



Fundusze Europejskie
dla Mazowsza



Rzeczpospolita
Polska

Dofinansowane przez
Unię Europejską



Mazowsze.
serce Polski

Umowa powierzenia przetwarzania danych osobowych

zawarta (DD-MM-RRRR) w Warszawie pomiędzy:

Województwem Mazowieckim z siedzibą w Warszawie 03-719, ul. Jagiellońska 26, 03-719 Warszawa, w imieniu którego na podstawie uchwały nr działają:

...

- Administratorem Danych Osobowych, zwanym dalej: **Administratorem**,

a

(NAZWA) z siedzibą w (MIEJSCOWOŚĆ, KOD, ULICA, NR), reprezentowanym/ną przez: (IMIĘ, NAZWISKO ORAZ STANOWISKO) – Podmiot przetwarzający, zwanym/ną dalej: **Procesorem**

Niniejsza umowa zostaje zawarta w związku z zawarciem umowy nr dotyczącej usługi zaprojektowania oraz obsługi systemu informatycznego wspomagającego nabór i obsługę wniosków stypendialnych w ramach projektów "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 – RWS" oraz "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 – RMR".

W niniejszej umowie zastosowano następujący skrót:

- 1) rozporządzenie - rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych);
- 2) naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
- 3) Administrator – osoba fizyczna lub prawna, organ publiczny, jednostka lub innym podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych;
- 4) Podmiot przetwarzający (Procesor) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora.

§ 1.

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

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

§ 2.

1. Na mocy niniejszej umowy Procesor będzie przetwarzał dane:

1) **uczniów** w zakresie danych zwykłych:

- a) imion i nazwiska;
- b) etapu edukacyjnego (klasa);
- c) kierunku rozwoju zawodowego;
- d) uzdolnień;
- e) zainteresowań, kompetencji i umiejętności;
- f) osiągnięć i możliwości (w tym nagrody, wyróżnienia, uczestnictwo w konkursach, olimpiadach i turniejach, certyfikaty językowe, inne);
- g) działań podejmowanych w ramach kierunku rozwoju oraz w kierunku osiągnięcia celu i rezultatów Planu Rozwoju Kompetencji;
- h) wydatków w ramach Planu Rozwoju Kompetencji;
- i) przedmiotów w ramach których będzie realizowany Plan Rozwoju Kompetencji;
- j) celów Planu Rozwoju Kompetencji;
- k) ocen/średnich ocen;
- l) wykształcenia;
- m) wyników egzaminu na zakończenie szkoły;
- n) planowanych kierunków studiów;
- o) miejsca nauki;
- p) adresu zamieszkania;
- q) PESEL;
- r) dochodu ucznia/członka rodziny ucznia oraz danych, które widnieją na dokumentach poświadczających osiągnięte dochody ucznia/członka rodziny ucznia;
- s) informacja o rachunku bankowym;
- t) obszaru dotyczącego adresu zamieszkania wg stopnia urbanizacji DEGURBA;
- u) numeru telefonu;
- v) adresu e-mail;
- w) daty urodzenia;
- x) uczestnictwa w projekcie w poprzednich latach szkolnych oraz pobierania stypendium na cele edukacyjne współfinansowanego ze środków unijnych;
- y) imion, nazwiska oraz adresu zamieszkania osoby udostępniającej rachunek bankowy na potrzeby wypłaty stypendium;
- z) statusu rodziny niepełnej, przebywaniu w pieczy zastępczej lub posiadaniu statusu osoby usamodzielnianej opuszczającej pieczę zastępczą;
- aa) statusu rodziny wielodzietnej;
- bb) informacji o statusie osoby na rynku pracy;
- cc) informacji o bezdomności lub dotknięciu wykluczeniem z dostępu do mieszkań;
- dd) numeru ID nadawanego przez system podczas rejestracji wniosku;
- ee) korzystania ze świadczeń z pomocy społecznej.

uczniów w zakresie szczególnych kategorii danych:

- a) informacji o byciu osobą posiadającą obywatelstwo kraju trzeciego, obcego pochodzenia (cudzoziemiec), przynależącą do mniejszości narodowej lub etnicznej;
- b) informacji o byciu migrantem;
- c) informacji o niepełnosprawności;
- d) informacji o specjalnych potrzebach rozwojowych i edukacyjnych uczniów.

