarzać wyłącznie, gdy istnieje wyraźna podstawa prawna, która do tego upoważnia, a także pod nadzorem odpowiednich organów publicznych. Przykładem może być konieczność przetwarzania danych o karalności w ramach rejestrów, takich jak Krajowy Rejestr Karny, który gromadzi informacje o skazanych. w tym o wyrokach sądowych i środkach zabezpieczających[7].

[6] Tamże.
[7] Tamże.

Przykłady przetwarzania danych o karalności

- **przetwarzanie danych o karalności w przypadku nauczycieli** – nauczyciele muszą przed podjęciem pracy posiadać zaświadczenie o niekaralności. Jest to wymóg prawny, który ma na celu zapewnienie bezpieczeństwa dzieciom i młodzieży, którym nauczyciele będą przekazywać wiedzę i pełnić rolę wychowawczą. Z tego względu, zaświadczenie o niekaralności jest wymagane przez przepisy prawa,
- **przetwarzanie danych o karalności w urzędach** – w przypadku niektórych stanowisk w urzędach, takich jak stanowiska kierownicze, pracodawca może wymagać od kandydatów zaświadczenia o niekaralności. Wymóg ten wynika z ustawy o pracownikach samorządowych, która przewiduje konieczność przedstawienia zaświadczenia o niekaralności, szczególnie w kontekście pełnienia funkcji publicznych[8],
- **niezgodne z prawem żądanie zaświadczenia o niekaralności** – pracodawca nie ma prawa żądać od pracownika zaświadczenia o niekaralności ani oświadczenia na ten temat, jeśli nie wynika to z przepisu prawa. Przykładem może być sytuacja, gdy pracodawca prosi o takie zaświadczenie od pracownika na stanowisku, które nie wiąże się z żadnymi szczególnymi wymaganiami dotyczącymi bezpieczeństwa publicznego, a żądanie to nie znajduje podstawy w przepisach.

Dane dotyczące karalności są szczególnym rodzajem danych osobowych, które wymagają szczególnej ochrony, ponieważ ujawniają wrażliwe informacje o osobach skazanych za przestępstwa. Ich przetwarzanie jest możliwe tylko w określonych przypadkach, w których istnieje wyraźna podstawa prawna np. w przypadku nauczycieli, pracowników urzędów lub osób pełniących funkcje publiczne. Pracodawcy nie mogą żądać takich informacji od pracowników, jeśli nie ma do tego podstawy prawnej, a jakiekolwiek naruszenie tych zasad może prowadzić do poważnych konsekwencji prawnych.

1.5. Naruszenie ochrony danych

Zgodnie z artykułem 4 punkt 12 RODO jak i artykułem 4 pkt 6 UDODO, naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa danych, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych, które są przesyłane, przechowywane lub w jakikolwiek sposób przetwarzane[9].

[8] Ustawa z dnia 21 listopada 2008 roku o pracownikach samorządowych (Dz.U. 2008 nr 223 poz.1458).

[9] UDODO.

Definicja naruszenia ochrony danych osobowych ma kluczowe znaczenie, ponieważ wyznacza granice odpowiedzialności administratorów danych za bezpieczeństwo informacji. Naruszenie ochrony danych osobowych nie odnosi się wyłącznie do fizycznego usunięcia danych, ale obejmuje także nieuprawnione zmiany, ujawnienie czy dostęp do danych, które nie były do tego upoważnione. Oznacza to, że w przypadku jakiejkolwiek sytuacji, w której dane osobowe zostaną narażone na niezamierzony dostęp, zmienione lub ujawnione, administrator danych ma obowiązek zgłoszenia tego faktu odpowiednim organom nadzorczym i poinformowania osób, których dane zostały naruszone.

Ważnym aspektem tej definicji jest fakt, że nie trzeba, aby naruszenie bezpieczeństwa danych miało charakter umyślny. Może również dojść do przypadkowego naruszenia ochrony danych osobowych, jeśli środki ochrony danych zawiodą, a wynikłe z tego konsekwencje mogą prowadzić do nieuprawnionego dostępu, zniszczenia, zmodyfikowania lub ujawnienia danych, mamy do czynienia z naruszeniem ochrony danych osobowych[10].

Przykłady naruszeń ochrony danych osobowych

- przypadkowe utracenie danych osobowych przechowywanych: laptop z danymi osobowymi klientów zostaje zgubiony przez pracownika firmy. W wyniku tego naruszenia dane zostały utracone, ponieważ laptop nie był odpowiednio zabezpieczony przed kradzieżą (np. brak szyfrowania). Przypadkowe utracenie danych jest więc naruszeniem integralności danych, jeśli dane znikną w sposób niezaplanowany i nieuprawniony,
- przypadkowe ujawnienie danych osobowych przesyłanych: przykładem może być firma, która wysyła dane osobowe swoich klientów do niewłaściwego odbiorcy (np. wysyłając e-mail z załącznikiem, który miał być wysłany do klienta A, a trafił do klienta B). Tego rodzaju przypadkowe ujawnienie danych osobowych stanowi naruszenie ochrony prywatności, ponieważ dane trafiły do osoby, która nie miała do nich prawa dostępu,
- niezgodny z prawem nieuprawniony dostęp do danych osobowych przechowywanych: Może się zdarzyć, że pracownik firmy, który nie ma odpowiednich uprawnień, uzyska dostęp do bazy danych zawierającej dane osobowe klientów. Na przykład, osoba pracująca w dziale marketingu przegląda pliki zawierające dane medyczne pacjentów, co stanowi nieuprawniony dostęp do danych osobowych wbrew przepisom prawa,

[10] E. Bielak-Jooma, W. Chomiczewski, *RODO Ogólne rozporządzenie o ochronie danych – komentarz*, str. 263-267.

– niezgodne z prawem zmodyfikowanie danych osobowych w inny sposób przetwarzanych: Zmiana danych osobowych bez odpowiednich uprawnień jest również naruszeniem ochrony danych osobowych. Przykładem może być sytuacja, w której pracownik działu HR zmienia dane kontaktowe pracownika bez jego zgody lub wiedzy, np. zmienia adres e-mail lub numer telefonu, co skutkuje niezgodnym z prawem przetwarzaniem tych danych.

Zrozumienie definicji naruszenia ochrony danych osobowych i praktycznych przykładów jej zastosowania jest istotne dla każdej osoby zajmującej się ochroną danych osobowych w firmach i instytucjach. Warto pamiętać, że naruszenie ochrony danych osobowych nie musi wiązać się z działaniem celowym – wystarczy, że dochodzi do sytuacji, w której dane osobowe są nieuprawnione zniszczone, zmodyfikowane, ujawnione lub dostępne. Każda organizacja przetwarzająca dane osobowe powinna dbać o odpowiednie zabezpieczenia i procedury zgłaszania naruszeń, aby zapewnić zgodność z przepisami RODO oraz UDODO i chronić prywatność osób, których dane są przetwarzane.

1.6. Prawa i wolności osób fizycznych

Zgodnie z artykułem 24 RODO jak i artykułem 31 UDODO, administrator danych osobowych ma obowiązek wdrożenia odpowiednich środków technicznych i organizacyjnych, które zapewnią zgodność przetwarzania danych z wymogami rozporządzenia i umożliwią wykazanie tego w razie potrzeby. Zgodnie z tym przepisem, administrator musi przeprowadzać ocenę ryzyka związaną z przetwarzaniem danych, uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw i wolności osób fizycznych. Środki ochrony danych są również poddawane regularnym przeglądom i aktualizacjom, w celu zapewnienia ich skuteczności. W przypadku przetwarzania danych, administrator może również wdrożyć odpowiednie polityki ochrony danych, które będą pomocne przy wykazaniu przestrzegania przepisów RODO. Natomiast w przypadku przetwarzania danych osobowych na podstawie UDODO, administrator ma ustawowy obowiązek opracowania i wdrożenia polityk ochrony danych osobowych.

Prawa i wolności osób fizycznych to zasady, które gwarantują ochronę prywatności i bezpieczeństwa danych osobowych w kontekście ich przetwarzania. Przepisy ochrony danych osobowych stawiają na pierwszym miejscu prawa jednostek, umożliwiając im kontrolę nad swoimi danymi osobowymi[11]. Prawa te obejmują m.in.:

[11] *RODO Ogólne rozporządzenie o ochronie danych, komentarz*, red. E. Bielak-Jooma, D. Lubasz, str. 585-599.

- **prawo do prywatności** – każda osoba ma prawo do ochrony swojego życia prywatnego. Dotyczy to nie tylko kwestii fizycznych, jak np. adres zamieszkania, ale także bardziej intymnych spraw, takich jak zdrowie, preferencje czy przekonania,
- **prawo do bycia poinformowanym** – osoba, której dane są przetwarzane ma prawo do jasnej informacji o tym, jakie dane są zbierane, w jakim celu i przez kogo. Oznacza to, że organizacje muszą zapewnić przejrzystość w kwestii przetwarzania danych,
- **prawo do dostępu** – osoba, której dane dotyczą, ma prawo do uzyskania informacji, czy jej dane są przetwarzane, a także do dostępu do nich. Przykładem może być sytuacja, w której klient banku prosi o kopię swoich danych, które bank przechowuje,
- **prawo do sprostowania danych** – każda osoba ma prawo do poprawienia swoich danych, jeśli są one nieaktualne lub nieprawdziwe. Przykładem może być aktualizacja adresu zamieszkania w firmie kurierskiej, gdyż poprzedni adres stał się nieaktualny,
- **prawo do usunięcia danych (prawo do bycia zapomnianym)** – osoby mogą żądać usunięcia swoich danych, gdy nie są one już potrzebne do celów, dla których zostały zgromadzone lub gdy przetwarzanie tych danych jest niezgodne z prawem,
- **prawo do przenoszenia danych** – osoby mają prawo do przenoszenia swoich danych z jednej organizacji do drugiej, co ma zastosowanie na przykład w przypadku zmiany dostawcy usług internetowych,
- **prawo do sprzeciwu** – osoba może sprzeciwić się przetwarzaniu jej danych w określonych sytuacjach, np. w przypadku marketingu bezpośredniego,
- **prawo do ograniczenia przetwarzania danych** – w określonych przypadkach, osoba może domagać się, aby jej dane nie były przetwarzane, np. gdy kwestionuje ich prawidłowość.

