

Umowa powierzenia przetwarzania danych osobowych

zawarta w Warszawie pomiędzy **Województwem Mazowieckim**, z siedzibą w Warszawie, przy ul. Jagiellońskiej 26, 03-719 Warszawa, NIP: 113-245-39-40, REGON: 015528910, zwanym dalej **Zamawiającym**, reprezentowanym przez Zarząd Województwa Mazowieckiego, w imieniu którego, na podstawie uchwały Nr 813/344/18 Zarządu Województwa Mazowieckiego z dnia 29 maja 2018 r. w sprawie upoważnienia do podpisywania i kontrolowania realizacji umów dotyczących udostępniania lub powierzenia przetwarzania danych osobowych osobom lub podmiotom zewnętrznym, dla których Administratorem Danych Osobowych lub podmiotem przetwarzającym jest Województwo Mazowieckie albo Zarząd Województwa Mazowieckiego, w zakresie zadań realizowanych przez Kancelarię Marszałka w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie, działającą:

Magdalena Flis – Dyrektor Kancelarii Marszałka w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie;

Marta Milewska – Zastępca Dyrektora Kancelarii Marszałka w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie,

a

.....
.....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.

§ 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....., zwaną dalej „umową główną”.
4. Na mocy niniejszej umowy Procesor będzie przetwarzał dane zwykłe osób znajdujących się w bazie wysyłkowej pisma „Mazowsze serce Polski”, takie jak: imię i nazwisko, adres korespondencyjny.

§ 2.

Dane osobowe powierzone przez Administratora będą przetwarzane przez Procesora wyłącznie w celu adresowania, kolportowania i dostawy w związku z realizacją umowy głównej.

§ 3.

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.

§ 4.

1. Procesor zapewnia, że powierzone dane osobowe będą przetwarzane wyłącznie przez osoby do tego upoważnione.
2. Procesor może upoważniać swoich pracowników – którzy zobowiążą się do zachowania tajemnicy lub podlegają odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy – do przetwarzania danych osobowych powierzonych niniejszą umową.
3. Czynności określone w ust. 2 wymagają zachowania formy pisemnej.
4. Procesor prowadzi ewidencję osób upoważnionych.

§ 5.

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.

2. 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 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 do niniejszej umowy.
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, poniesione przez Administratora, osoby, których dane zostały powierzone lub osoby trzecie, 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.

§ 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 zawarcia umowy nr do końca jej obowiązywania, tj. nie dłużej niż do **30 kwietnia 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.

Po zakończeniu realizacji umowy 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. Umowa została sporządzona w formie elektronicznej i podpisana przez każdą ze Stron kwalifikowanym podpisem elektronicznym.
4. Datą zawarcia niniejszej umowy jest data złożenia oświadczenia woli o jej zawarciu przez ostatnią ze Stron.

Administrator

Procesor

Załącznik nr 1 do umowy powierzenia przetwarzania danych osobowych
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 nadzorcemu;
 - 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 oraz w wersji papierowej.

