#

**Załącznik nr 4**

**Umowa powierzenia przetwarzania danych osobowych**

Zawarta…………………………w Warszawie pomiędzy:

**Zarządem Województwa Mazowieckiego** z siedzibą w Warszawie, ul. Jagiellońska 26, 03-719 Warszawa**,** w imieniu którego, na podstawie uchwały Nr 146/467/24 Zarządu Województwa Mazowieckiego z dnia 23 stycznia 2024, w sprawie upoważnienia do podpisywania, rozwiązywania i kontrolowania realizacji umów i porozumień dotyczących współadministrowania, udostępniania lub powierzania przetwarzania danych osobowych, dla których Administratorem Danych Osobowych lub podmiotem przetwarzającym jest Województwo Mazowieckie albo Zarząd Województwa Mazowieckiego, w zakresie zadań realizowanych przez Departament Rozwoju Regionalnego i Funduszy Europejskich w Urzędzie Marszałkowskim Województwa Mazowieckiego w Warszawie działają:

1. Pan Marcin Wajda – Dyrektor Departamentu Rozwoju Regionalnego i Funduszy Europejskich Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie;
2. Pani Anna Gręda – Zastępca Dyrektora Departamentu Rozwoju Regionalnego i Funduszy Europejskich Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie,

– Administrator Danych Osobowych,

zwanym dalej: **Administratorem**,

a

…………………………z siedzibą przy ul……………, ………….., NIP ……………., REGON …………….*,* zwanym dalej „Wykonawcą”, reprezentowanym przez: ……………………………., zgodnie z ……………., według stanu na dzień……………. (aktualny odpis z właściwego rejestru albo aktualne zaświadczenie o wpisie do ewidencji działalności gospodarczej) – Podmiot przetwarzający,

zwaną 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;
		5. SL 2014 - aplikacja główna centralnego systemu teleinformatycznego, o którym mowa w rozdziale 16 ustawy o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014-2020 (Dz. U. z 2020 r. poz. 818, z późn. zm.). Administratorem danych osobowych przetwarzanych
		w SL2014 jest Minister Inwestycji i Rozwoju z siedzibą w Warszawie, przy ul. Wspólnej 2/4. Porozumieniem Nr RPMA/07/2015 z dnia 09.09.2015 r. Minister Infrastruktury i Rozwoju powierzył przetwarzanie danych zgromadzonych w centralnym systemie informatycznym Zarządowi Województwa Mazowieckiego,
		z umocowaniem do dalszego powierzania przetwarzania danych osobowych,
		6. MEWA 2.0 - Mazowiecki Elektroniczny Wniosek Aplikacyjny Regionalnego Programu Operacyjnego Województwa Mazowieckiego 2014 – 2020. Administratorem danych osobowych przetwarzanych w MEWA 2.0 jest Zarząd Województwa Mazowieckiego;
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 **………………………..** dotyczącą przeprowadzenia badania i opracowania raportu pn***.*** ***„***Ocena realizacji Regionalnego Programu Zdrowotnego Samorządu Województwa Mazowieckiego „*Regionalny program zdrowotny w zakresie chorób kręgosłupa
i otyłości wśród dzieci z województwa mazowieckiego*”*”****”.***
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 mocy niniejszej umowy Procesor będzie przetwarzał wszystkie ujęte w systemie MEWA 2.0 oraz SL 2014 dane osobowe uczestników projektów oraz Wnioskodawców i Beneficjentów aplikujących w ramach RPO WM 2014-2020.
1. Dane osobowe powierzone przez Administratora będą przetwarzane przez Procesora wyłącznie w okresie realizacji umowy, o której mowa w §1 ust. 3 celu wykonania zadań z niej wynikających.

# § 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 1 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.

Procesor nie będzie korzystał z usług Dalszego podmiotu przetwarzającego.

# § 6.

1. Procesor, biorąc pod uwagę charakter przetwarzania danych osobowych, 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, 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 realizowany jest w związku 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 2 tworzący integralną część 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 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 przez okres realizacji umowy, o której mowa w §1 ust. 3
2. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Procesor:
3. nie wykona zaleceń, o których mowa w § 7 ust. 4;
4. 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 w formie papierowej sporządzono w Umowę sporządzono w czterech jednobrzmiących egzemplarzach, z czego jeden otrzymuje Procesor, a trzy Administrator.

