

Umowa powierzenia przetwarzania danych osobowych nr

Zawarta 2021 r. w Warszawie pomiędzy:

Województwem Mazowieckim, ul. Jagiellońska 26, 03-719 Warszawa, NIP: 113-245-39-40, REGON 015528910, reprezentowanym przez:

- 1) -,
- 2) -,

działającymi na podstawie uchwały nr 485/220/21 Zarządu Województwa Mazowieckiego z dnia 6 kwietnia 2021 r. oraz uchwały nr 1509/92/15 Zarządu Województwa Mazowieckiego z dnia 10 listopada 2015 r.¹

– Podmiot powierzający, zwanym dalej: **Powierzającym**,

a

..... z siedzibą w, ul.,,
reprezentowanym/ną przez:

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

Niniejsza umowa zostaje zawarta w związku z zawarciem umowy nr z dnia 2021 r.

§ 1.

W niniejszej umowie zastosowano następujące skróty:

- 1) Instytucja Pośrednicząca – instytucja pełniąca funkcję Instytucji Pośredniczącej, którą jest Mazowiecka Jednostka Wdrażania Programów Unijnych, działająca w imieniu Instytucji Zarządzającej;
- 2) Instytucja Zarządzająca - Zarząd Województwa Mazowieckiego będący Instytucją Zarządzającą Regionalnym Programem Operacyjnym Województwa Mazowieckiego na lata 2014-2020;
- 3) 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;
- 4) Powierzający (podmiot powierzający) - Województwo Mazowieckie umocowane do dalszego powierzenia danych osobowych zgodnie z Zasadami realizacji Projektu grantowego „Modelowanie Systemu Ofert Dla Innowacji” nr RPMA.03.01.02-14-b657/18-00 współfinansowanego z Europejskiego Funduszu Rozwoju Regionalnego w ramach Osi Priorytetowej III „Rozwój potencjału innowacyjnego i przedsiębiorczości” 3.1 „Poprawa rozwoju MŚP na Mazowszu” 3.1.2 „Rozwój MŚP” Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, stanowiącymi załącznik do uchwały nr 177/9/18 Zarządu Województwa Mazowieckiego z dnia 18 grudnia 2018 r.²;
- 5) Procesor – podmiot, któremu powierzono przetwarzanie danych osobowych na mocy niniejszej umowy powierzenia;

¹ Zmienionej uchwałami Zarządu Województwa Mazowieckiego: nr 1695/105/15 z dnia 15 grudnia 2015 r., nr 448/229/17 z dnia 27 marca 2017 r., nr 1450/274/17 z dnia 19 września 2017 r., nr 1437/372/18 z 10 września 2018 r. oraz nr 1157/63/19 z dnia 13 sierpnia 2019 r.

² Zmienionej uchwałą nr 1542/171/20 Zarządu Województwa Mazowieckiego z dnia 7 października 2020 r.

- 6) Projekt MSODI – pozakonkursowy projekt grantowy „Modelowanie Systemu Ofert Dla Innowacji” realizowany w ramach Poddziałania 3.1.2 Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, którego Beneficjentem jest Województwo Mazowieckie;
- 7) Przetwarzanie danych - operacje lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
- 8) 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);
- 9) Umowa - niniejsza Umowa powierzenia przetwarzania danych osobowych;
- 10) Zlecenie – przedmiot umowy nr dotyczącej wykonania usługi organizacji i przeprowadzenia spotkań networkingowych.

§ 2.

1. Procesor będzie przetwarzał w imieniu Powierającego dane osobowe, w rozumieniu art. 4 pkt 1 RODO, dotyczące osób biorących udział w realizacji spotkań networkingowych online, powierzone w trybie art. 28 RODO, na warunkach i w celu określonym w niniejszej Umowie (w dalszej części Umowy: „dane osobowe”).
2. Procesor może przetwarzać dane osobowe wyłącznie na udokumentowane polecenie Powierającego – 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 Powierającego 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 zlecenie, o którym mowa w § 1 pkt.10.

§ 3.