Z perspektywy przetwarzania danych osobowych, prawa i wolności osób fizycznych są zagwarantowane przez szereg przepisów zawartych w RODO i UDODO. Administrator danych musi podejmować odpowiednie kroki, aby zminimalizować ryzyko naruszenia tych praw. Przykładem jest firma, która przechowuje dane osobowe swoich klientów, musi zapewnić ich ochronę przed nieuprawnionym dostępem, usunięciem czy modyfikacją. Dodatkowo firma ta musi mieć możliwość udokumentowania, że przetwarzanie danych odbywa się zgodnie z przepisami o ochronie danych osobowych.

Przykłady naruszenia praw i wolności osób fizycznych

- **kradzież tożsamości** – przykładem ryzyka naruszenia prawa do prywatności może być sytuacja, w której dane osobowe, takie jak numer PESEL, adres zamieszkania

czy dane dotyczące płatności, zostaną wykradzione przez cyberprzestępców. Może to prowadzić do oszustwa lub kradzieży tożsamości,
- **dyskryminacja** – jeśli firma zbiera dane o pochodzeniu etnicznym swoich pracowników i wykorzystuje te informacje w sposób dyskryminujący, np. przy ustalaniu wynagrodzenia, stanowi to poważne naruszenie prawa do prywatności i wolności osób fizycznych,
- **naruszenie dobrego imienia** – ujawnienie nieaktualnych danych osobowych, np. wyroku sądowego w sprawie niekaralności, w sytuacji, gdy osoba już została zrehabilitowana, może prowadzić do naruszenia jej dobrego imienia i reputacji,
- **nieuprawniony dostęp do danych** – pracownicy w firmie mogą mieć dostęp do danych osobowych tylko w zakresie niezbędnym do realizacji swoich obowiązków służbowych. Jeśli nieautoryzowana osoba uzyska dostęp do tych danych, na przykład poprzez atak hakerski, może to prowadzić do poważnych naruszeń praw i wolności osób fizycznych.

Prawa i wolności osób fizycznych są kluczowe w kontekście przetwarzania danych osobowych, ponieważ każda osoba ma prawo do ochrony swojej prywatności. Administrator danych ma obowiązek wdrożenia odpowiednich środków ochrony, aby przetwarzanie danych było zgodne z prawem i nie naruszało tych praw. Przykłady z życia codziennego pokazują, jak łatwo naruszyć te prawa, co może prowadzić do poważnych konsekwencji zarówno dla osób, jak i organizacji. Dlatego też każda firma i instytucja przetwarzająca dane osobowe musi przestrzegać przepisów RODO/UDODO i dbać o bezpieczeństwo tych danych.

1.7. Przetwarzanie danych osobowych

Zgodnie z przepisami RODO i UDODO przetwarzanie danych osobowych oznacza „operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych, takich jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie”[12].

Pojęcie przetwarzania danych osobowych jest kluczowe w kontekście ochrony prywatności i bezpieczeństwa informacji, ponieważ określa wszelkie działania, które mogą wpływać na dane osobowe. Dane osobowe są wszelkimi informacjami, które umożliwiają identyfikację osoby fizycznej, takich jak imię, nazwisko, numer telefonu,

[12] UDODO.

adres zamieszkania, a także dane bardziej wrażliwe, takie jak dane zdrowotne czy dane biometryczne.

Przetwarzanie tych danych w sposób zgodny z prawem, sprawiedliwy i transparentny jest fundamentem ochrony prywatności osób fizycznych. Na podstawie RODO, każde przetwarzanie danych osobowych wymaga podstawy prawnej, na przykład zgody osoby, której dane dotyczą, lub konieczności przetwarzania danych w celu realizacji umowy. Zatem proces przetwarzania danych osobowych powinien odbywać się w sposób, który gwarantuje poszanowanie praw i wolności osób, których te dane dotyczą, w tym prawo do dostępu, poprawiania, usuwania, a także prawo do sprzeciwu wobec przetwarzania[13].

Wybrane przykłady przetwarzania danych

1. **zautomatyzowane przetwarzanie** – odnosi się do wszelkich operacji przeprowadzanych za pomocą systemów komputerowych bez udziału człowieka. Przykładem jest przetwarzanie danych osobowych w bazach danych lub systemach CRM, gdzie dane klientów są automatycznie zbierane, sortowane i wykorzystywane do analizy marketingowej, personalizacji ofert lub segmentacji rynku. Taki sposób przetwarzania danych jest szczególnie popularny w dużych firmach e-commerce i bankach, gdzie operacje są realizowane za pomocą algorytmów,
2. **niezautomatyzowane przetwarzanie** – odnosi się do działań wykonywanych manualnie, bez użycia specjalistycznych narzędzi informatycznych. Przykładem może być wypełnianie formularzy papierowych z danymi osobowymi, jak zgłoszenie do konkursu lub rejestracja na wydarzenie. Po zebraniu danych pracownik ręcznie wprowadza je do systemu komputerowego. Pomimo że dane są wprowadzane manualnie, proces ich przetwarzania jest częścią cyklu przetwarzania danych osobowych, który obejmuje zbieranie, przechowywanie, a w dalszej kolejności wykorzystywanie tych danych do określonego celu,
3. **zbieranie danych** – jest pierwszym etapem przetwarzania danych osobowych, który obejmuje pozyskiwanie informacji od osób, których dane dotyczą. Przykładami mogą być formularze zgłoszeniowe wypełniane online (np. rejestracja na stronie internetowej), wypełnianie ankiet w badaniach rynkowych, czy zbieranie CV podczas rekrutacji. Zbieranie danych może również obejmować gromadzenie informacji z publicznych źródeł, takich jak rejestry publiczne,
4. **utrwalanie danych** – oznacza ich zapisanie na nośnikach danych, które umożliwiają ich późniejsze wykorzystanie. Przykładem może być zapisanie rozmowy

[13] E. Bielak-Jooma, W. Chomiczewski, tamże, str. 263-267.

telefonicznej z klientem, zapisanie dokumentu zawierającego dane pracowników w systemie komputerowym lub nagrywanie obrazu z kamer monitoringu, gdzie rejestrowane są dane o wizerunku osób,

5. **usuwanie i niszczenie danych** – to operacje, które mają na celu całkowite usunięcie danych z systemu lub nośnika. Usuwanie polega na skasowaniu danych w sposób umożliwiający ich odzyskanie jedynie za pomocą specjalistycznych narzędzi, natomiast niszczenie danych oznacza fizyczne zniszczenie nośnika, na którym te dane były zapisane, np. zniszczenie twardego dysku komputerowego lub pocięcie papierowych dokumentów w niszczarce. Te operacje są szczególnie istotne w kontekście ochrony danych po zakończeniu ich przetwarzania, w celu zapewnienia, że dane nie będą dostępne dla nieupoważnionych osób,
6. **udostępnianie danych** – może odbywać się na różne sposoby. Może to obejmować przekazywanie danych pomiędzy różnymi podmiotami. Na przykład w ramach współpracy biznesowej lub między firmą a organem publicznym. Przykładem może być wysyłanie danych osobowych przez firmę kurierską do kontrahenta lub przekazywanie danych bankowych instytucjom finansowym w celu przeprowadzenia transakcji. W każdym przypadku udostępnienie danych powinno odbywać się na podstawie odpowiednich przepisów prawa i z poszanowaniem zgody osoby, której dane dotyczą.

Przetwarzanie danych osobowych to szereg różnorodnych działań, które są niezbędne w praktyce codziennej działalności biznesowej oraz w administracji publicznej. Jednakże każde przetwarzanie musi być zgodne z prawem i odbywać się w sposób, który gwarantuje ochronę praw osób fizycznych. Każda operacja na danych osobowych, począwszy od ich zbierania, przez przechowywanie, aż po usunięcie, musi być odpowiednio uzasadniona i oparta na podstawie prawnej, takiej jak zgoda osoby, której dane dotyczą lub inne uzasadnione podstawy przewidziane przez prawo.

Rozdział 2.
Zgłaszanie naruszeń ochrony danych osobowych

2.1. Art. 33 RODO

Artykuł 33 RODO precyzuje obowiązki administratora danych osobowych związane z zgłoszeniem naruszenia ochrony danych osobowych organowi nadzorczemu. Zgodnie z tym artykułem administrator danych musi zgłosić naruszenie danych osobowych w terminie nie dłuższym niż 72 godziny od momentu stwierdzenia naruszenia. Przepis ten odnosi się do sytuacji, w których dojdzie do naruszenia ochrony danych osobowych, np. gdy dane osobowe zostaną przypadkowo ujawnione lub zniszczone, gdy dojdzie do nieuprawnionego dostępu lub utraty danych, a także w innych przypadkach, które mogą zagrozić prywatności osób fizycznych.

Obowiązek administratora danych osobowych

Obowiązek zgłoszenia naruszenia ochrony danych osobowych nie jest zależny od tego, czy naruszenie spowoduje realne szkody dla osób, których dane dotyczą, czy też nie. Zgłoszenie ma na celu zapewnienie odpowiedniej reakcji ze strony organu nadzorczego, który może podjąć odpowiednie kroki w celu ochrony praw osób fizycznych. Należy podkreślić, że administrator danych jest odpowiedzialny za zgłoszenie naruszenia, ale to on również ocenia, czy naruszenie wiąże się z ryzykiem naruszenia praw i wolności osób fizycznych.

W zgłoszeniu administrator musi opisać charakter naruszenia ochrony danych, wskazać kategorie i liczbę osób, których dane zostały naruszone, a także kategorie danych, których naruszenie dotyczy. Ponadto zgłoszenie powinno zawierać dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego, pod którym można uzyskać więcej informacji na temat naruszenia. Ważne jest, aby zgłoszenie zawierało także opis możliwych konsekwencji naruszenia ochrony danych osobowych oraz informacje o środkach, które zostały podjęte w celu zaradzenia naruszeniu i minimalizacji jego skutków.

Zgłoszenie to ma być przekazane bez zbędnej zwłoki, a jeśli nie jest możliwe zgłoszenie w ciągu 72 godzin. Administrator musi dostarczyć pisemne wyjaśnienie przyczyn opóźnienia. Zgłoszenie to może być uzupełniane sukcesywnie, jeżeli nie wszystkie wymagane informacje są dostępne w momencie jego składania. Jednakże, jak wskazuje RODO, uzupełnienie musi odbywać się bez zbędnej zwłoki, co oznacza, że administrator ma obowiązek dostarczyć brakujące informacje w jak najkrótszym czasie.

Kiedy naruszenie nie wymaga zgłoszenia?