2) **rodziców/opiekunów prawnych/członków rodziny uczniów** w zakresie danych zwykłych:

- a) imiona i nazwiska rodzica/opiekuna prawnego/członków rodziny;
- b) PESEL rodzica/opiekuna prawnego;
- c) adresu zamieszkania rodzica/opiekuna prawnego;
- d) stopnia pokrewieństwa;
- e) daty urodzenia członków rodziny ucznia;
- f) numeru telefonu (opcjonalnie) rodzica/opiekuna prawnego;
- g) adresu e-mail rodzica/opiekuna prawnego

3) **nauczycieli - opiekunów stypendystów** w zakresie danych zwykłych:

- a) imion i nazwisk;
- b) wykładanego przedmiotu;
- c) zawodu;
- d) numeru telefonu;
- e) adresu e-mail;

4) **pracowników Mazowieckiego Samorządowego Centrum Doskonalenia Nauczycieli oraz pracowników Departamentu Edukacji Publicznej i Sportu Urzędu Marszałkowskiego w Warszawie** w zakresie danych zwykłych:

- a) imion i nazwiska;
- b) adresu e-mail.

2. Dane osobowe powierzone przez Administratora będą przetwarzane przez Procesora wyłącznie w celu realizacji umowy Nr..... dotyczącej usługi zaprojektowania oraz obsługi systemu informatycznego wspomagającego nabór i obsługę wniosków stypendialnych w ramach projektów "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 – RWS" oraz "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 - RMR", do czasu zakończenia wyżej wymienionej umowy.

§ 3.

1. Procesor, uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zobowiązuje się do wdrożenia odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku.
2. W przypadku, gdy przetwarzanie obejmuje szczególne kategorie danych osobowych, Procesor stosuje dodatkowe zabezpieczenia tych danych.

3. W celu zapewnienia bezpieczeństwa danych osobowych procesor wdraża co najmniej środki techniczne i organizacyjne określone w załączniku nr 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.

1. *Procesor nie będzie korzystał z usług Dalszego podmiotu przetwarzającego. (jeżeli ma zastosowanie)*

§ 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 pomaga Administratorowi w realizacji postanowień art. 13 i 14 rozporządzenia poprzez udostępnianie osobom, których dane dotyczą klauzuli informacyjnej stanowiącej załącznik nr 2.
3. Procesor, uwzględniając charakter przetwarzania danych osobowych oraz dostępne mu informacje, pomaga Administratorowi wywiązać się z obowiązków określonych w art. 32-36 rozporządzenia.

§ 7.

1. Procesor udostępnia Administratorowi wszelkie informacje niezbędne do wykazania spełnienia obowiązków określonych w art. 28 rozporządzenia oraz umożliwia Administratorowi lub audytorowi upoważnionemu przez Administratora przeprowadzanie audytów i przyczynia się do nich.
2. Administrator informuje Procesora o terminie i zakresie audytu 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 3.
3. Zmiana instrukcji nie wymaga dla swojej ważności zmiany umowy a jedynie notyfikację ze strony Administratora.
4. Procesor niezwłocznie informuje Administratora o każdym postępowaniu administracyjnym lub sądowym dotyczącym powierzonych do przetwarzania danych osobowych, a także o każdej kontroli lub audycie dotyczącym tychże danych osobowych.
5. Procesor ponosi pełną odpowiedzialność za wszelkie szkody powstałe w związku z przetwarzaniem przez niego danych osobowych, w sposób niezgodny z rozporządzeniem, niniejszą umową lub zaleceniami, o których mowa w § 7 ust. 4 – poniesione przez Administratora, osoby, których dane zostały powierzone lub osoby trzecie.

§ 9.

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

§ 10.

1. Niniejsza umowa obowiązuje od dnia jej zawarcia do czasu zakończenia realizacji umowy Nr dotyczącej usługi zaprojektowania oraz obsługi systemu informatycznego wspomagającego nabór i obsługę wniosków stypendialnych w ramach projektów "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 – RWS" oraz "Mazowiecki program stypendialny dla uczniów szkół zawodowych 2024/2025 - RMR".
2. Administrator może rozwiązać niniejszą umowę ze skutkiem natychmiastowym, gdy Procesor:
 - a) nie wykona zaleceń, o których mowa w § 7 ust. 4;
 - b) przetwarza powierzone dane osobowe w sposób niezgodny z przepisami o ochronie danych osobowych lub niniejszą umową.

§ 11.