1. Przedmiotem umowy jest powierzenie Procesorowi przez Powierającego danych osobowych w zbiorach, o których mowa w Załączniku nr 1 do niniejszej Umowy, w zakresie zgodnym z ust. 2.
2. Dane osobowe powierzone przez Powierającego będą przetwarzane przez Powierającego wyłącznie w celu organizacji i przeprowadzenia spotkań networkingowych w związku z realizacją Zlecenia.

§ 4.

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.

§ 5.

1. Do przetwarzania danych osobowych mogą być dopuszczone jedynie osoby upoważnione przez Procesora, które zobowiązały się do zachowania tajemnicy lub podlegały odpowiedniemu ustawowemu obowiązkowi zachowania tajemnicy, zgodnie z zapisami art. 28 RODO.
2. Powierający, w imieniu Instytucji Zarządzającej, zobowiązuje Procesora i osoby upoważnione do zachowania tajemnicy danych osobowych oraz informacji o stosowanych sposobach ich zabezpieczenia.

3. Procesor jest zobowiązany do wydawania oraz odwoływania upoważnień do przetwarzania danych osobowych w formie w jakiej zostały określone odpowiednio w Załączniku nr 2 i 3 niniejszej Umowy lub w innej formie zawierającej wszystkie elementy wskazane odpowiednio w Załączniku nr 2 i 3 niniejszej Umowy.
4. Czynności określone w ust. 1 wymagają zachowania formy pisemnej.
5. Upoważnienie wygasa z chwilą ustania stosunku prawnego łączącego Procesora z osobą wskazaną w ust. 1.
6. Procesor prowadzi ewidencję osób upoważnionych.

§ 6.

1. Procesor nie korzysta z usług innego podmiotu przetwarzającego (zwanego dalej Podwykonawcą) bez uprzedniej szczegółowej lub ogólnej pisemnej zgody Powierzającego. W przypadku ogólnej pisemnej zgody Procesor informuje Powierzającego o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia Podwykonawców, dając tym samym Powierzającemu 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 Powierzającego za wypełnienie obowiązków Podwykonawcy spoczywa na Procesorze.

§ 7.

1. Procesor, biorąc pod uwagę charakter przetwarzania danych, w miarę możliwości pomaga Powierzającemu 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 pomaga Powierzającemu w realizacji postanowień art. 13 i 14 rozporządzenia.
3. W celu zrealizowania, wobec osoby fizycznej biorącej udział w realizacji zlecenia, obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO, Procesor jest zobowiązany odebrać oświadczenie, którego wzór stanowi Załącznik nr 4 do niniejszej Umowy. Oświadczenia przechowuje Procesor w swojej siedzibie lub w innym miejscu, w którym są zlokalizowane dokumenty związane z realizacją Zlecenia. Zmiana wzoru oświadczenia nie wymaga aneksowania niniejszej Umowy.
4. Procesor, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, pomaga Powierzającemu wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia.

§ 8.

1. Procesor umożliwi Instytucji Zarządzającej, Powierzającemu, Instytucji Pośredniczącej lub podmiotom przez nie upoważnionym, w miejscach, w których są przetwarzane powierzone dane osobowe, dokonanie kontroli lub audytu zgodności przetwarzania powierzonych danych osobowych z ustawą o ochronie danych osobowych, RODO, przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych oraz z niniejszą Umową. Zawiadomienie o zamiarze przeprowadzenia kontroli lub audytu powinno być przekazane podmiotowi kontrolowanemu co najmniej 5 dni roboczych przed rozpoczęciem kontroli/audytu.
2. W przypadku powzięcia przez Instytucję Zarządzającą, Powierzającemu lub Instytucję Pośredniczącą wiadomości o rażącym naruszeniu przez Procesora obowiązków wynikających z ustawy o ochronie danych osobowych, RODO, przepisów prawa powszechnie obowiązującego dotyczących ochrony danych osobowych lub z niniejszej Umowy, Procesor umożliwi Instytucji Zarządzającej, Instytucji Pośredniczącej, Powierzającemu

lub podmiotom przez nie upoważnionym dokonanie niezapowiedzianej kontroli lub audytu, w celu określonym w ust. 1.

