

Umowa powierzenia przetwarzania danych osobowych

zawarta w Warszawie pomiędzy:

Województwem Mazowieckim z siedzibą w Warszawie, ul. Jagiellońska 26, 03-719 Warszawa, NIP: 113-245-39-40; REGON: 015528910, reprezentowanym przez Zarząd Województwa Mazowieckiego, w imieniu którego na podstawie uchwały Nr 33/198/21 Zarządu Województwa Mazowieckiego z dnia 12 stycznia 2021 r. w sprawie upoważnienia do podpisywania, rozwiązywania i kontrolowania realizacji umów i porozumień dotyczących współadministrowania, udostępniania lub powierzenia przetwarzania danych osobowych, dla których Administratorem Danych Osobowych lub podmiotem przetwarzającym jest Województwo Mazowieckie albo Zarząd Województwa Mazowieckiego, w zakresie zadań realizowanych przez Departament Zdrowia i Polityki Społecznej w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie, działają:

- 1) – Dyrektor Departamentu Zdrowia i Polityki Społecznej Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie,
- 2) – Zastępca Dyrektora Departamentu Zdrowia i Polityki Społecznej Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie,

zwanym dalej: **Administratorem**,

a

....., – Podmiot przetwarzający,
zwanym dalej: **Procesorem**.

W niniejszej umowie zastosowano następujący skrót:

1. rozporządzenie - 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. naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
3. Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub innym podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
4. Podmiot przetwarzający (procesor) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

§ 1.

1. Procesor będzie przetwarzał w imieniu Administratora dane osobowe powierzone w trybie art. 28 rozporządzenia, na warunkach i w celu określonym w niniejszej umowie.
2. Procesor może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Administratora – co dotyczy też przekazywania danych osobowych do państwa trzeciego lub organizacji międzynarodowej – chyba że obowiązek taki nakłada na Procesora prawo Unii Europejskiej lub prawo państwa członkowskiego, któremu podlega Procesor. W takim przypadku przed rozpoczęciem przetwarzania Procesor informuje Administratora o tym obowiązku prawnym, o ile prawo to nie zabrania udzielania takiej informacji z uwagi na ważny interes publiczny.
3. Za udokumentowane polecenie przetwarzania przyjmuje się Umowę nr W/UMWM-UU/UM/ZD/...../2024 z 2024 roku łączącą Administratora i Procesora.

4. Administrator może wydawać kolejne polecenia w postaci wytycznych i instrukcji przez cały okres przetwarzania danych osobowych o ile nie są one sprzeczne z umową główną. Polecenia te są zawsze dokumentowane.

§ 2.

1. Na mocy niniejszej umowy Procesor będzie przetwarzał „dane zwykłe” uczestników konferencji pt.: „Profilaktyka i diagnostyka przesiewowa chorób cywilizacyjnych oczu mieszkańców Mazowsza” w następującym zakresie: imion, nazwiska, stopnia naukowego, tytułu zawodowego, miejsca pracy, stanowiska i wizerunku.
2. Dane osobowe powierzone przez Administratora będą przetwarzane przez Procesora wyłącznie w celu realizacji umowy nr W/UMWM-UU/UM/ZD/...../2024 z 2024 roku dotyczącej usługi streamingu na konferencji pt.: „Profilaktyka i diagnostyka przesiewowa chorób cywilizacyjnych oczu mieszkańców Mazowsza”. Dane osobowe będą przetwarzane do czasu zakończenia wyżej wymienionej umowy.

§ 3.

1. Procesor, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zobowiązuje się do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. W przypadku, gdy przetwarzanie obejmuje szczególne kategorie danych osobowych, Procesor stosuje dodatkowe zabezpieczenia tych danych.
3. *W celu zapewnienia bezpieczeństwa danych osobowych procesor wdraża co najmniej środki techniczne i organizacyjne określone w załączniku nr X (OPIS ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH WDROŻONYCH PRZEZ PODMIOT PRZETWARZAJĄCY, NALEŻY OPISAĆ SZCZEGÓŁOWO – NP. WSZELKIE POSIADANE CERTYFIKATY DOTYCZĄCE ZAPEWNIENIA BEZPIECZEŃSTWA PROCESÓW I PRODUKTÓW, ŚRODKI UMOŻLIWIAJĄCE PSEUDONIMIZACJĘ I SZYFROWANIE, ŚRODKI SŁUŻĄCE ZAPEWNIENIU BEZPIECZEŃSTWA FIZYCZNEGO MIEJSC, W KTÓRYCH PRZETWARZANE SĄ DANE, ITP). Zapewnienie bezpieczeństwa danych osobowych obejmuje ochronę danych osobowych przed naruszeniem bezpieczeństwa prowadzącym w szczególności do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych.*
4. Administrator akceptuje, że środki techniczne i organizacyjne mogą podlegać zmianom wynikającym z rozwoju technologicznego. W związku z tym, Procesor będzie posiadać prawo do wdrożenia adekwatnych alternatywnych środków, pod warunkiem utrzymania poziomu ich bezpieczeństwa.