Zgłoszenie naruszenia do organu nadzorczego jest obowiązkowe, ale istnieje wyjątek, który dotyczy sytuacji, w których ryzyko naruszenia praw lub wolności osób fizycznych jest mało prawdopodobne. Oznacza to, że jeśli po dokonaniu oceny naruszenia administrator uzna, iż nie wiąże się ono z ryzykiem, które mogłoby zagrozić prawom osób fizycznych, nie ma obowiązku zgłaszania naruszenia do organu nadzorczego. Należy jednak pamiętać, że ryzyko to musi zostać ocenione przez administratora w sposób obiektywny, a decyzja o braku zgłoszenia musi być oparta na rzetelnej ocenie sytuacji.

Przykład sytuacji, w której ryzyko naruszenia praw osób fizycznych jest mało prawdopodobne to przypadek przypadkowego skasowania danych osobowych, które mogą zostać odzyskane z kopii zapasowej. Podobnie, jeśli dane zostały zaszyfrowane i utracony nośnik nie budzi ryzyka nieautoryzowanego dostępu do tych danych, administrator może uznać, że ryzyko jest znikome i naruszenie nie wymaga zgłoszenia.

Dokumentowanie naruszeń

Bez względu na to, czy naruszenie danych osobowych zostało zgłoszone do organu nadzorczego, administrator danych ma obowiązek dokumentowania naruszeń ochrony danych. W przypadku, gdy zgłoszenie nie zostało dokonane z powodu mało prawdopodobnego ryzyka naruszenia praw osób fizycznych, administrator nadal musi odnotować takie naruszenie w odpowiedniej dokumentacji, np. w rejestrze naruszeń ochrony danych. Dokumentacja ta jest niezbędna do późniejszej weryfikacji przez organ nadzorczy, aby upewnić się, że administrator spełnia swoje obowiązki wynikające z RODO.

Jakie informacje muszą znaleźć się w zgłoszeniu?

Zgodnie z artykułem 33 RODO, zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego musi zawierać szereg informacji. Należy podać:

1. **Opis charakteru naruszenia ochrony danych osobowych**, w tym wskazanie kategorii osób, których dane zostały naruszone, oraz kategorii danych, które zostały naruszone. Należy również podać przybliżoną liczbę osób, których dane zostały naruszone oraz liczbę danych osobowych, których dotyczy naruszenie,
2. **Dane kontaktowe inspektora ochrony danych lub innego punktu kontaktowego**, od którego można uzyskać więcej informacji w sprawie naruszenia. Administrator danych musi zapewnić dostępność do osoby lub zespołu odpowiedzialnego za ochronę danych, aby organ nadzorczy mógł uzyskać dodatkowe informacje na temat naruszenia,
3. **Opis możliwych konsekwencji naruszenia ochrony danych osobowych**. W tej części zgłoszenia administrator powinien określić, jakie skutki mogą wystąpić

w wyniku naruszenia ochrony danych, np. ryzyko nieautoryzowanego dostępu do danych, utrata kontroli nad danymi osobowymi, ewentualne straty finansowe czy negatywne skutki dla reputacji osoby, której dane dotyczą,

4. **Środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych**. Administrator powinien wskazać, jakie działania zostały podjęte, aby zminimalizować skutki naruszenia i zapobiec podobnym incydentom w przyszłości. Może to obejmować np. wymianę haseł, wzmocnienie zabezpieczeń systemu, czy też informowanie osób, których dane zostały naruszone.

Zgłoszenie naruszenia a sukcesywne uzupełnianie informacji

Jeżeli administrator nie jest w stanie zebrać wszystkich wymaganych informacji w momencie pierwszego zgłoszenia naruszenia ochrony danych osobowych, RODO przewiduje możliwość sukcesywnego uzupełniania zgłoszenia. Oznacza to, że administrator może początkowo zgłosić naruszenie bez wszystkich szczegółów, ale musi je uzupełniać bez zbędnej zwłoki, jak tylko pozyska brakujące dane. Takie podejście ma na celu umożliwienie szybkiego zgłoszenia naruszenia, nawet jeżeli wszystkie szczegóły nie są od razu dostępne.

Zgłoszenie naruszenia ochrony danych osobowych jest jednym z kluczowych obowiązków administratorów, który ma na celu zapewnienie ochrony praw osób fizycznych[14].

2.2. Art. 44 UDODO

Zgodnie z przepisami RODO, naruszenie ochrony danych osobowych to każde zdarzenie, które prowadzi do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub dostępu do danych osobowych, które są przesyłane, przechowywane lub w inny sposób przetwarzane. Warto dodać, że naruszenie może wynikać z nieprawidłowych działań człowieka, problemów z zabezpieczeniami technicznymi lub nawet z systemowymi błędami w organizacji.

Stąd też, w kontekście zgłaszania naruszenia ochrony danych osobowych do Prezesa Urzędu, należy reagować na wszelkie takie zdarzenia, które mogą mieć wpływ na bezpieczeństwo danych. Zgłoszenie takie jest wymagane tylko wtedy, gdy naruszenie wiąże się z ryzykiem naruszenia praw lub wolności osób fizycznych, czyli gdy może to prowadzić do istotnych konsekwencji dla osób, których dane zostały naruszone.

[14] E. Bielak-Jooma, W. Chomiczewski, tamże, str. 708-717.

Zgodnie z art. 44 ust. 1, administrator danych osobowych ma obowiązek zgłoszenia naruszenia ochrony danych do Prezesa UODO bez zbędnej zwłoki, nie później jednak niż w ciągu 72 godzin po stwierdzeniu naruszenia. To oznacza, że po wykryciu naruszenia, administrator musi w jak najkrótszym czasie poinformować odpowiednie organy, by te mogły podjąć odpowiednie środki zaradcze i zapobiec dalszym szkodom.

Należy pamiętać, że zgłoszenie naruszenia nie jest wymagane, jeśli po dokonaniu analizy ryzyka okaże się, że naruszenie nie ma wpływu na prawa i wolności osób fizycznych. Administrator musi przeprowadzić ocenę ryzyka, aby upewnić się, czy dane naruszenie ma potencjał, by stanowić zagrożenie dla osób, których dane zostały naruszone.

Zgłoszenie naruszenia w przypadku opóźnienia

Jeżeli administrator nie zgłosi naruszenia w wymaganym terminie 72 godzin, musi niezwłocznie wyjaśnić przyczyny tego opóźnienia oraz dostarczyć Prezesowi UODO uzasadnienie. Ważne jest, by w przypadku takiej sytuacji, administrator działał szybko i zgodnie z zasadami, by nie narażać praw osób, których dane zostały naruszone.

Obowiązki podmiotu przetwarzającego dane

Podmiot przetwarzający dane osobowe ma obowiązek niezwłocznego zgłoszenia stwierdzonego naruszenia administratorowi danych osobowych, w terminie nie później niż 48 godzin po jego wykryciu. Jest to istotne, ponieważ podmiot przetwarzający może mieć dostęp do danych, jednak to administrator ostatecznie ponosi odpowiedzialność za ich zabezpieczenie i zgłoszenie naruszenia[15].

Treść zgłoszenia naruszenia do UODO

Zgłoszenie naruszenia ochrony danych osobowych do Prezesa UODO musi zawierać:

1. **opis charakteru naruszenia:** zawierać powinien szczegóły dotyczące naruszenia, takie jak kategorie osób i danych, których to dotyczy, oraz liczbę osób i danych,
2. **dane kontaktowe:** imię i nazwisko inspektora ochrony danych lub punkt kontaktowy, do którego można się zwrócić po dodatkowe informacje,
3. **opis możliwych konsekwencji naruszenia:** należy wskazać potencjalne skutki naruszenia ochrony danych osobowych,
4. **podjęte środki zaradcze:** administrator musi opisać, jakie środki zostały podjęte w celu usunięcia naruszenia oraz jakie działania zostały podjęte w celu zminimalizowania skutków dla osób, których dane zostały naruszone.

[15] *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości. Komentarz*, red. A. Grzelak, M. Gumularz, str. 398-421.

Dokumentowanie przypadków naruszenia

Zgodnie z ustawą, administrator ma obowiązek dokumentować przypadki naruszenia ochrony danych osobowych. Powinien on stworzyć rejestr naruszeń, który zawierać będzie m.in. okoliczności, skutki oraz podjęte działania naprawcze. Dzięki temu dokumentowanie przypadków naruszenia umożliwia zarówno kontrolę przez Prezes Urzędu Ochrony Danych Osobowych, jak i weryfikację przestrzegania wymogów wynikających z przepisów prawa.

Zgodnie z art. 45 Ustawy o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, administrator danych osobowych ma obowiązek zawiadomienia osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, gdy takie naruszenie może wiązać się z wysokim ryzykiem naruszenia jej praw lub wolności.

Rozdział 3.
Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

3.1. Art. 34 RODO

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych jest obowiązkowe w przypadku, gdy naruszenie to może **spowodować wysokie ryzyko naruszenia jej praw lub wolności**. Wysokie ryzyko może dotyczyć takich sytuacji, jak:

1. utrata kontroli nad danymi osobowymi (np. kradzież danych w wyniku ataku hakerskiego),
2. możliwość wykorzystania danych osobowych w sposób, który mógłby prowadzić do oszustwa (np. dostęp do numeru konta bankowego, który umożliwia przelewy),
3. poważne zagrożenie dla prywatności (np. nieautoryzowany dostęp do wrażliwych danych zdrowotnych).

Warto podkreślić, że **zawiadomienie nie jest wymagane**, jeśli ryzyko naruszenia praw lub wolności osoby jest **mało prawdopodobne**. W takich sytuacjach, pomimo naruszenia ochrony danych, administrator nie musi informować osoby, której dane dotyczą, o zaistniałym incydencie.

Przykładem sytuacji, w której ryzyko naruszenia praw lub wolności osób jest mało prawdopodobne, może być przypadek, gdy administrator danych przechowuje dane w postaci zaszyfrowanej, co uniemożliwia dostęp do nich osobom nieuprawnionym. Nawet jeśli dane zostałyby skradzione, to brak dostępu do treści danych z powodu zastosowanego szyfrowania powoduje, że ryzyko ich wykorzystania jest minimalne.

Zawiadomienie musi być napisane w prostym i zrozumiałym języku

Zawiadomienie, które administrator danych wysyła do osoby, której dane dotyczą, musi być napisane **jasnym, prostym i zrozumiałym językiem**. Ma to na celu zapewnienie, że osoba, której dane dotyczą, łatwo zrozumie, w jaki sposób jej dane zostały naruszone i jakie kroki powinna podjąć, by chronić swoje prawa i wolności.

W praktyce oznacza to unikanie skomplikowanego języka prawniczego, który mógłby utrudnić zrozumienie sytuacji przez zwykłego odbiorcę. Zawiadomienie nie może zawierać zbyt wielu technicznych szczegółów dotyczących np. zastosowanych środków ochrony, chyba że jest to niezbędne do wyjaśnienia sytuacji.