3. Kontrolerzy Instytucji Zarządzającej, Instytucji Pośredniczącej, Powierzającego lub podmiotów przez nie upoważnionych, mają w szczególności prawo:
 - 1) wstępu, w godzinach pracy Procesora, za okazaniem imiennego upoważnienia, do pomieszczenia, w którym jest zlokalizowany zbiór powierzonych do przetwarzania danych osobowych oraz pomieszczenia, w którym są przetwarzane powierzone dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych osobowych z RODO, przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych oraz z Umową;
 - 2) żądać złożenia pisemnych lub ustnych wyjaśnień przez osoby upoważnione do przetwarzania danych osobowych, przedstawiciela Procesora oraz pracowników w zakresie niezbędnym do ustalenia stanu faktycznego;
 - 3) wglądu do wszelkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli lub audytu oraz sporządzania ich kopii;
 - 4) przeprowadzania oględzin urządzeń, nośników oraz systemu informatycznego służącego do przetwarzania danych osobowych.
4. Procesor może zostać poddany kontroli lub audytowi zgodności przetwarzania powierzonych do przetwarzania danych osobowych z ustawą o ochronie danych osobowych, RODO, przepisami prawa powszechnie obowiązującego dotyczącymi ochrony danych osobowych w miejscach, w których są one przetwarzane przez instytucje uprawnione do kontroli lub audytu na podstawie odrębnych przepisów.
5. Po audycie/kontroli podmiot przeprowadzający audyt/kontrolę może przekazać Procesorowi pisemne zalecenia wraz z terminem ich realizacji.
6. Procesor zobowiązuje się zastosować zalecenia dotyczące poprawy jakości zabezpieczenia danych osobowych oraz sposobu ich przetwarzania sporządzonych w wyniku kontroli lub audytu przeprowadzonych przez Instytucję Zarządzającą, Instytucję Pośredniczącą, Powierzającego lub przez podmioty przez nie upoważnione albo przez inne instytucje upoważnione do kontroli na podstawie odrębnych przepisów.
7. Procesor niezwłocznie informuje podmiot przeprowadzający audyt/kontrolę, jeżeli jego zdaniem zalecenie, o którym mowa w ust. 5, stanowi naruszenie rozporządzenia lub innych przepisów Unii Europejskiej lub krajowych.
8. Audyt, o którym mowa w ust. 1 jest realizowany w oparciu o „Regulamin audytu i ochrony danych osobowych, których administratorem jest Województwo Mazowieckie lub Zarząd Województwa Mazowieckiego, dostępny na stronie internetowej Samorządu Województwa Mazowieckiego w Warszawie.

§ 9.

1. Procesor jest zobowiązany do podjęcia wszelkich kroków służących zachowaniu tajemnicy danych osobowych przetwarzanych przez mające do nich dostęp osoby upoważnione do przetwarzania danych osobowych, w szczególności niezwłocznie informując Powierzającego o:
 - 1) wszelkich przypadkach naruszenia ochrony danych osobowych lub o ich niewłaściwym użyciu;
 - 2) wszelkich czynnościach z własnym udziałem w sprawach dotyczących ochrony danych osobowych prowadzonych w szczególności przed Prezesem Urzędu Ochrony Danych Osobowych, Europejskim Inspektorem Ochrony Danych, urzędami państwowymi, policją lub przed sądem;
 - 3) wynikach kontroli prowadzonych przez podmioty uprawnione w zakresie przetwarzania danych osobowych wraz z informacją na temat zastosowania się do wydanych zaleceń, o których mowa w ust. 3.