§ 4.

1. Procesor zapewnia, że powierzone dane osobowe będą przetwarzane wyłącznie przez osoby do tego upoważnione.
2. Procesor udziela swoim pracownikom dostępu do powierzonych niniejszą umową danych osobowych jedynie w zakresie niezbędnym do wykonania umowy, zarządzania nią i jej monitorowania. Procesor zapewnia, by osoby upoważnione do przetwarzania powierzonych niniejszą umową danych osobowych zobowiązały się do zachowania poufności lub by podlegały odpowiedniemu ustawowemu obowiązkowi zachowania poufności.
3. Czynności określone w ust. 2 wymagają zachowania formy pisemnej.
4. Procesor prowadzi ewidencję osób upoważnionych.

§ 5.

1. *Procesor będzie korzystał z usług innego podmiotu przetwarzającego (zwanego dalej Podwykonawcą), któremu powierzy przetwarzanie danych osobowych na zasadach opisanych w niniejszej umowie. Lista planowanych podwykonawców stanowi załącznik nr X. Procesor informuje Administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Podwykonawców, dając tym samym Administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.*
2. *Procesor zapewnia, że na Podwykonawcę nałożone zostaną – na mocy umowy lub innego aktu prawnego, które podlegają prawu Unii Europejskiej lub prawu krajowemu – te same obowiązki ochrony danych, jakie na Procesora nakłada niniejsza umowa, a w szczególności obowiązek zapewnienia wystarczających gwarancji wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie odpowiadało wymogom rozporządzenia.*
3. *Jeżeli Podwykonawca nie wywiąże się ze spoczywających na nim obowiązków ochrony danych, pełna odpowiedzialność wobec Administratora za wypełnienie obowiązków Podwykonawcy spoczywa na Procesorze.*

ALBO

Procesor nie będzie korzystał z usług innego podmiotu przetwarzającego.

§ 6.

1. *Procesor, biorąc pod uwagę charakter przetwarzania danych, w miarę możliwości pomaga Administratorowi poprzez odpowiednie środki techniczne i organizacyjne wywiązać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, w zakresie wykonywania jej praw określonych w rozdziale III rozporządzenia. Procesor niezwłocznie zawiadamia administratora o każdym wniosku otrzymanym od osoby, której dane dotyczą. Procesor nie odpowiada na taki wniosek samodzielnie, chyba że administrator wyraził na to zgodę.*
2. *„Procesor pomaga Administratorowi w realizacji postanowień art. 13 i 14 rozporządzenia poprzez udostępnianie osobom, których dane dotyczą klauzuli informacyjnej stanowiącej załącznik nr X.” – JEŻELI MA ZASTOSOWANIE*
3. *Procesor, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia.*

§ 7.

1. *Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów i przyczynia się do nich.*
2. *Administrator informuje Procesora o terminie i zakresie audytu/inspekcji z co najmniej 5 - dniowym wyprzedzeniem.*
3. *Jeżeli audyt jest realizowany w związku z naruszeniem ochrony danych osobowych lub uzasadnionym podejrzeniem takiego naruszenia, Administrator może odstąpić od obowiązku określonego w ust. 2.*
4. *Po audycie Administrator może przekazać Procesorowi pisemne zalecenia wraz z terminem ich realizacji.*
5. *Procesor niezwłocznie informuje Administratora, jeżeli jego zdaniem zalecenie, o którym mowa w ust. 4, stanowi naruszenie rozporządzenia lub innych przepisów Unii Europejskiej lub krajowych.*
6. *Audyt, o którym mowa w ust. 1 jest realizowany w oparciu o "Regulamin audytu bezpieczeństwa informacji" dostępny na stronie internetowej Administratora.*

§ 8.

