

Załącznik nr 5 do Umowy o powierzenia przetwarzania danych osobowych

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

Par. 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.

Par. 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 Par. 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 nadzorcemu.

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.

Par. 3.

Elementy zawiadomienia

1. Zawiadomienie, o którym mowa w Par. 2 ust. 1, musi zawierać co najmniej:
 - 1) wyrażne wskazanie że dane osobowe, których poufność, integralność lub dostępność została naruszona, są danymi osobowymi przetwarzanymi w imieniu Administratora Danych Osobowych, o którym mowa w Par. 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 Par. 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.

Par. 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. Par. 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 wypełniania 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 nieznane)

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**

☐ **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.

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

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

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