Jeżeli doszło do naruszenia ochrony danych dotyczących hasła do konta użytkownika, zawiadomienie powinno jasno informować, że „Twoje hasło zostało skradzione w wyniku ataku hakerskiego. W celu ochrony swojego konta, prosimy o natychmiastową zmianę hasła."

Przypadki, kiedy zawiadomienie nie jest wymagane

Chociaż głównym obowiązkiem administratora jest zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych, to jednak przepisy art. 34 przewidują pewne wyjątki od tej zasady. Zawiadomienie **nie jest wymagane**, jeśli spełniony zostanie którykolwiek z poniższych warunków:

1. **Zastosowanie odpowiednich środków ochrony danych**: jeśli administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony danych, takie jak np. szyfrowanie, które uniemożliwia nieuprawnionym osobom dostęp do danych, wtedy naruszenie może nie powodować wysokiego ryzyka, a powiadomienie nie będzie konieczne.

   Przykład: jeśli dane osobowe przechowywane w bazie danych zostałyby wykradzione, ale zostały zaszyfrowane, co uniemożliwia ich odczytanie przez osobę nieuprawnioną, administrator nie ma obowiązku zawiadamiania osoby, której dane dotyczą.
2. **Środki eliminujące ryzyko**: jeśli po stwierdzeniu naruszenia administrator podejmie odpowiednie działania eliminujące ryzyko wysokiego naruszenia praw lub wolności podmiotów danych, również zawiadomienie nie jest wymagane.

   Przykład: administrator, po stwierdzeniu naruszenia ochrony danych, wprowadza dodatkowe zabezpieczenia, takie jak wzmocnienie systemów ochrony danych i audyt dostępu, które minimalizują ryzyko dalszych szkód.
3. **Niewspółmiernie duży wysiłek**: zawiadomienie nie jest wymagane, jeżeli wykonanie go wiązałoby się z niewspółmiernie dużym wysiłkiem, np. w przypadku, gdy administrator nie ma danych kontaktowych osób, których dane zostały naruszone, a zbieranie tych danych byłoby zbyt czasochłonne lub kosztowne. W takim przypadku administrator może zamiast indywidualnego zawiadomienia, opublikować ogólny komunikat.

   Przykład: jeśli administrator danych nie posiada aktualnych adresów e-mail dla wszystkich swoich użytkowników, ale ma dostęp do publicznych informacji (np. stron internetowych), może wydać ogólny komunikat na swojej stronie, informując użytkowników o zaistniałym naruszeniu.

Zawiadomienia o naruszeniu ochrony danych osobowych mogą przybrać różną formę, w zależności od sytuacji i charakteru naruszenia. Zdarza się, że organizacje

muszą informować o takich naruszeniach swoich użytkowników w przypadkach, kiedy dane są używane do nieautoryzowanych celów lub kiedy wyciekają szczególnie wrażliwe informacje.

Przykład: naruszenie ochrony danych w banku

Jeżeli bank wykryje, że dane logowania do konta klienta zostały wykradzione przez hakerów, klient powinien zostać natychmiast powiadomiony, gdyż istnieje wysokie ryzyko naruszenia jego praw, np. kradzieży pieniędzy. Zawiadomienie powinno zawierać informacje o tym, jak zmienić hasło i jakie dodatkowe środki bezpieczeństwa zostały wdrożone przez bank w celu ochrony konta.

Przykład: przypadek naruszenia danych u dostawcy usług internetowych

Dostawca usług internetowych, który zauważy, że dane klientów zostały nieautoryzowane skopiowane przez cyberprzestępców, będzie miał obowiązek powiadomienia swoich klientów, jeżeli naruszenie może prowadzić do wysokiego ryzyka kradzieży tożsamości lub oszustw związanych z danymi kontaktowymi użytkowników.

Zawiadomienie przez Urząd Ochrony Danych Osobowych

W przypadku gdy administrator nie zawiadomił osoby, której dane dotyczą, o naruszeniu, organ nadzorczy (np. Urząd Ochrony Danych Osobowych) może wymagać od administratora, aby ten poinformował daną osobę, jeśli naruszenie skutkuje wysokim ryzykiem. Organ może także stwierdzić, że w sytuacji spełnienia warunków wymienionych w art. 34 ust. 3 zawiadomienie nie jest wymagane.

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych jest kluczowym elementem zapewniającym ochronę jej praw i wolności. Zgodnie z RODO, zawiadomienie to jest wymagane w przypadkach, gdy naruszenie może powodować wysokie ryzyko dla praw osoby. W innych przypadkach, np. gdy ryzyko jest mało prawdopodobne lub gdy zastosowano odpowiednie zabezpieczenia, zawiadomienie nie jest konieczne. Ważne jest, aby informacja ta była prosta, zrozumiała i zawierała szczegóły dotyczące podjętych działań zaradczych. Zgodność z obowiązkami dotyczącymi zawiadomienia podmiotu danych o naruszeniu ochrony danych osobowych zapewnia ochronę tych danych i pozwala na szybszą reakcję ze strony osoby, której dane dotyczą, co jest kluczowe w procesie ochrony jej prywatności[16].

[16] E. Bielak-Jooma, W. Chomiczewski, tamże, str. 717-728.

3.2. Art. 45 UODO

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych ma miejsce, gdy naruszenie to może wiązać się z wysokim ryzykiem naruszenia jej praw lub wolności. Zgodnie z przepisem, powiadomienie nie jest wymagane w sytuacji, gdy naruszenie danych nie prowadzi do wysokiego ryzyka. W takim przypadku administrator danych nie ma obowiązku zawiadamiania osoby, której dane zostały naruszone, jeśli ryzyko związane z naruszeniem jest mało prawdopodobne. Przykładami mogą być drobne błędy w przetwarzaniu danych, które nie mają wpływu na prawa i wolności osoby fizycznej, takie jak pomyłki w danych kontaktowych, które nie powodują realnego ryzyka ich nadużycia.

Prosty i zrozumiały język w zawiadomieniu

Zawiadomienie o naruszeniu ochrony danych osobowych musi być sporządzone w sposób zrozumiały i przystępny. Administrator danych powinien zadbać, aby komunikat był napisany prostym językiem, który będzie jasny dla osoby, której dane dotyczą. Należy unikać używania skomplikowanego języka prawniczego lub technicznego, który mógłby utrudnić zrozumienie istoty naruszenia oraz działań podjętych w celu zaradzenia sytuacji. Na przykład, jeżeli doszło do wycieku danych osobowych, osoba powinna zostać poinformowana o tym w sposób klarowny, z wyjaśnieniem, jak może się zabezpieczyć, np. zmieniając hasła dostępu do swoich kont.

Przypadki, kiedy zawiadomienie nie jest wymagane

Zawiadomienie osoby, której dane dotyczą, nie jest wymagane, gdy spełniony jest jeden z poniższych warunków:

1. **zastosowanie odpowiednich środków ochrony:** jeśli administrator zastosował odpowiednie środki ochrony danych osobowych, takie jak szyfrowanie, które uniemożliwia dostęp do tych danych osobom nieuprawnionym, to naruszenie nie wymaga zawiadomienia osoby, której dane dotyczą. Przykładem może być szyfrowanie danych kart kredytowych, które sprawia, że nawet w przypadku ich wycieku, dostęp do tych danych jest niemożliwy bez odpowiedniego klucza,
2. **środki eliminujące ryzyko:** jeśli administrator podjął środki, które eliminują ryzyko naruszenia praw lub wolności osób, takich jak natychmiastowa zmiana haseł dostępu w przypadku ich wycieku, wtedy nie ma potrzeby informowania osoby o naruszeniu, ponieważ ryzyko zostało zniwelowane,
3. **niewspółmierny wysiłek:** jeżeli zawiadomienie osoby wymagałoby niewspółmiernie dużego wysiłku, na przykład, gdy administrator nie dysponuje odpowiednimi

danymi kontaktowymi osób, których dane zostały naruszone, wówczas może zamiast zawiadomienia wysłać publiczny komunikat.

Dokumentowanie naruszeń

Administrator musi prowadzić dokumentację dotyczącą wszelkich przypadków naruszeń ochrony danych osobowych. Rejestr naruszeń powinien zawierać informacje o okolicznościach naruszenia, jego skutkach oraz działaniach podjętych w celu naprawy sytuacji. Taka dokumentacja pozwala organom nadzorczym na weryfikację przestrzegania obowiązków przez administratora i zapewnia dodatkowy mechanizm ochrony przed ewentualnymi sankcjami.

Podsumowanie

Art. 45 ustawy o ochronie danych osobowych dotyczących zapobiegania przestępczości nakłada na administratorów obowiązek informowania osób, których dane zostały naruszone, o zaistniałej sytuacji, w szczególności w przypadku wysokiego ryzyka naruszenia ich praw lub wolności. Zawiadomienie musi być jasne i zrozumiałe, a sytuacje, w których nie jest wymagane, obejmują zastosowanie odpowiednich środków ochrony, eliminację ryzyka lub zbyt duży wysiłek związany z powiadomieniem[17].

[17] *Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, komentarz*, red. A. Grzelak, M. Wróblewski, str. 421-431.

Rozdział 4.
Metoda oceny wagi naruszenia wg Agencji Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA)

WN = KPD * PI + ON

WN – Waga Naruszenia

KPD – Kontekst Przetwarzania Danych: główny czynnik określający poziom krytyczności zestawu naruszonych danych, w określonym kontekście przetwarzania.

PI – Prawdopodobieństwo Identyfikacji: czynnik korygujący KPD, który może obniżyć wynik. Prawdopodobieństwo (łatwość) identyfikacji osoby na podstawie naruszonych danych dla osób, które uzyskały dostęp do nich.

ON – Okoliczności Naruszenia: czynnik, który odnosi się do okoliczności naruszenia, które wystąpiły lub nie w danym przypadku.

KONTEKST PRZETWARZANIA DANYCH
KPD = A + B

A – rodzaj i poziom wrażliwych danych

- Dane podstawowe = 1

Dane podstawowe to informacje odnoszące się m.in. do tożsamości (np. imię i nazwisko, nick internetowy, data urodzenia, imiona rodziców, numer PESEL), danych teleadresowych (adres e-mail, numer telefonu) lub danych korespondencyjnych (adres zamieszkania lub do korespondencji) osoby, której dane dotyczą.

- Dane dotyczące zachowań osoby = 2

Dane dotyczące zachowania to informacje odnoszące się m.in. do lokalizacji, pokonywania tras, preferencji, gustów lub upodobań osoby, której dane dotyczą.