 **Administrator Procesor**

Załączniki:

### Zał. 1 - Wykaz środków technicznych i organizacyjnych wdrożonych przez podmiot przetwarzający;

Zał. 2 - Wyciąg z instrukcji zgłaszania zdarzeń zagrażających bezpieczeństwu danych osobowych przetwarzanych na podstawie umów powierzenia przetwarzania danych osobowych

## Załącznik 1 do Umowy o powierzenie przetwarzania danych osobowych

### Wykaz środków technicznych i organizacyjnych wdrożonych przez podmiot przetwarzający

*Instrukcja dla osoby sporządzającej umowę[[1]](#footnote-1):*

*Środki techniczne i organizacyjne należy opisać szczegółowo, a nie w sposób ogólny. Przykłady wskazane w załączniku mają jedynie charakter wspierający, należy odpowiednio uzupełnić i określić zastosowane lub planowane środki ochrony. Wykaz środków powinien dotyczyć bezpośrednio zabezpieczeń powierzanych danych osobowych na drodze umowy.*

*Jeśli ADO lub powierzającym jest WM, MWM, ZWM lub Urząd, to za opis środków technicznych odpowiada Procesor (tj. Procesor opisuje jakie środki zastosuje w celu zapewnienia ochrony powierzonym mu danym osobowym).*

*Przy opisywaniu środków technicznych i organizacyjnych należy wziąć pod uwagę charakter, zakres, cel i kontekst przetwarzania oraz ryzyko dla praw i wolności osób fizycznych.*

*Przykłady ewentualnych środków:*

1. *Środki dotyczące pseudonimizacji i szyfrowania danych osobowych*

*(w ramach kategorii możemy opisać, czy dane są szyfrowane, jakie metody szyfrowania lub pseudonimizacji będą zastosowane, np. szyfrowanie TLS, AES256, tokenizacja, skracanie danych);*

1. *Środki mające na celu ciągłe zapewnienie poufności, integralności, dostępności i odporności systemów i usług przetwarzania*

*(w ramach kategorii możemy opisać wszelkie zabezpieczenia mające wpływ na nieujawnianie danych osobowych, ich kompletność i prawidłowość, dostępność dla osób uprawnionych oraz odporność na ataki zewnętrzne mające na celu nieuprawniony dostęp do danych ich zmianę lub zniszczenie);*

1. *Środki mające na celu zapewnienie zdolności szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego*

*(w ramach kategorii możemy opisać, czy* wykonuje się kopie zapasowe, czy kopie są testowane i przechowywane poza miejscem ich wykonywania);

1. *Procedury regularnego testowania, mierzenia i oceniania skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania*

*(w ramach kategorii możemy opisać czy podmiot przetwarzający wdrożył i stosuje ww. procedury);*

1. *Środki identyfikacji i autoryzacji użytkowników*

*(w ramach kategorii możemy opisać, czy dane będą przetwarzane przez użytkowników posiadających unikalny identyfikator w systemie informatycznym oraz czy dostęp do systemu możliwy jest wyłącznie za uwierzytelnieniem: hasło, token, lub inna metoda);*

1. *Środki ochrony danych podczas przekazywania*

*(w ramach kategorii możemy opisać jakie są stosowane zabezpieczenia przy przekazywaniu danych osobowych do innych osób/podmiotów. W systemie elektronicznym: szyfrowanie, udostępnianie poprzez zabezpieczony serwer FTP; udostępnianie poprzez zabezpieczony kontener w chmurze, np. onedrive, google drive, inne. W systemie tradycyjnym: teczki na dokumenty, plombowanie, firma kurierska, operator pocztowy, torby/walizki z szyfrem, inne);*

1. *Środki ochrony danych podczas przechowywania*

*(w ramach kategorii możemy opisać jakie zabezpieczenia będą stosowane podczas przechowywania danych np. zabezpieczone pomieszczenia, meble, infrastruktura IT);*

1. *Środki mające na celu zapewnienie bezpieczeństwa fizycznego miejsc, w których odbywa się przetwarzanie danych osobowych*

*(w ramach kategorii możemy opisać jakie będą zabezpieczenia fizyczne w obszarze przetwarzania powierzonych danych osobowych będą stosowane np. utworzenie stref dostępu, zamykanie pomieszczeń na klucz/zamek elektroniczny z ewidencją dostępu/inne oraz w jaki sposób miejsca przetwarzania będą zabezpieczone przed niekorzystnymi warunkami środowiskowymi np. nadmierna wilgotnością, pożarem, zalaniem itp.);*