1. *W sytuacji naruszenia lub podejrzenia naruszenia ochrony danych osobowych powierzonych na mocy niniejszej umowy Procesor obowiązany jest postępować zgodnie z instrukcją zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych przyjętą przez Administratora.*
2. *Wyciąg z instrukcji, o której mowa w ust. 1 stanowi załącznik nr 1.*

3. Zmiana instrukcji nie wymaga dla swojej ważności zmiany umowy a jedynie notyfikację ze strony Administratora.
4. Procesor niezwłocznie informuje Administratora o każdym postępowaniu administracyjnym lub sądowym dotyczącym powierzonych do przetwarzania danych osobowych, a także o każdej kontroli lub audycie dotyczącym tychże danych osobowych.
5. Procesor ponosi pełną odpowiedzialność za wszelkie szkody powstałe w związku z przetwarzaniem przez niego danych osobowych, w sposób niezgodny z rozporządzeniem, niniejszą umową lub zaleceniami, o których mowa w § 7 ust. 4 – poniesione przez Administratora, osoby, których dane zostały powierzone lub osoby trzecie.

§ 9.

W przypadku, kiedy Administrator - działając w ramach odpowiedzialności solidarnej, o której mowa w art. 82 ust. 4 rozporządzenia zapłaci odszkodowanie, ma prawo roszczenia regresowego w stosunku do procesora.

§ 10.

1. Niniejsza umowa obowiązuje od dnia jej zawarcia do czasu obowiązywania UMOWY nr W/UMWM-UU/UM/ZD/...../2024 z 2024 r.).
2. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Procesor:
 - a) nie wykona zaleceń, o których mowa w § 7 ust. 4;
 - b) przetwarza powierzone dane osobowe w sposób niezgodny z przepisami o ochronie danych osobowych lub niniejszą umową.

§ 11.

1. Po zakończeniu świadczenia usług, o których mowa w § 2, Procesor – zależnie od decyzji Administratora – usuwa lub zwraca Administratorowi wszelkie dane osobowe oraz usuwa wszelkie istniejące ich kopie, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego nakazują przechowywanie danych osobowych.

§ 12.

1. Wszelkie zmiany niniejszej umowy powinny być dokonane w formie pisemnej pod rygorem nieważności.
2. W sprawach nieuregulowanych niniejszą umową mają zastosowania przepisy kodeksu cywilnego oraz rozporządzenia.
3. Umowę sporządzono w 2 egzemplarzach – 1 dla Procesora i 1 dla Administratora.
4. Datą zawarcia niniejszej umowy jest data złożenia oświadczenia woli o jej zawarciu przez ostatnią ze Stron.
5. Integralną częścią niniejszej Umowy stanowią: załącznik nr 1 – wyciąg z instrukcji zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych przetwarzanych na podstawie umowy powierzenia przetwarzania danych osobowych oraz załącznik do wyciągu z instrukcji zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych przetwarzanych na podstawie umowy powierzenia przetwarzania danych osobowych.

Administrator

Procesor

WYCIĄG Z INSTRUKCJI ZGŁASZANIA ZDARZEŃ ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH PRZETWARZANYCH NA PODSTAWIE UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

§ 1.

Zakres obowiązywania instrukcji

Instrukcja zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych ma zastosowanie w sytuacji naruszenia ochrony danych osobowych lub podejrzenia naruszenia danych osobowych powierzonych do przetwarzania, przez podmioty przetwarzające na podstawie umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego, zarówno bezpośrednio lub przy wykorzystaniu podmiotów trzecich – pracowników, współpracowników czy podmiotów, którym zlecono dalsze przetwarzanie w imieniu Administratora Danych Osobowych, tj.:

1. Zarządu Województwa Mazowieckiego;
2. Województwa Mazowieckiego;
3. Marszałka Województwa Mazowieckiego;
4. Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie.

§ 2.

Obowiązki podmiotu przetwarzającego

1. W razie stwierdzenia lub powzięcia informacji o zagrożeniu bezpieczeństwa danych osobowych podmiot przetwarzający zobowiązany jest niezwłocznie, dokonać oceny zdarzenia oraz:
 - 1) w przypadku braku naruszenia ochrony danych osobowych zawiadomić Sekretarza Województwa – Dyrektora Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie upoważnionego przez Administratora Danych Osobowych, o którym mowa w § 1 (zwanego dalej „Sekretarzem Województwa”) oraz Inspektora Ochrony Danych w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie, (zwanego dalej „Inspektorem Ochrony Danych”) o zagrożeniu bezpieczeństwa danych osobowych, które nie doprowadziło do naruszenia ochrony danych osobowych;