- Dane finansowe = 3

Dane finansowe to dowolny rodzaj danych odnoszących się do finansów osoby, której dane dotyczą (np. dochody, transakcje finansowe, wyciągi bankowe, inwestycje,

numer kart kredytowych, faktury, itp.). Wskazana kategoria obejmuje także informacje dotyczące pomocy ze strony opieki społecznej, odnośnie do wsparcia materialnego.

- Dane szczególne = 4

Dane szczególnej kategorii to dane ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, dane genetyczne, biometryczne, dotyczące zdrowia, seksualności lub orientacji seksualnej albo dane dotyczące wyroków skazujących i naruszeń prawa.

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę

- Szeroki zakres danych/wolumen danych (+1)

Szeroki zakres danych należy rozpatrywać pod kątem ilości danych objętych naruszeniem, ale i czasem jego trwania. Przykładowo, taki charakter miałoby ujawnienie przez dostawcę usług internetowych danych na temat historii stron internetowych, które przeglądał użytkownik, w zakresie obejmującym okres jednego roku (a nie np. tygodnia). Jako inny przykład można wskazać ujawnienie przez bank pełnego wniosku kredytowego (a nie np. jednego z załączników).

- Charakter danych (+1/-1)

Szczególny charakter danych należy rozumieć jako czynnik wpływający na poziom ryzyka poprzez charakter i kontekst informacji, które uległy naruszeniu. Przykładowo, zagubienie zaświadczenia lekarskiego zawierającego wyłącznie informację o dobrym stanie zdrowia osoby, której dane dotyczą – pomimo ujawnienia danych szczególnej kategorii ryzyko nie będzie się zwielokrotniać, ponieważ zaistniałe zdarzenie nie wpływa na sytuację tej osoby.

- Specyfikacja podmiotu danych lub administratora (+1/-1)

Specyfika administratora danych odnosi się do jego profilu działalności, który może zwiększać ryzyko naruszenia praw i wolności osoby, której dane dotyczą. Przykładowo, ujawnienie danych na temat klientów apteki lub poradni psychiatrycznej niesie ze sobą wyższe ryzyko niż w przypadku klientów sklepu papierniczego. Specyfika osób, których dane dotyczą, odnosi się do ich cech, sytuacji życiowej lub potrzeb, które mogą zwiększać ryzyko naruszenia ich praw i wolności. Przykładowo, ujawnienie numerów telefonów parlamentarzystów lub pracowników ministerstwa niesie ze sobą wyższe ryzyko niż w przypadku numerów telefonów pracowników sklepu spożywczego.

- Możliwe negatywne skutki dla podmiotu danych (+1)

Naruszenie może powodować negatywne skutki dla osób, których dane dotyczą, np. kradzież tożsamości, szkodę finansową, szkodę wizerunkową, dyskryminację.

- Publiczna dostępność danych przed naruszeniem (-1)

Dostępność danych oznacza możliwość zapoznania się z nimi poprzez otwarte źródła informacji (np. KRS, CEIDG, Facebook).

- Nieważność danych (-1)

Aktualność danych to inaczej ich merytoryczna poprawność, a więc pewność, że są one zgodne ze stanem faktycznym. Przykładowo, lista adresów pocztowych, pod które nie można dostarczyć listów do wskazanych odbiorców, może świadczyć o nieaktualności danych na temat osób mających zamieszkiwać pod wskazanymi adresami.

Prawdopodobieństwo identyfikacji
PI

Prawdopodobieństwo Identyfikacji

Ważnym czynnikiem do uwzględnienia jest łatwość identyfikacji osoby. W zależności od okoliczności identyfikacja może być możliwa bezpośrednio w oparciu o dane osobowe, których dotyczyło naruszenie, bez konieczności zbierania dodatkowych informacji, lub dopasowanie danych osobowych do konkretnej osoby fizycznej może okazać się bardzo trudne, ale wciąż możliwe w konkretnych okolicznościach. Identyfikacja może być możliwa bezpośrednio lub pośrednio w oparciu o naruszone dane, ale może również zależeć od konkretnego kontekstu naruszenia i publicznej dostępności powiązanych danych osobowych.

Znikome = 0,25
Ograniczone = 0,5
Wysokie = 0,75
Maksymalne = 1

Okoliczności Naruszenia
ON = NP + NI + ND + IDS

NP – Naruszenie Poufności

Utrata poufności ma miejsce, gdy dostęp do danych uzyskują osoby lub podmioty, które nie są do tego uprawnione lub nie mają uzasadnionego celu, aby taki dostęp posiadać.

Dane ujawnione:

- znanym odbiorcom (+0,25)
- nieznanej liczbie odbiorców danych (+0,5)
- nie dotyczy (0)

NI – Naruszenie Integralności

Utrata integralności następuje, gdy oryginalne informacje zostaną zmienione, a przetwarzanie danych zmodyfikowanych w ten sposób może być szkodliwe dla osoby.

Dane zmienione:

- możliwe jest ich odzyskanie (+0,25)
- brak jest możliwości ich odzyskania (0,5)
- nie dotyczy (0)

ND – Naruszenie Dostępności

Utrata dostępności występuje, gdy nie można uzyskać dostępu do danych osobowych wtedy, gdy jest taka potrzeba. Może to być czasowe (dane można odzyskać dopiero po pewnym czasie) lub trwałe (dane nie mogą być odzyskane).

Niedostępność danych:

- czasowa (+0,25)
- pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)
- nie dotyczy (0)

IDS – Intencjonalne Działanie Sprawcy

Przypadki kradzieży i włamania, w celu wyrządzenie szkody osobom fizycznym (np. poprzez ujawnienie ich danych osobowych); przekazywanie danych osobowych stronom trzecim w celach zarobkowych (np. sprzedaż list danych osobowych).

- zidentyfikowano potencjalne działanie sprawcy (+0,5)
- nie dotyczy (0)[18]

[18] *Zalecenia w sprawie metodyki oceny powagi naruszeń danych osobowych.* Dokument roboczy, v1.0, Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji Clara Galan Manso, S. Górniak, grudzień 2013.

Ocena wagi naruszenia

Wynik	Waga naruszenia	Opis
WN< 2	**Niska**	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<= **WN**<3	**Średnia**	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=**WN**<4	**Wysoka**	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=**WN**	**Bardzo wysoka**	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

Rozdział 5.
Dokumentowanie naruszeń ochrony danych osobowych na wybranym przykładzie

Aby lepiej zobrazować sposób obsługi naruszenia ochrony danych, wskazuje się poniższy przykład, który posłuży jako podstawa do opracowania w dalszej części odpowiedniej praktycznej dokumentacji.

W dniu 01.01.2024 roku policjant Komisariatu Policji I w XYZ zagubił bloczek pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA 0000001-AA0000025 zawierający dane 5 osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.

Oceny wagi naruszenia metodą ENISA

Zakres danych: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania, własnoręczny podpis

KPD= A + B = 1 + 4 = **5**

A – rodzaj i poziom wrażliwych danych

Dane podstawowe = 1
Dane dotyczące zachowań osoby = 2
Dane finansowe = 3
Dane szczególne = 4

B – kontekst przetwarzania, który może podwyższyć lub obniżyć wycenę

Szeroki zakres danych/wolumen danych (+1)
Charakter danych (+1/-1)
Specyfikacja podmiotu danych lub administratora (+1/-1)
Możliwe negatywne skutki dla podmiotu danych (+1)
Publiczna dostępność danych przed naruszeniem (-1)
Nieważność danych (-1)

PI = 0,5

Prawdopodobieństwo Identyfikacji

Znikome = 0,25

Ograniczone = 0,5
Wysokie = 0,75
Maksymalne = 1

ON = NP + NI + ND + IDS = 0,5 + 0 + 0 + 0 = 0,5

NP – Naruszenie Poufności

Dane ujawnione:

- znanym odbiorcom (+0,25)
- nieznanej liczbie odbiorców danych (+0,5)
- nie dotyczy (0)

NI – Naruszenie Integralności

Dane zmienione:

- możliwe jest ich odzyskanie (+0,25)
- brak jest możliwości ich odzyskania (0,5)
- nie dotyczy (0)

ND – Naruszenie Dostępności

Niedostępność danych:

- czasowa (+0,25)
- pełna i brak możliwości ich odzyskania przez administratora lub podmiot danych (+0,5)
- nie dotyczy (0)

IDS – Intencjonalne Działanie Sprawcy

- zidentyfikowano potencjalne działanie sprawcy (+0,5)
- nie dotyczy (0)

WN = KPD * PI + ON

WN = 5 * 0,5 + 0,5

WN = 3

Ocena wagi naruszenia – WYSOKA

Wynik	Waga naruszenia	Opis
~~**WN**< 2~~	~~**Niska**~~	Osoby nie zostaną dotknięte naruszeniem lub wywoła ono drobne niedogodności
2<= **WN**<3	~~**Średnia**~~	Osoby mogą napotkać niedogodności, które są możliwe do pokonania
3<=**WN**<4	**Wysoka**	Mogą wystąpić konsekwencje możliwe do pokonania, ale z poważnymi skutkami
4<=**WN**	~~**Bardzo wysoka**~~	Mogą wystąpić znaczące, nawet nieodwracalne konsekwencje

5.1. Informacja o przypadku naruszenia ochrony danych osobowych – KWP

……
(miejscowość, data)

l. dz. ……

Pan *stopień, imię i nazwisko*
Komendant Wojewódzki Policji
w XYZ

Za pośrednictwem
Naczelnika Wydziału Bezpieczeństwa Informacji
KWP w XYZ

INFORMACJA O PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA Jak ustalono bloczek ten posiadał wystawionych 5 blankietów oznaczonych nr 0000001-0000005 zawierające dane 5 osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.

Wobec powyższego wykonano kalkulację wagi naruszeń ochrony danych osobowych, która wykazała wysoką wagę naruszenia. Przedmiotowe fakt naruszenia danych osobowych zgłoszono do Urzędu Ochrony Danych Osobowych zs. Warszawa, ul. Stawki 2.

Mając powyższe na uwadze przedmiotowa sprawa została objęta nadzorem Komendanta Miejskiego Policji w XYZ celem wyjaśnienia okoliczności incydentu. Poinformowano również o zdarzeniu Inspektora Ochrony Danych KWP w XYZ.

Ponadto informuję, iż zrealizowano ustawowy obowiązek zawiadomienia osób o możliwych konsekwencjach oraz skutkach naruszenia. Poinformowano listownie osobę, której dane dotyczą o naruszeniu jej danych osobowych, pouczono ją o możliwych konsekwencjach, a także zaproponowano środki i działania w celu zminimalizowania negatywnych skutków naruszenia ochrony danych osobowych. Ponadto osoba, której dane dotyczą została poinformowana o prawie do złożenia skargi do Prezesa UODO.