1. *Środki mające na celu zapewnienie ewidencji zdarzeń*

*(w ramach kategorii możemy opisać w jaki sposób ewidencjonuje się operacje wykonywane na danych tj. utrzymuje zapisy z logów systemowych, dzienników zdarzeń dla zapewnienia rozliczalności wykonywanych operacji na danych, w tym informacji o tym, kto te operacje wykonał);*

1. *Środki mające na celu zapewnienie konfiguracji systemu, w tym konfiguracji domyślnej*

*(w ramach kategorii możemy opisać jaką dokumentację dotyczącą konfiguracji systemu informatycznego posiada Procesor, czy stosuje domyślne konfiguracje systemu np. dla konkretnych ról użytkowników itp.);*

1. *Środki wewnętrznego zarządzania i kierowania w zakresie technologii informacji i bezpieczeństwa informatycznego*

*(w ramach kategorii możemy opisać jaki udokumentowane procedury opracowano i wdrożono w zakresie bezpieczeństwa przetwarzania danych osobowych np. Polityki bezpieczeństwa informacji/danych osobowych; Procedury operacyjne np. uwierzytelniania; zarzadzania uprawnieniami użytkowników, kopii zapasowych; zgłaszania naruszeń itp.);*

1. *Środki certyfikacji/zapewnienia procesów i produktów*

*(w ramach kategorii możemy opisać jakie w organizacji wdrożono formalne systemy bezpieczeństwa informacji np. ISO 27001, ISO 22301 lub inne np. zatwierdzone kodeksy postepowania, o których mowa w art. 40 RODO);*

1. *Środki mające na celu zapewnienie minimalizacji danych*

*(w ramach kategorii możemy opisać jakie procedury w zakresie minimalizacji danych tj. zapewnienia przetwarzania danych wyłącznie niezbędnych do procesu przetwarzania zostały wdrożone);*

1. *Środki mające na celu zapewnienie jakości danych*

*(w ramach kategorii możemy opisać jakie wdrożono rozwiązania gwarantujące zapewnienie odpowiedniej jakość danych tj., że te dane są prawdziwe i poprawne np. ich walidację przed wprowadzeniem do systemu);*

1. *Środki mające na celu zapewnienie ograniczonego zatrzymywania danych*

*(w ramach kategorii możemy opisać jakie narzędzia zagwarantują realizację prawa do ograniczenia przetwarzania danych);*

1. *Środki mające na celu zapewnienie odpowiedzialności*

*(w ramach kategorii możemy opisać jakie wdrożono zabezpieczenia w zakresie odpowiedzialności użytkowników za przetwarzanie danych np. umowy o zachowaniu poufności ”NDA”);*

1. *Środki mające na celu umożliwienie przenoszenia danych*

*(w ramach kategorii możemy opisać jakie narzędzia zagwarantują realizację prawa do przenoszenia danych);*

1. *Środki mające na celu zapewnienie usuwania danych*

*(w ramach kategorii możemy opisać jakie będą stosowane metody niszczenia danych/nośników).*

## Załącznik 2 do Umowy o powierzenie 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:
2. 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;
3. w przypadku naruszenia ochrony danych osobowych, które:
4. nie naraziło na ryzyko naruszenia praw i wolności osób fizycznych,
5. 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,
6. 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.
7. 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:
2. 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;
3. elementy określone w art. 33 ust. 3 RODO:
4. 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;
5. imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji,
6. możliwe konsekwencje naruszenia ochrony danych osobowych,
7. 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;
8. informacje umożliwiające określenie czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych;
9. 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;
10. 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;
11. w przypadku naruszenia terminu, o którym mowa w § 2 ust. 2, wyjaśnienie przyczyn opóźnienia.
12. 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 późnej 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**
 |
| 1. **Wykrycie naruszenia i powiadomienie organu nadzorczego**
 |
| Data stwierdzenia naruszeniaWskaż, kiedy dowiedziałeś/aś się o naruszeniu.Jeśli nie znasz dokładnego terminu, podaj czas przybliżony. | Kliknij tutaj, aby wprowadzić datę. |
| Sposób stwierdzenia naruszeniaNp. zgłoszenie osoby której dane dotyczą czy cykliczny przegląd logów systemowych zgodnie z wdrożoną polityką bezpieczeństwaKliknij 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 naruszeniuPole 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 OSOBOWYCHKliknij tutaj, aby wprowadzić tekst. |
| 1. **Czas naruszenia**
 |
| Data i czas zaistnienia/rozpoczęcia naruszeniaJeśli nie znasz dokładnego terminu, podaj czas przybliżony. | Kliknij tutaj, aby wprowadzić tekst. |
| **☐** Trwające naruszenieZaznacz 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. |
| 1. **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. |