2. Procesor zobowiązuje się do udzielenia Powierzającemu, na każde jego żądanie, informacji na temat przetwarzania danych osobowych, o których mowa w niniejszym paragrafie, w szczególności niezwłocznego przekazywania informacji o każdym przypadku naruszenia przez niego i osoby przez niego upoważnione do przetwarzania danych osobowych obowiązków dotyczących ochrony danych osobowych.
3. W przypadku wystąpienia naruszenia ochrony danych osobowych, mogącego powodować w ocenie Powierzającego wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Procesor na wniosek Powierzającego, bez zbędnej zwłoki zawiadomi osoby, których naruszenie ochrony danych osobowych dotyczy.
4. 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 Powierzającego. Wyciąg z instrukcji, o której mowa w ust. 5 stanowi załącznik do niniejszej Umowy.
5. Zmiana instrukcji nie wymaga dla swojej ważności zmiany niniejszej Umowy a jedynie notyfikację ze strony Powierzającego.
6. Procesor niezwłocznie informuje Powierzającego o każdym postępowaniu administracyjnym lub sądowym dotyczącym powierzonych do przetwarzania danych osobowych, a także o każdej kontroli lub audycie dotyczącym tychże danych osobowych.
7. Procesor z chwilą zawarcia niniejszej Umowy przejmuje pełną odpowiedzialność z tytułu wszelkich szkód poniesionych przez Instytucję Zarządzającą, Instytucję Pośredniczącą, Powierzającego oraz przez osoby, których dane zostały powierzone Procesorowi, wynikłych na skutek celowych lub przypadkowych działań jego lub jego pracowników, stanowiących naruszenie przepisów o ochronie danych osobowych, RODO, w szczególności za szkody powstałe na skutek nieuprawnionego dostępu do danych osobowych, nieuprawnionego udostępnienia danych osobowych osobom trzecim oraz przetwarzania danych osobowych w celach i zakresie innym, niż określone w § 2 Umowy lub niezgodnie z zaleceniami, o których mowa w § 8 ust. 5.

§ 10.

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.

§ 11.

1. Niniejsza umowa obowiązuje od dnia jej zawarcia do dnia zaakceptowania przez Zamawiającego raportu końcowego z realizacji przedmiotu umowy.
2. Powierzający może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Procesor:
 - 1) przetwarza powierzone dane osobowe w sposób niezgodny z przepisami o ochronie danych osobowych lub niniejszą umową;
 - 2) nie wykona zaleceń, o których mowa w § 7 ust. 4.

§ 12.

1. Po zakończeniu świadczenia usług, o których mowa w § 1, w terminie 7 dni Procesor zwraca Powierzającemu wszelkie dane osobowe oraz usuwa wszelkie istniejące ich kopie z systemu informatycznego oraz ze wszystkich nośników, zarówno w wersji elektronicznej jak i papierowej.
2. W przypadku korzystania z usług Podwykonawcy, Procesor zapewnia realizację obowiązku, o którym mowa w ust. 1 przez Podwykonawcę.

§ 13.

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 dwóch jednobrzmiących egzemplarzach, po jednym dla każdej ze Stron.

Powierzający

Procesor

Załącznik 1 do Umowy o powierzenie przetwarzania danych osobowych

Zakres danych osobowych powierzonych do przetwarzania

Nazwa i adres Procesora

(miejsce i data)

Zakres danych osobowych przetwarzanych w projekcie w ramach organizowanych spotkań networkingowych

1.	Imię
2.	Nazwisko
3.	Miejsce pracy-Instytucja
4.	Stanowisko
5.	Telefon kontaktowy
6.	Adres e-mail

Załącznik 2 do Umowy o powierzenie przetwarzania danych osobowych

Wzór upoważnienia do przetwarzania danych osobowych na poziomie Procesora i podmiotów przez niego umocowanych**Upoważnienie nr
do przetwarzania danych osobowych**

Z dniemr. na podstawie art. 29 w związku z art. 28 rozporządzenia 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.), zwanego dalej RODO, upoważniam Pana/Panią* do przetwarzania danych osobowych w zbiorach: RPO WM 2014-2020, CST i Zbiorze danych osobowych przetwarzanych w projekcie w ramach organizowanych spotkań networkingowych. Upoważnienie wygasa z chwilą ustania Pana/Pani* zatrudnienia w /zaprzestania wykonywania przez Pana/Panią* zadań na podstawie stosunku cywilnoprawnego*, lub z chwilą jego odwołania.