Zgodnie z pismem Nti-345/21 dyrektora Biura Bezpieczeństwa Informacji KGP z dnia 15.12.2021 roku o przedmiotowym zdarzeniu zostanie również poinformowane Biuro Nadzoru Wewnętrznego MSWIA oraz Biuro Informacji Komendy Głównej Policji w Warszawie.

5.2. Zawiadomienie osoby, której dane dotyczą o naruszeniu ochrony danych osobowych

……
(miejscowość, data)

l. dz. ……

Pan
Imię i nazwisko
adres

ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

Realizując obowiązek wynikający z art. 34 ust 1 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), przekazujemy informację o zaistniałym naruszeniu ochrony Pana danych osobowych. Szczegółowe informacje związane z naruszeniem zostały wskazane poniżej.

Charakter oraz okoliczności naruszenia:

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA nr 0000001-0000025. Jak ustalono bloczek ten posiadał pokwitowanie oznaczone serią AAA nr 0000001 zawierającym Pana dane osobowe w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz Pana własnoręczny podpis.

W związku powyższym informuję, że Pana dane osobowe mogą zostać wykorzystane w następujący sposób np. do:

– podszycia się pod Pana w mediach społecznościowych;
– założenia konta internetowego;
– wykorzystania Pana danych do zarejestrowania karty telefonicznej typu pre-paid, co może posłużyć do celów przestępczych;
– uzyskania przez osoby trzecie korzyści finansowych (np. kredytów w instytucjach poza bankowych);
– uzyskania dostępu do systemów rejestracji świadczeń opieki zdrowotnej (np. ujawnienia informacji o stanie zdrowia – ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie, potwierdzając swoja tożsamość za pomocą nr PESEL);
– korzystania z praw obywatelskich (np. przy głosowaniu nad środkami budżetu obywatelskiego – uniemożliwiłoby to skorzystanie z przysługujących Panu praw);
– podjęcia próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia (co może doprowadzić do negatywnych konsekwencji w postaci problemów związanych z odpowiedzialnością za dokonanie takiego czynu);
– podjęcia próby zawarcia umów cywilno-prawnych;
– naruszenia Pana dobra osobistego w postaci prawa do prywatności;
– ujawnienia czynności policyjnych wobec Pana;
– kradzieży lub sfałszowania Pana tożsamości;
– wykorzystania Pana danych do ukrycia tożsamości osoby trzeciej, np. przy otrzymywaniu mandatów.

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy, aby Pan:

1) założył konto w systemie informacji kredytowej lub gospodarczej w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym wykorzystaniem, a także sprawdził dotychczasową historię kredytową – np. poprzez założenie konta w:
   - Biurze Informacji Kredytowej (strona https://www.bik.pl) oraz aktywowanie funkcji alerty BIK, która poinformuje SMS-em o próbie uzyskania kredytu
   - Biurze Informacji Gospodarczej Info Monitor S.A (strona https://big.pl)
   - Krajowym Rejestrze Długów (strona https://krd.pl), który na stronie www.konsument.krd.pl umożliwia wszystkim konsumentom bezpłatne założenie konta.

   Dzięki temu można sprawdzić czy jakiś podmiot złożył zapytanie dotyczące Pana osoby oraz jakie informacje zostały udzielone. Strona wprowadza możliwość powiadomienia SMS-em lub e-mailem w sytuacji, gdy ktoś spyta o historię kredytową

bez Pańskiego pozwolenia. Daje to możliwość szybkiej reakcji – skontaktowania się z firmą, która pobrała raport, bądź z Policją,

2) zachował ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu;
3) dokonał samodzielnego zgłoszenia faktu naruszenia ochrony danych osobowych właściwym organom w celu zapobieżenia tzw. „kradzieży tożsamości";
4) rozważył zastrzeżenie danych w banku;
5) rozważył zastrzeżenie dowodu osobistego;
6) rozważył zastrzeżenie nr PESEL np. aktywowanie usługi Bezpieczny PESEL;
7) rozważył wymianę dowodu osobistego/prawa jazdy;
8) ignorował nieoczekiwane wiadomości, w szczególności namawiające do podjęcia dodatkowego działania, jak odesłanie wiadomości SMS lub zrobienie przelewu.

Ma Pan prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki 2) w tym zakresie na działanie administratora danych osobowych.

Jeśli dowie się Pan o wykorzystaniu Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie nam tej informacji.

Więcej informacji:

Jeżeli ma Pan jakiekolwiek pytania lub chciałby nam Pan przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z Inspektorem Ochrony Danych w Komendzie Miejskiej Policji w XYZ ul. Główna 19, 40-018, dane kontaktowe IOD – Jan Kowalski, adres e-mail jan.kowalski@ka.policja.gov.pl, 47 800 00 00

.....

(data i podpis Administratora)

5.3.Informacja o przypadku naruszenia ochrony danych osobowych – BBI KGP

……
(miejscowość, data)

l. dz. ……

Dyrektor Biura Bezpieczeństwa Informacji
Komendy Głównej Policji

INFORMACJA O PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Realizując obowiązek wynikający z pisma Nti-3451/21 z dnia 15.12.2021 r. Dyrektora Biura Bezpieczeństwa Informacji KGP, informuję o przypadku naruszenia ochrony danych osobowych.

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA Jak ustalono bloczek ten posiadał wystawionych 5 blankietów oznaczonych nr 0000001-0000005 zawierający dane pięciu osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.

Przeprowadzono kalkulację wagi naruszeń ochrony danych osobowych, która wykazała wysoką wagę naruszenia. W związku z tym zgłoszono ten incydent naruszenia danych osobowych do Urzędu Ochrony Danych Osobowych zs. Warszawa, ul. Stawki 2.

W związku z powyższym, sprawa została objęta nadzorem Komendanta Miejskiego Policji w XYZ celem wyjaśnienia okoliczności incydentu. Poinformowano również o tym zdarzeniu Komendanta Wojewódzkiego Policji w XYZ za pośrednictwem Inspektora Ochrony Danych KWP w XYZ.

Jednocześnie informuję, iż zrealizowano ustawowy obowiązek zawiadomienia o możliwych konsekwencjach oraz skutkach naruszenia. Poinformowano listownie osoby, których dane dotyczą o naruszeniu ich danych osobowych, pouczono o możliwych konsekwencjach, a także zaproponowano środki i działania w celu zminimalizowania negatywnych skutków naruszenia ochrony danych osobowych. Ponadto osoba, której dane dotyczą została poinformowana o prawie złożenia skargi do Prezesa UODO.

5.4.Informacja o przypadku naruszenia ochrony danych osobowych – INW BNW

……
(miejscowość, data)

l. dz. ……

Pan Inspektor Nadzoru Wewnętrznego
Biuro Nadzoru Wewnętrznego
MSWiA w Warszawie

INFORMACJA O PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Realizując obowiązek wynikający z pisma Nti-3451/21 z dnia 15.12.2021 r. Dyrektora Biura Bezpieczeństwa Informacji KGP, informuję o przypadku naruszenia ochrony danych osobowych.

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA numer 0000001-0000025. Jak ustalono bloczek ten posiadał wystawiony 5 blankietów oznaczonych nr 0000001-0000005 zawierających dane 5 osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.

Przeprowadzono kalkulację wagi naruszeń ochrony danych osobowych, która wykazała wysoką wagę naruszenia. W związku z tym zgłoszono ten incydent naruszenia danych osobowych do Urzędu Ochrony Danych Osobowych zs. Warszawa, ul. Stawki 2.

W związku z powyższym sprawa została objęta nadzorem Komendanta Miejskiego Policji w XYZ celem wyjaśnienia okoliczności incydentu. Poinformowano również o tym zdarzeniu Komendanta Wojewódzkiego Policji w XYZ za pośrednictwem Inspektora Ochrony Danych KWP w XYZ.

Jednocześnie informuję, iż zrealizowano ustawowy obowiązek zawiadomienia o możliwych konsekwencjach oraz skutkach naruszenia. Poinformowano listownie osoby, których dane dotyczą o naruszeniu ich danych osobowych, pouczono o możliwych konsekwencjach, a także zaproponowano im środki i działania w celu zminimalizowania negatywnych skutków naruszenia ochrony danych osobowych. Ponadto osoby, których dane dotyczą zostały poinformowane o prawie złożenia skargi do Prezesa UODO. 5.5. Formularz zgłoszenia naruszenia danych osobowych

5.5. Formularz zgłoszenia naruszenia ochrony danych UODO – zgłoszenie naruszenia ochrony danych osobowych[19]

1. Typ zgłoszenia

Wskaż, czy zgłaszasz naruszenie ochrony danych osobowych mające charakter jednorazowego zdarzenia (np. zgubienie, kradzież nośnika danych, przypadkowe wysłanie danych osobie nieuprawnionej), czy przygotowujesz wstępne zgłoszenie, które uzupełnisz później, lub czy uzupełniasz lub zmieniasz wcześniejsze zgłoszenie.

Podaj swoją sygnaturę sprawy (opcjonalnie) (np. sygnatura w Twoim wewnętrznym rejestrze naruszeń)	IOD.01/24

☑ Zgłoszenie kompletne/jednorazowe	☐ Zgłoszenie wstępne	☐ Zgłoszenie uzupełniające/zmieniające
	Podaj przybliżoną datę uzupełnienia zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę.	Podaj datę poprzedniego zgłoszenia (opcjonalnie) Kliknij tutaj, aby wprowadzić datę. Podaj sygnaturę sprawy UODO Kliknij tutaj, aby wprowadzić datę.

2. Podmiot zgłaszający

2A. Dane administratora danych

Pełna nazwa administratora	Komendant Miejski Policji w XYZ				
REGON (opcjonalnie)	Podaj numer.	NIP (opcjonalnie)	Podaj numer.	KRS (opcjonalnie)	Podaj numer.
Sektor (opcjonalnie)	Administracja publiczna	Dla sektora prywatnego: Wpisz nazwę sektora			

2B. Adres siedziby administratora danych

Ulica	Główna	Numer domu	19	Numer lokalu	Podaj numer
Miejscowość	XYZ	Kod pocztowy	40-018		
Gmina	.....	Powiat	.....		
Województwo	śląskie	Państwo	Polska		

2C. Osoby uprawnione do reprezentowania administratora

1.	Imię i nazwisko	Jan Nowak	Stanowisko	Komendant Miejski Policji w XYZ
2.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
3.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
4.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.
5.	Imię i nazwisko	Kliknij tutaj, aby wprowadzić tekst.	Stanowisko	Kliknij tutaj, aby wprowadzić tekst.