§ 3. Elementy zawiadomienia

1. Zawiadomienie, o którym mowa w § 2 ust. 1, 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 przestać 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	Kliknij tutaj, aby wprowadzić datę.
<small>Wskaż kiedy dowiedziałeś/aś się o naruszeniu. Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.</small>	
Sposób stwierdzenia naruszenia	Kliknij tutaj, aby wprowadzić tekst.
<small>Np. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwa</small>	
Data powiadomienia przez podmiot przetwarzający	Kliknij tutaj, aby wprowadzić tekst.
<small>(opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.</small>	
Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu	Kliknij tutaj, aby wprowadzić tekst.
<small>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</small>	
B. Czas naruszenia	
Data i czas zaistnienia/rozpoczęcia naruszenia	Kliknij tutaj, aby wprowadzić tekst.
<small>Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.</small>	
<input type="checkbox"/> Trwające naruszenie	
<small>Zaznacz to pole, jeśli naruszenie trwa nadal w momencie zgłaszania.</small>	
Data i czas zakończenia naruszenia	Kliknij tutaj, aby wprowadzić tekst.
<small>(opcjonalnie) Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.</small>	
C. Komentarz do czasu naruszenia <small>(opcjonalnie)</small>	
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	
<input type="checkbox"/> Naruszenie poufności danych	
<small>Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych</small>	
<input type="checkbox"/> Naruszenie integralności danych	
<small>Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania</small>	
<input type="checkbox"/> Naruszenie dostępności danych	
<small>Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną</small>	
B. Na czym polegało naruszenie?	
<input type="checkbox"/> Zgubienie lub kradzież nośnika/urządzenia	<input type="checkbox"/> Nieprawidłowa anonimizacja danych osobowych w dokumentce
<input type="checkbox"/> Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji	<input type="checkbox"/> Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora
<input type="checkbox"/> Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy	<input type="checkbox"/> Niezamierzona publikacja
<input type="checkbox"/> Nieuprawnione uzyskanie dostępu do informacji	<input type="checkbox"/> Dane osobowe wysłane do niewłaściwego odbiorcy
<input type="checkbox"/> Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń	<input type="checkbox"/> Ujawnienie danych niewłaściwej osobie
<input type="checkbox"/> Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych	<input type="checkbox"/> Ustne ujawnienie danych osobowych
<input type="checkbox"/> Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)	
Opisz szczegółowo na czym polegało naruszenie.	
Kliknij tutaj, aby wprowadzić tekst.	
C. Dzieci	
<input type="checkbox"/> Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.	
<small>(opcjonalnie)</small>	

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.

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

- | | |
|--|--|
| <input type="checkbox"/> Dane identyfikacyjne
np. imię, nazwisko, nr dowodu osobistego, adres IP | <input type="checkbox"/> Oficjalne dokumenty
np. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje |
| <input type="checkbox"/> Krajowy numer identyfikacyjny
np. PESEL, SSN | <input type="checkbox"/> Dane lokalizacyjne
np. GPS, dane o przemieszczaniu, miejsce zamieszkania |
| <input type="checkbox"/> Dane kontaktowe
np. e-mail, numer telefonu, adres korespondencyjny | <input type="checkbox"/> Inne
Opisz poniżej kategorie danych: |
| <input type="checkbox"/> Dane ekonomiczne i finansowe
np. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe | Kliknij tutaj, aby wprowadzić tekst. |

C. Dane szczególnej kategorii

- | | |
|---|---|
| <input type="checkbox"/> Dane o pochodzeniu rasowym lub etnicznym | <input type="checkbox"/> Dane dotyczące seksualności lub orientacji seksualnej |
| <input type="checkbox"/> Dane o poglądach politycznych | <input type="checkbox"/> Dane dotyczące zdrowia |
| <input type="checkbox"/> Dane o przekonaniach religijnych lub światopoglądowych | <input type="checkbox"/> Dane genetyczne |
| <input type="checkbox"/> Dane o przynależności do związków zawodowych | <input type="checkbox"/> 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. Kategorie osób

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

A. Kategorie osób, których dane dotyczą

- | | |
|---|--|
| <input type="checkbox"/> Pracownicy | <input type="checkbox"/> Klienci (obecni i potencjalni) |
| <input type="checkbox"/> Użytkownicy | <input type="checkbox"/> Klienci podmiotów publicznych |
| <input type="checkbox"/> Subskrybenci | <input type="checkbox"/> Pacjenci |
| <input type="checkbox"/> Studenci | <input type="checkbox"/> Dzieci |
| <input type="checkbox"/> Uczniowie | <input type="checkbox"/> Osoby o szczególnych potrzebach (np. osoby starsze, niepełnosprawne itp.) |
| <input type="checkbox"/> Służby mundurowe (np. wojsko, policja) | |

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 sfałszowanie 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.