.....
(czytelny podpis osoby upoważnionej do
wydawania i odwoływania upoważnień)

Oświadczam, że zapoznałem/am się z przepisami powszechnie obowiązującymi dotyczącymi ochrony danych osobowych, w tym RODO, a także z obowiązującym w opisem technicznych i organizacyjnych środków zapewniających ochronę i bezpieczeństwo przetwarzania danych osobowych i zobowiązuję się do przestrzegania zasad przetwarzania danych osobowych określonych w tych dokumentach.

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie zatrudnienia w / wykonywania zadań na podstawie stosunku cywilnoprawnego*, jak też po jego ustaniu/po zrealizowaniu zadań wykonywanych na podstawie stosunku cywilnoprawnego*.

.....
(czytelny podpis osoby składającej
oświadczenie)

Upoważnienie otrzymałem/am

.....
(miejscowość, data, podpis)

*niepotrzebne skreślić

Załącznik 3 do Umowy o powierzenie przetwarzania danych osobowych

**Wzór odwołania upoważnienia do przetwarzania danych osobowych na poziomie
Procesora i podmiotów przez niego umocowanych****Odwołanie upoważnienia nr
do przetwarzania danych osobowych**

Z dniem r., na podstawie na podstawie art. 29 w związku z art. 28 rozporządzenia 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) (Dz. Urz. UE L 119 z 4.05.2016, str. 1, z późn. zm.), odwołuję upoważnienie Pana/Pani* do przetwarzania powierzonych do przetwarzania danych osobowych nr..... wydane w dniur.

.....
(czytelny podpis osoby, upoważnionej do wydawania i odwoływania upoważnień)

.....
(miejscowość, data)

*niepotrzebne skreślić

Załącznik 4 do Umowy o powierzenie przetwarzania danych osobowych

Wzór oświadczenia osoby fizycznej, której dane osobowe są przetwarzane w ramach Umowy.....**Oświadczenie osoby fizycznej, której dane osobowe są przetwarzane w ramach Umowy.....**

(obowiązek informacyjny realizowany w związku z art. 13 i art. 14 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679)

W związku z zawarciem Umowy nr oświadczam, że przyjmuję do wiadomości, iż:

1. Administratorem moich danych osobowych jest:
 - 1) Zarząd Województwa Mazowieckiego dla zbioru Regionalny Program Operacyjny Województwa Mazowieckiego na lata 2014-2020, stanowiący Instytucję Zarządzającą dla Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, z siedzibą w Warszawie, ul. Jagiellońskiej 26, 03-719 Warszawa;
 - 2) Minister właściwy do spraw rozwoju regionalnego dla zbioru centralny system teleinformatyczny wspierający realizację programów operacyjnych, z siedzibą w Warszawie, ul. Wspólna 2/4, 00-926 Warszawa.
2. Podstawę prawną przetwarzania moich danych osobowych stanowi art. 6 ust. 1 lit. c rozporządzenia 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) (Dz. Urz. UE. L 119 04.05.2016, str. 1, z późn. zm.) – dane osobowe są niezbędne dla realizacji Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020:
 - 1) w odniesieniu do zbioru Regionalny Program Operacyjny Województwa Mazowieckiego na lata 2014-2020:
 - a) rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylające rozporządzenie Rady (WE) nr 1083/2006;
 - b) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1301/2013 z dnia 17 grudnia 2013 r. w sprawie przepisów szczegółowych dotyczących Europejskiego Funduszu Rozwoju Regionalnego i celu „Inwestycje na rzecz wzrostu i zatrudnienia” oraz w sprawie uchylenia rozporządzenia (WE) nr 1080/2006;
 - c) ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki

sójności finansowanych w perspektywie finansowej 2014–2020 (Dz. U. z 2018 r. poz. 1431);