2D. Pełnomocnik

☐Wniosek wypełniany przez pełnomocnika(opcjonalnie)

Jeśli zgłoszenie przesyłane jest w formie elektronicznej, należy załączyć pełnomocnictwo **udzielone w formie elektronicznej** oraz dowód uiszczenia opłaty skarbowej

2E. Inspektor ochrony danych

Imię i nazwisko	Jan Kowalski	Numer telefonu	47-800 00 00		jan.kowalski@ka.policja.gov.pl

☐Inspektor nie został wyznaczony

[19] Wzór formularza dostępny na stronie: https://uodo.gov.pl/pl/492/2278 (dostęp 28.11.2024 r.)

Jeśli inspektor nie został wyznaczony podaj dane innego punktu kontaktowego, od którego można uzyskać więcej informacji o naruszeniu.

Kliknij tutaj, aby wprowadzić tekst.

2F. Inne podmioty uczestniczące w przetwarzaniu danych, których dotyczy naruszenie (opcjonalnie)

Podaj nazwy podmiotów, dane kontaktowe i wyjaśnij ich rolę w procesie przetwarzania, którego dotyczy naruszenie (np. podmiot przetwarzający, współadministratora, operator pocztowy itp.)

1.	Nazwa i dane kontaktowe		Rola	
2.	Nazwa i dane kontaktowe		Rola	
3.	Nazwa i dane kontaktowe		Rola	
4.	Nazwa i dane kontaktowe		Rola	

3. Czas naruszenia

3A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia Wskaż, kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	03.01.2024

Sposób stwierdzenia naruszenia Np. zgłoszenie osoby, której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa

Notatka służbowa

Data powiadomienia przez podmiot przetwarzający (opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	.....

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu Pole obowiązkowe, jeśli czas od momentu stwierdzenia naruszenia do czasu wypełniania formularza jest dłuższy niż 72h

Nie dotyczy

3B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	01.01.2024, godz.10:00
Data i czas zakończenia naruszenia (opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.	nadal

4. Charakter naruszenia

4A. Opisz szczegółowo na czym polegało naruszenie

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA numer 0000001-0000025. Jak ustalono bloczek ten posiadał wystawionych 5 blankietów oznaczonych nr 0000001-0000005 zawierających dane 5 osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.

4B. Na czym polegało naruszenie?

- ☐ Zgubienie lub kradzież nośnika/urządzenia
- **x** Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji
- ☐ Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy
- ☐ Nieuprawnione uzyskanie dostępu do informacji
- ☐ Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń
- ☐ Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych
- ☐ Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)
- ☐ Nieprawidłowa anonimizacja danych osobowych w dokumencie
- ☐ Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
- ☐ Niezamierzona publikacja
- ☐ Dane osobowe wysłane do niewłaściwego odbiorcy
- ☐ Ujawnienie danych niewłaściwej osoby
- ☐ Ustne ujawnienie danych osobowych

4C. Przyczyna naruszenia

- **x** Wewnętrzne działanie niezamierzone
- ☐ Wewnętrzne działanie zamierzone
- ☐ Zewnętrzne działanie niezamierzone
- ☐ Zewnętrzne działanie zamierzone

4D. Charakter

- **x** Naruszenie poufności danych
  Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych
- ☐ Naruszenie integralności danych
  Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania
- ☐ Naruszenie dostępności danych
  Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

4E. Dzieci

- ☐ Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
  (opcjonalnie)

5. Liczba osób i wpisów

Przybliżona liczba osób, których mogło dotyczyć naruszenie
Pięć osób

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie
Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów (np. jednej osobie można przypisać kilka wykonanych transakcji)

6. Kategorie danych osobowych

UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.

6A. Dane podstawowe

- [x] Nazwiska i imiona
- [x] Imiona rodziców
- [x] Data urodzenia
- [ ] Numer rachunku bankowego
- [x] Adres zamieszkania lub pobytu
- [x] Numer ewidencyjny PESEL
- [ ] Adres e-mail
- [ ] Nazwa użytkownika i/lub hasło
- [ ] Dane dotyczące zarobków i/lub posiadanego majątku
- [ ] Nazwisko rodowe matki
- [x] Seria i numer dowodu osobistego
- [ ] Numer telefonu
- [ ] Wizerunek
- [x] Inne, wskaż jakie:

własnoręczny podpis

6B. Dane szczególnej kategorii

- [ ] Dane o pochodzeniu rasowym lub etnicznym
- [ ] Dane o poglądach politycznych
- [ ] Dane o przekonaniach religijnych lub światopoglądowych
- [ ] Dane o przynależności do związków zawodowych
- [ ] Dane dotyczące seksualności lub orientacji seksualnej
- [ ] Dane dotyczące zdrowia
- [ ] Dane genetyczne
- [ ] Dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej

6C. Dane, o których mowa w art. 10 RODO

- [ ] Dane dotyczące wyroków skazujących
- [ ] Dane dotyczące czynów zabronionych
- [x] Inne

132 ust. 1 pkt 1 lit. a, c prawo o ruchu drogowym

7. Kategorie osób

- [ ] Pracownicy
- [ ] Użytkownicy
- [ ] Subskrybenci
- [ ] Studenci
- [ ] Uczniowie
- [ ] Służby mundurowe (np. wojsko, policja)
- [ ] Klienci (obecni i potencjalni)
- [ ] Klienci podmiotów publicznych
- [ ] Pacjenci
- [ ] Dzieci
- [ ] Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.)

Szczegółowy opis kategorii osób, których dotyczy naruszenie: Opisz np. kogo i w jakim przedziale czasowym dotyczy naruszenie **W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.**

Zawiadomiono osoby, której dane dotyczą

8. Możliwe konsekwencje

8A. Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą

- [x] Utrata kontroli nad własnymi danymi osobowymi
- [ ] Ograniczenie możliwości realizowania praw z art. 15-22 RODO
- [ ] Ograniczenie możliwości realizowania praw
- [ ] Dyskryminacja
- [x] Kradzież lub sfałszowanie tożsamości
- [x] Strata finansowa
- [ ] Naruszenie dobrego imienia
- [ ] Utrata poufności danych osobowych chronionych tajemnicą zawodową
- [ ] Nieuprawnione odwrócenie pseudonimizacji
- [x] Inne

Opisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:

podjęcia próby zawarcia umów cywilno-prawnych, ujawnienia czynności policyjnych wobec osób

8B. Czy wystąpiło wysokie ryzyko naruszenia praw lub wolności osób fizycznych?

(•) Tak ( ) Nie

Uzasadnienie

Wysokie ryzyko ustalono w oparciu o przeprowadzoną ocenę ryzyka wg. kalkulatora wagi naruszeń metodą ENISA

9. Środki bezpieczeństwa i środki zaradcze

9A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa dotychczas stosowanych

W celu zapewnienia bezpieczeństwa ochrony danych osobowych w KMP w XYZ wdrożona jest m.in. decyzja Komendanta Miejskiego Policji w XYZ z dnia 01.01.2019 roku w sprawie wprowadzenia „Polityki bezpieczeństwa xxxxxxxxxxxx".

9B. Środki bezpieczeństwa zastosowane lub proponowane w celu zminimalizowana ryzyka ponownego wystąpienia naruszenia

Komendant Miejski Policji w XYZ polecił wdrożenie czynności wyjaśniających w tej sprawie; przedmiotowe zdarzenie zostanie omówione na najbliższej doprawie kadry kierowniczej KMP w XYZ celem wzmocnienia nadzoru w tym zakresie; polecił ponownie przeszkolić w zakresie ochrony danych osobowych funkcjonariusza – sprawcę przedmiotowego incydentu,

9C. Środki zastosowane lub proponowane celu zaradzenia naruszeniu i zminimalizowania negatywnych skutków dla osób, których dane dotyczą

Wysłano osobom, których dane dotyczą zawiadomienie o możliwych konsekwencjach i skutkach naruszenia. Poinformowano listownie osoby, których dane dotyczą o naruszeniu ich danych osobowych, pouczono je o możliwych konsekwencjach, a także zaproponowano im środki działania w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych osobowych. Ponadto osoby te zostały poinformowane o prawie do złożenia skargi do Prezesa UODO

10. Zawiadamianie osób, których dane dotyczą

Czy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu?

(•) Tak

( ) Nie, ale zostaną zawiadomione

Pamiętaj, że po zawiadomieniu osób, należy przesłać treść zawiadomienia do UODO.

( ) Nie, nie zostaną zawiadomione

( ) Nie oceniłem jeszcze

Jeśli jeszcze nie oceniłeś, czy zamierzasz zawiadomić osoby, których dane dotyczą, pamiętaj, że po podjęciu takiej decyzji będziesz musiał złożyć zgłoszenie uzupełniające.

Czy indywidualnie?

(•) Tak

( ) Nie, gdyż indywidualne zawiadomienie każdej osoby, której dane dotyczą wymagałoby niewspółmiernie dużego wysiłku. W związku z tym został wydany publiczny komunikat lub zastosowano podobny środek, za pomocą którego osoby, których dane dotyczą, zostały poinformowane w równie skuteczny sposób.

Wskaż datę, kiedy osoby, których dane dotyczą, zostały zawiadomione o naruszeniu

.....

Wskaż datę, kiedy zamierzasz zawiadomić osoby, których dane dotyczą, o naruszeniu

.....

☐ Nie znam jeszcze daty, kiedy zamierzam powiadomić osoby, których dane dotyczą

Liczba zawiadomionych osób, których dane dotyczą

.....

Powód niezawiadomienia osób, których dane dotyczą:

( ) Przed naruszeniem wdrożono odpowiednie techniczne i organizacyjne środki ochrony (wskazane w pkt. 9A formularza) i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, anonimizacja czy pseudonimizacja uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych.

( ) Po naruszeniu zastosowano środki (wskazane w pkt. 9C formularza) eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą.

( ) Brak wysokiego ryzyka naruszenia praw lub wolności osób fizycznych (uzasadnienie w pkt. 8B formularza).

Środki komunikacji wykorzystane do zawiadomienia osoby, której dane dotyczą

ZAWIADOMIENIE LISTOWNE

Umieść zanonimizowaną treść zawiadomienia, którą przesłałeś bądź zamierzasz przesłać do osób, których dane dotyczą.

Pamiętaj, że zawiadomienie powinno:

- opisywać jasnym i prostym językiem charakter naruszenia ochrony danych osobowych,
- zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
- opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
- opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych.