- 2) w przypadku naruszenia ochrony danych osobowych, które:
 - a) nie naraziło na ryzyko naruszenia praw i wolności osób fizycznych,
 - b) wiązało się z małym prawdopodobieństwem naruszenia praw i wolności osób fizycznych – zawiadomić Sekretarza Województwa oraz Inspektora Ochrony Danych o naruszeniu ochrony danych osobowych, które nie podlega zgłoszeniu organowi nadzorczemu;
 - 3) w przypadku naruszenia ochrony danych osobowych, które naraziło na ryzyko naruszenia praw i wolności osób fizycznych zawiadomić Sekretarza Województwa oraz Inspektora Ochrony Danych o naruszeniu ochrony danych osobowych, które podlega zgłoszeniu organowi nadzorczemu.
2. Przekazanie zawiadomienia, o którym mowa w ust. 1, następuje niezwłocznie, nie później niż w ciągu 24 godzin od wykrycia zdarzenia w wersji elektronicznej na adresy mailowe: waldemar.kulinski@mazovia.pl i iod@mazovia.pl.

§ 3.

Elementy zawiadomienia

1. Zawiadomienie, o którym mowa w § 2 ust. 1 pkt 2 musi zawierać co najmniej:
 - 1) wyraźne wskazanie że dane osobowe, których poufność, integralność lub dostępność została naruszona, są danymi osobowymi przetwarzanymi w imieniu Administratora Danych Osobowych, o którym mowa w § 1;
 - 2) elementy określone w art. 33 ust. 3 RODO:
 - a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
 - b) imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji;
 - c) możliwe konsekwencje naruszenia ochrony danych osobowych;
 - d) środki zastosowane lub proponowane przez podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych

przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;

- 3) informacje umożliwiające określenie czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych;
 - 4) w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych wykaz osób, których to naruszenie dotyczyło wraz z danymi umożliwiającymi ich powiadomienie o naruszeniu ochrony danych osobowych;
 - 5) w przypadku naruszenia ochrony danych osobowych niepodlegającego zgłoszeniu do organu nadzoru informacje umożliwiające określenie czy naruszenie wiąże się z brakiem ryzyka lub małym prawdopodobieństwem naruszenia praw i wolności osób fizycznych;
 - 6) w przypadku naruszenia terminu, o którym mowa w § 2 ust. 2, wyjaśnienie przyczyn opóźnienia.
2. Elementy określone w ust. 1 pkt 2 -5 należy przesłać poprzez wypełnienie tabeli określonej w załączniku do instrukcji.

§ 4.

Ocena zawiadomienia

1. Biuro Bezpieczeństwa Informacji w Departamencie Organizacji Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie (zwane dalej „Biurem Bezpieczeństwa Informacji”), we współpracy z dyrektorem/ zastępcą dyrektora departamentu/kancelarii który podpisał z upoważnienia Administratora Danych Osobowych umowę powierzenia przetwarzania danych osobowych oraz Inspektorem Ochrony Danych dokonuje analizy i oceny całokształtu zdarzenia zagrażającego bezpieczeństwu danych osobowych niezwłocznie, nie później niż w terminie 24 godzin, liczonych od momentu wpłynięcia zgłoszenia.
2. Biuro Bezpieczeństwa Informacji we współpracy z Inspektorem Ochrony Danych, z zachowaniem drogi służbowej, może wystąpić do podmiotu przetwarzającego o uzupełnienie przesłanego zawiadomienia lub o przekazanie dodatkowych wyjaśnień.
3. Podmiot przetwarzający jest związany żądaniem, o którym mowa w ust. 2 i realizuje je w terminie w nim wskazanym. § 3 ust. 1 pkt 6 stosuje się odpowiednio.

Załącznik do wyciągu z instrukcji zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych ma zastosowanie w sytuacji naruszenia ochrony danych osobowych lub podejrzenia naruszenia danych osobowych powierzonych do przetwarzania

Zgłoszenie naruszenia ochrony danych osobowych

1. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia

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

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia

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

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający

(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu

Pole obowiązkowe jeśli czas od momentu stwierdzenia naruszenia do czasu wypełnienia formularza jest dłuższy niż wskazany w INSTRUKCJI ZGŁASZANIA ZDARZEŃ ZAGRAŻAJĄCYCH BEZPIECZEŃSTWU DANYCH OSOBOWYCH PRZETWARZANYCH NA PODSTAWIE UMÓW POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Kliknij tutaj, aby wprowadzić tekst.

B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Trwające naruszenie

Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.

Data i czas zakończenia naruszenia

(opcjonalnie)
Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

C. Komentarz do czasu naruszenia (opcjonalnie)

Możesz podać więcej szczegółów dotyczących czasu naruszenia i uzasadnić dlaczego nie są znane dokładne terminy zaistnienia naruszenia.

Kliknij tutaj, aby wprowadzić tekst.