- 2) w odniesieniu do zbioru centralny system teleinformatyczny wspierający realizację programów operacyjnych:
 - a) rozporządzenia Parlamentu Europejskiego i Rady (UE) Nr 1303/2013 z dnia 17 grudnia 2013 r. ustanawiające wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności, Europejskiego Funduszu Rolnego na rzecz Rozwoju Obszarów Wiejskich oraz Europejskiego Funduszu Morskiego i Rybackiego oraz ustanawiające przepisy ogólne dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego, Funduszu Spójności i Europejskiego Funduszu Morskiego i Rybackiego oraz uchylające rozporządzenie Rady (WE) nr 1083/2006;
 - b) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1301/2013 z dnia 17 grudnia 2013 r. w sprawie przepisów szczegółowych dotyczących Europejskiego Funduszu Rozwoju Regionalnego i celu „Inwestycje na rzecz wzrostu i zatrudnienia” oraz w sprawie uchylecia rozporządzenia (WE) nr 1080/2006;
 - c) ustawy z dnia 11 lipca 2014 r. o zasadach realizacji programów w zakresie polityki spójności finansowanych w perspektywie finansowej 2014–2020;
 - d) rozporządzenia Wykonawczego Komisji (UE) Nr 1011/2014 z dnia 22 września 2014 r. ustanawiające szczegółowe przepisy wykonawcze do rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1303/2013 w odniesieniu do wzorów służących do przekazywania Komisji określonych informacji oraz szczegółowe przepisy dotyczące wymiany informacji między beneficjentami a instytucjami zarządzającymi, certyfikującymi, audytowymi i pośredniczącymi.
3. Moje dane osobowe będą przetwarzane wyłącznie w celu realizacji Umowy nr, w szczególności
4. Moje dane osobowe zostały powierzone do przetwarzania Instytucji Pośredniczącej – Mazowieckiej Jednostce Wdrażania Programów Unijnych, ul. Jagiellońska 74, 03-301 Warszawa, Beneficjentowi realizującemu Projekt grantowy – Województwu Mazowieckiemu, ul. Jagiellońska 26, 03-719 Warszawa, oraz podmiotom, które na zlecenie Beneficjenta uczestniczą w realizacji Projektu grantowego Grantobiorcy i jednostki współpracujące z Beneficjentem przy realizacji zadań projektu. Moje dane osobowe mogą zostać przekazane podmiotom realizującym badania ewaluacyjne na zlecenie Instytucji Zarządzającej, Instytucji Pośredniczącej lub Beneficjenta. Moje dane osobowe mogą zostać również powierzone specjalistycznym firmom, realizującym na zlecenie Instytucji Zarządzającej, Instytucji Pośredniczącej oraz Beneficjenta kontrole i audyt w ramach Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020, innym podmiotom uprawnionym na podstawie przepisów prawa oraz podmiotom świadczącym obsługę administracyjno-organizacyjną Instytucji Zarządzającej, Instytucji Pośredniczącej lub Beneficjenta.
5. Podanie danych jest warunkiem koniecznym zawarcia Umowy nr, a odmowa ich podania jest równoznaczna z brakiem możliwości realizacji zadania na podstawie ww. umowy.

6. Moje dane osobowe nie będą przekazywane do państwa trzeciego lub organizacji międzynarodowej.
7. Moje dane osobowe nie będą poddawane zautomatyzowanemu podejmowaniu decyzji w sprawie indywidualnej.
8. Moje dane osobowe będą przechowywane do czasu rozliczenia Regionalnego Programu Operacyjnego Województwa Mazowieckiego na lata 2014-2020 oraz zakończenia archiwizowania dokumentacji.
9. Mogę skontaktować się z Inspektorem Ochrony Danych wysyłając wiadomość na adres poczty elektronicznej: iod@mazovia.pl.
10. Mam prawo do wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych.
11. Mam prawo żądać dostępu do treści swoich danych, ich sprostowania, ograniczenia przetwarzania oraz usunięcia.

.....
Miejscowość i data

.....
Czytelny podpis osoby fizycznej, której dane są przetwarzane w ramach Projektu grantowego

**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 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.

§ 3.

Elementy zawiadomienia

1. Zawiadomienie, o którym mowa w § 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 § 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 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

☐ Oficjalne dokumenty

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

☐ 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

☐ 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.