Realizując obowiązek wynikający z art. 34 ust 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 216/679 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), przekazujemy informację o zaistniałym naruszeniu ochrony Pana danych osobowych.

Szczegółowe informacje związane z naruszeniem zostały wskazane poniżej.

Charakter oraz okoliczności naruszenia:

W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA numer 0000001-0000025 Jak ustalono bloczek ten posiadał wystawionych 5 blankietów oznaczonych nr 0000001 zawierający Pana dane w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz własnoręczny Pana podpis.

W związku powyższym informuję, iż Pana dane osobowe mogą zostać wykorzystane w następujący sposób np. do:

- podszycia się pod Pana w mediach społecznościowych;
- założenia konta internetowego;
- wykorzystania Pana danych do zarejestrowania karty telefonicznej typu pre-paid, co może posłużyć do celów przestępczych;
- uzyskania przez osoby trzecie korzyści finansowych (np. kredytów w instytucjach poza bankowych);
- uzyskania dostępu do systemów rejestracji świadczeń opieki zdrowotnej (np. ujawnienia informacji o stanie zdrowia – ponieważ często dostęp do systemów rejestracji pacjenta można uzyskać telefonicznie, potwierdzając swoja tożsamość za pomocą nr PESEL);
- korzystania z praw obywatelskich (np. przy głosowaniu nad środkami budżetu obywatelskiego – uniemożliwiłoby to skorzystanie z przysługujących Panu praw);
- podjęcia próby wyłudzenia ubezpieczenia lub środków z ubezpieczenia (co może doprowadzić do negatywnych konsekwencji w postaci problemów związanych z odpowiedzialnością za dokonanie takiego czynu);
- podjęcia próby zawarcia umów cywilno-prawnych;
- naruszenia Pana dobra osobistego w postaci prawa do prywatności;
- ujawnienia czynności policyjnych wobec Pana;
- kradzieży lub sfałszowania Pana tożsamości;
- wykorzystania Pana danych do ukrycia tożsamości osoby trzeciej, np. przy otrzymywaniu mandatów.

W celu zminimalizowania ewentualnych negatywnych skutków naruszenia zalecamy, aby Pan:

a. założył konto w systemie informacji kredytowej lub gospodarczej w celu dodatkowego zabezpieczenia swoich danych przed nieuprawnionym

wykorzystaniem, a także sprawdził dotychczasową historię kredytową – np. poprzez założenie konta w: • Biurze Informacji Kredytowej (strona https://www.bik.pl) oraz aktywowanie funkcji alerty BIK, która poinformuje SMS-em o próbie uzyskania kredytu • Biurze Informacji Gospodarczej Info Monitor S.A (strona https://big.pl) • Krajowym Rejestrze Długów (strona https://krd.pl), który na stronie www.konsument.krd.pl umożliwia wszystkim konsumentom bezpłatne założenie konta. Dzięki temu można sprawdzić czy jakiś podmiot złożył zapytanie dotyczące Pana osoby oraz jakie informacje zostały udzielone. Strona wprowadza możliwość powiadomienia SMS-em lub e-mailem w sytuacji, gdy ktoś spyta o historię kredytową bez Pańskiego pozwolenia. Daje to możliwość szybkiej reakcji – skontaktowania się z firmą, która pobrała raport, bądź z Policją, b. zachował ostrożność przy podawaniu danych osobowych innym osobom, zwłaszcza za pośrednictwem Internetu czy telefonu; c. dokonał samodzielnego zgłoszenia faktu naruszenia ochrony danych osobowych właściwym organom w celu zapobieżenia tzw. "kradzieży tożsamości"; d. rozważył zastrzeżenie danych w banku; e. rozważył zastrzeżenie dowodu osobistego; f. rozważył zastrzeżenie numeru PESEL np. poprzez aktywowanie usługi Bezpieczny PESEL; g. rozważył wymianę dowodu osobistego/prawa jazdy; h. ignorował nieoczekiwane wiadomości, w szczególności namawiające do podjęcia dodatkowego działania, jak odesłanie wiadomości SMS lub zrobienie przelewu. Ma Pan prawo złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych (00-193 Warszawa, ul. Stawki nr 2) w tym zakresie na działanie administratora danych osobowych. Jeśli dowie się Pan o wykorzystaniu Pana danych przez osobę nieuprawnioną, prosimy o jak najszybsze przekazanie nam tej informacji. Więcej informacji: Jeżeli ma Pan jakiekolwiek pytania lub chciałby nam Pan przekazać dodatkowe informacje w związku z zaistniałym zdarzeniem, prosimy o kontakt z Inspektorem Ochrony Danych w Komendzie Miejskiej Policji w XYZ adres e-mail: jan.kowalski@ka.policja.gov.pl, numer telefonu 47800 00 00		

11. Przetwarzanie transgraniczne i inne powiadomienie

☐ Naruszenie ma charakter transgraniczny

Zaznacz kraje Europejskiego Obszaru Gospodarczego, których dotyczy naruszenie:

☐ Austria	☐ Belgia	☐ Bułgaria	☐ Chorwacja
☐ Cypr	☐ Czechy	☐ Dania	☐ Estonia
☐ Finlandia	☐ Francja	☐ Grecja	☐ Hiszpania
☐ Holandia	☐ Irlandia	☐ Islandia	☐ Liechtenstein
☐ Litwa	☐ Luksemburg	☐ Łotwa	☐ Malta
☐ Niemcy	☐ Norwegia	☐ Portugalia	☐ Rumunia
☐ Słowacja	☐ Słowenia	☐ Szwecja	☐ Węgry
☐ Wielka Brytania	☐ Włochy		

Naruszenie zostało lub zostanie zgłoszone innemu organowi ochrony danych osobowych (opcjonalnie)

Wymień inne organy nadzorcze ochrony danych osobowych, którym naruszenie zostało lub zostanie zgłoszone

x Naruszenie zostało lub zostanie zgłoszone innemu organowi nadzorczemu z powodu innych zobowiązań prawnych (opcjonalnie)

Np. obowiązek zgłoszenia incydentu wynikający z ustawy o krajowym systemie cyberbezpieczeństwa. Wymień inne organy, którym naruszenie zostało lub zostanie zgłoszone z powodu innych zobowiązań prawnych.

1) Komendant Wojewódzki Policji w XYZ 2) Dyrektor Biura Bezpieczeństwa Informacji Komendy Głównej Policji 3) Inspektor Nadzoru Wewnętrznego MSWIA.

_____

Data, miejscowość
(dla zgłoszenia w formie papierowej)

_____

Podpis osoby lub osób upoważnionych do reprezentowania administratora
(dla zgłoszenia w formie papierowej)

Lp.	Informacje o wystąpieniu zdarzenia i stwierdzeniu naruszenia			Okoliczności naruszenia				Skutki naruszenia
	Data zdarzenia	Data i źródło uzyskania informacji	Data i godzina stwierdzenia naruszenia	Charakter naruszenia	Kategorie osób	Liczba osób	Kategoria i liczba wpisów	Opis konsekwencji naruszenia
1.	01.01.2024	01.01.2024 notatka służbowa	03.01.2024 10:00	W dniu 01.01.2024 roku Komendant Miejski Policji w XYZ poinformowany został o fakcie zdarzenia, które dotyczyło naruszenia bezpieczeństwa danych osobowych będącego rezultatem zagubienia przez funkcjonariusza Komisariatu Policji I w XYZ bloczka pokwitowań zatrzymanych dokumentów dowodów rejestracyjnych seria AAA numer 0000001-0000025. Jak ustalono bloczek ten posiadał wystawionych 5 blankietów oznaczonych nr 0000001-0000005 zawierających dane 5 osób w następującym zakresie: imię i nazwisko, imiona rodziców, numer PESEL, numer dowodu osobistego, adres zamieszkania oraz podpis.	Osoby wobec których policjanci podejmowali czynności	5	Dane podstawowe, 7	Utrata kontroli nad własnymi danymi osobowymi, kradzież lub sfałszowanie tożsamości, strata finansowa, inne, podjęcie próby zawarcia umów cywilno-prawnych, ujawnienie czynności policyjnych wobec osób

Środki naprawcze i zaradcze			Zgłoszenie naruszenia do Prezesa Urzędu			Uwagi
Czy poinformowano osoby, których dane dotyczą? (jeśli tak, to w jaki sposób, jeśli nie, to dlaczego)	Działania naprawcze	Działania zaradcze	Czy dokonano zgłoszenia? (jeśli nie, przyczyna niedokonania zgłoszenia)	Data zgłoszenia	Data zgłoszenia uzupełniającego	
Tak, zawiadomienie listowne	Komendant Miejski Policji w XYZ polecił wdrożenie czynności wyjaśniających w tej sprawie; przedmiotowe zdarzenie zostanie omówione na najbliższej doprawie kadry kierowniczej KMP w XYZ celem wzmocnienia nadzoru w tym zakresie; polecił ponownie przeszkolić w zakresie ochrony danych osobowych funkcjonariusza – sprawcę przedmiotowego incydentu,	Wysłano osobom, których dane dotyczą zawiadomienie o możliwych konsekwencjach i skutkach naruszenia. Poinformowano listownie osoby, których dane dotyczą o naruszeniu ich danych osobowych, pouczono je o możliwych konsekwencjach, a także zaproponowano im środki działania w celu zminimalizowania ewentualnych negatywnych skutków naruszenia ochrony danych osobowych. Ponadto osoby te zostały poinformowane o prawie do złożenia skargi do Prezesa UODO	tak	03.01.2024		

Bibliografia

- *Ogólne rozporządzenie o ochronie danych RODO, komentarz*, red. nauk. Edyta Bielak-Jooma, Dominik Lubasz, praca zbiorowa, str. 163-185, wyd. Wolters Kluwer, Warszawa 2018.
- Ustawa z dnia 14 grudnia 2018 r. o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości dalej UDODO (Dz.U.2023.1206).
- Ustawa o ochronie danych osobowych przetwarzanych w związku z zapobieganiem i zwalczaniem przestępczości, komentarz, red. Agnieszka Grzelak, Mirosław Wróblewski, str. 421-431, C.H.Beck, Warszawa 2019.
- *Zalecenia w sprawie metodyki oceny powagi naruszeń danych osobowych*, dokument roboczy, v1.0, grudzień 2013 r. Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji Clara Galan Manso, Sławomir Górniak.

Zakład Prewencji i Ruchu Drogowego

podkom. Paweł Dobaj
podkom. Grzegorz Waleczek

Szkoła Policji w Katowicach
ul. gen. Jankego 276
40-684 Katowice-Piotrowice
www.katowice.szkolapolicji.gov.pl