|  |
| --- |
| 1. **Charakter naruszenia**
 |
| 1. **Charakter**
 |
| **☐** Naruszenie poufności danychNieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych**☐** Naruszenie integralności danychWprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania**☐** Naruszenie dostępności danychBrak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną |
| 1. **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. |
| 1. **Dzieci**
 |
| **☐** Naruszenie dotyczy przetwarzania danych w związku ze świadczeniem usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.(opcjonalnie) |
| 1. **Przyczyna naruszenia**
 |
| **☐** Wewnętrzne działanie niezamierzone**☐** Wewnętrzne działanie zamierzone**☐** Zewnętrzne działanie niezamierzone**☐** Zewnętrzne działanie zamierzoneInne przyczyny (w tym nieznane)Kliknij tutaj, aby wprowadzić tekst. |

|  |
| --- |
| * 1. **Kategorie danych osobowych**

**UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** |
| 1. **Kategorie danych**
 |
| Szczegółowy opis kategorii danych, których dotyczy naruszenieWymień 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. |
| 1. **Dane podstawowe**
 |
| **☐** Dane identyfikacyjnenp. imię, nazwisko, nr dowodu osobistego, adres IP **☐** Krajowy numer identyfikacyjnynp. PESEL, SSN **☐** Dane kontaktowenp. e-mail, numer telefonu, adres korespondencyjny **☐** Dane ekonomiczne i finansowenp. historie transakcji, faktury, dane o rachunkach bankowych, wnioski o wsparcie finansowe  | **☐** Oficjalne dokumentynp. akty notarialne, dowody osobiste, prawa jazdy, karty pobytu, legitymacje **☐** Dane lokalizacyjnenp. GPS, dane o przemieszczaniu, miejsce zamieszkania **☐** InneOpisz poniżej kategorie danych:Kliknij tutaj, aby wprowadzić tekst. |
| 1. **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 |
| 1. **Dane, o których mowa w art. 10 RODO**
 |
| **☐** Dane dotyczące wyroków skazujących**☐** Dane dotyczące czynów zabronionych**☐** InneOpisz poniżej kategorie danych:Kliknij tutaj, aby wprowadzić tekst. |
| 1. **Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenie**
 |
| Przybliżona liczba wpisów danych osobowych, których dotyczy naruszenieNie 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. |
| * 1. **Kategorie osób**

**UWAGA: W zgłoszeniu nie podawaj danych konkretnych osób, których dotyczy naruszenie.** |
| 1. **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 naruszenieKliknij tutaj, aby wprowadzić tekst. |
| 1. **Liczba osób, których mogło dotyczyć naruszenie**
 |
| Przybliżona liczba osób, których mogło dotyczyć naruszenie | Kliknij tutaj, aby wprowadzić tekst. |
| 1. **Środki bezpieczeństwa zastosowane przed naruszeniem oraz po naruszeniu**
 |
| 1. **Ogólny opis technicznych i organizacyjnych środków bezpieczeństwa stosowanych przed naruszeniem**
 |
| Kliknij tutaj, aby wprowadzić tekst. |
| 1. **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. |
| 1. **Możliwe konsekwencje**
 |
| 1. **Uszczerbek fizyczny, majątkowy, niemajątkowy lub inne znaczące konsekwencje dla osoby, której dane dotyczą**
 |
| **☐** Utrata kontroli nad własnymi danymi osobowymi**☐** Ograniczenie możliwości realizowania praw z art. 15-22 RODO**☐** Ograniczenie możliwości realizowania praw**☐** Dyskryminacja**☐** Kradzież lub sfałszowanie tożsamości | **☐** Strata finansowa**☐** Naruszenie dobrego imienia**☐** Utrata poufności danych osobowych chronionych tajemnicą zawodową**☐** Nieuprawnione odwrócenie pseudonimizacji**☐** InneOpisz poniżej inne skutki naruszenia prawa do ochrony danych osoby, której dane dotyczą:Kliknij tutaj, aby wprowadzić tekst. |
| 1. **Ryzyko naruszenia praw i wolności osób fizycznych**
 |
| BRAK/NISKIE/ŚREDNIE/WYSOKIENiepotrzebne skreślićSzczegółowy opis dokonanej oceny ryzyka dla naruszenia praw i wolności osób fizycznychOkreśl 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. |

1. Usuń instrukcję oraz przykłady ewentualnych środków po uzupełnieniu wykazu. [↑](#footnote-ref-1)