2. Charakter naruszenia

A. Charakter

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

B. Na czym polegało naruszenie?

Zgubienie lub kradzież nośnika/urządzenia

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

Opisz szczegółowo na czym polegało naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

C. Dzieci

Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

(opcjonalnie)

D. Przyczyna naruszenia

Wewnętrzne działanie niezamierzone

Wewnętrzne działanie zamierzone

Zewnętrzne działanie niezamierzone

Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznanne)

Kliknij tutaj, aby wprowadzić tekst.

2.1. Kategorie danych osobowych

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

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

Wymień jakie dane uległy naruszeniu. Odwołaj się do typów kategorii danych przetwarzanych na podstawie umowy lub innego instrumentu prawnego (np. dane o stanie zdrowia, dokumentacje uczniów z placówek oświaty, informacje dotyczące opieki społecznej, szczegóły finansowe, numery rachunków bankowych, numery paszportów).

Kliknij tutaj, aby wprowadzić tekst.

B. Dane podstawowe

Dane identyfikacyjne

np. imię, nazwisko, nr dowodu osobistego, adres IP

Krajowy numer identyfikacyjny

np. PESEL, SSN

Dane kontaktowe

np. e-mail, numer telefonu, adres korespondencyjny

Dane ekonomiczne i finansowe

np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe

Oficjalne dokumenty

np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje

Dane lokalizacyjne

np. GPS, dane o przemieszczaniu, miejsce zamieszkania

Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

C. 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

D. Dane, o których mowa w art. 10 RODO

Dane dotyczące wyroków skazujących

Dane dotyczące czynów zabronionych

Inne

Opisz poniżej kategorie danych:

Kliknij tutaj, aby wprowadzić tekst.

E. Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie

Nie dotyczy to liczby osób. Jednej osobie można przypisać kilka wpisów w zależności od kategorii danych przetwarzanych w ramach umowy lub innego instrumentu prawnego (np. jednej osobie można przypisać kilka wykonanych transakcji; w stosunku do pojedynczej osoby mogło dojść do naruszenia bezpieczeństwa w zakresie zarówno informacji dotyczącej opieki społecznej jak i informacji dot. finansów)

Kliknij tutaj, aby wprowadzić tekst.

2.2. Kategorie osób

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

A. Kategorie osób, których dane dotyczą

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

Kliknij tutaj, aby wprowadzić tekst.

B. Liczba osób, których mogło dotyczyć naruszenie

Przybliżona liczba osób, których mogło dotyczyć naruszenie

Kliknij tutaj, aby wprowadzić tekst.

3. Środki bezpieczeństwa zastosowane przed naruszeniem oraz po naruszeniu

A. Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przed naruszeniem

Kliknij tutaj, aby wprowadzić tekst.

B. Środki w celu zaradzenia naruszeniu ochrony danych osobowych

Opisz środki zastosowane lub proponowane w celu zminimalizowania ewentualnych negatywnych skutków naruszenia i jego ponownego wystąpienia.

Kliknij tutaj, aby wprowadzić tekst.

4. Możliwe konsekwencje

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

- | | |
|--|---|
| <input type="checkbox"/> Utrata kontroli nad własnymi danymi osobowymi | <input type="checkbox"/> Strata finansowa |
| <input type="checkbox"/> Ograniczenie możliwości realizowania praw z art. 15-22 RODO | <input type="checkbox"/> Naruszenie dobrego imienia |
| <input type="checkbox"/> Ograniczenie możliwości realizowania praw | <input type="checkbox"/> Utrata poufności danych osobowych chronionych tajemnicą zawodową |
| <input type="checkbox"/> Dyskryminacja | <input type="checkbox"/> Nieuprawnione odwrócenie pseudonimizacji |
| <input type="checkbox"/> Kradzież lub sfalszowanie tożsamości | <input type="checkbox"/> Inne |

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

Kliknij tutaj, aby wprowadzić tekst.

B. Ryzyko naruszenia praw i wolności osób fizycznych

BRAK/NISKIE/ŚREDNIE/WYSOKIE

Niepotrzebne skreślić

Szczegółowy opis dokonanej oceny ryzyka dla naruszenia praw i wolności osób fizycznych

Określ metodologię oceny i czynniki zdarzenia, które zostały wzięte pod uwagę przy ocenie ryzyka naruszenia praw i wolności osób fizycznych (np. na brak ryzyka może wpływać fakt, że naruszenie dotyczyło poufności danych zapisanych na szyfrowanym nośniku, lub danych powszechnie dostępnych)

Kliknij tutaj, aby wprowadzić tekst.