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

2. Procesor zapewnia realizację obowiązku, o którym mowa w ust. 1 przez Podwykonawcę. (jeżeli ma zastosowanie)

§ 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 trzech jednobrzmiących egzemplarzach: dwa dla Województwa oraz jeden dla Procesora/Umowę sporządzono w formie elektronicznej i podpisano przez Administratora i Procesora kwalifikowanym podpisem elektronicznym. Za datę podpisania umowy Administrator i Procesor uznają dzień złożenia podpisu przez ostatnią z osób podpisujących w imieniu Administratora lub Procesora.

Procesor

Województwo Mazowieckie

.....

.....

(podpis i data)

(podpis i data)

Funkcja

Funkcja

Województwo Mazowieckie

.....

(podpis i data)

Funkcja

Wykaz środków technicznych i organizacyjnych wdrożonych przez podmiot przetwarzający

Instrukcja dla osoby sporządzającej umowę¹:

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.
2. 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).
3. Przy opisywaniu środków technicznych i organizacyjnych należy wziąć pod uwagę charakter, zakres, cel i kontekst przetwarzania oraz ryzyko dla praw i wolności osób fizycznych.
4. 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);
 - 2) 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);
 - 3) 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);
 - 4) 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);
 - 5) 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);
 - 6) 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);
 - 7) Środki ochrony danych podczas przechowywania
(w ramach kategorii możemy opisać jakie zabezpieczenia będą stosowane podczas przechowywania danych np. zabezpieczone pomieszczenia, meble, infrastruktura IT);
 - 8) 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

¹ Usui instrukcję oraz przykłady ewentualnych środków po uzupełnieniu wykazu.

sposób miejsca przetwarzania będą zabezpieczone przed niekorzystnymi warunkami środowiskowymi np. nadmierna wilgotnością, pożarem, zalaniem itp.);

9) 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);

10) 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.);

11) Środki wewnętrznego zarządzania i kierowania w zakresie technologii informacji i bezpieczeństwa informatycznego

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

12) 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 postępowania, o których mowa w art. 40 RODO);

13) 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);

14) Środki mające na celu zapewnienie jakości danych

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

15) Środki mające na celu zapewnienie ograniczonego zatrzymywania danych

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

16) 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");

17) Środki mające na celu umożliwienie przenoszenia danych

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

18) Środki mające na celu zapewnienie usuwania danych

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

Klauzula informacyjna

W celu wykonania obowiązku nałożonego art. 13 RODO²⁾, w związku z art. 88 ustawy o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027³⁾, informujemy o zasadach przetwarzania Państwa danych osobowych:

1. Administratorem danych osobowych jest:
 - 1) Województwo Mazowieckie, w ramach którego działa Urząd Marszałkowski Województwa Mazowieckiego w Warszawie, Departament Edukacji Publicznej i Sportu, z siedzibą przy ul. Jagiellońskiej 26, 03-719 Warszawa – Beneficjent realizujący projekty „Mazowiecki program stypendialny dla uczniów szkół zawodowych – Region Warszawski Stołeczny” oraz „Mazowiecki program stypendialny dla uczniów szkół zawodowych – Region Mazowiecki Regionalny”, w ramach programu Fundusze Europejskie dla Mazowsza 2021-2027 (dalej: „FEM 2021-2027”);
 - 2) Mazowiecka Jednostka Wdrażania Programów Unijnych będąca Instytucją Pośredniczącą (dalej: „IP”) FEM 2021-2027, z siedzibą przy ul. Inflanckiej 4, 00-189 Warszawa;
 - 3) Zarząd Województwa Mazowieckiego będący Instytucją Zarządzającą (dalej: „IZ”) FEM 2021-2027, z siedzibą przy ul. Jagiellońskiej 26, 03-719 Warszawa.
2. Podstawę prawną przetwarzania danych osobowych stanowi art. 6 ust. 1 lit. c i e oraz art. 9 ust. 2 lit. a RODO. Podstawę prawną przetwarzania danych osobowych dla IP oraz IZ stanowi art. 6 ust. 1 lit. c i art. 9 ust. 2 lit. g RODO.
3. Dane osobowe będą przetwarzane w związku z realizacją programu Fundusze Europejskie dla Mazowsza 2021-2027, Priorytet VII „Fundusze Europejskie dla nowoczesnej i dostępnej edukacji na Mazowszu”, Działanie 7.2 „Wzmocnienie kompetencji uczniów” na podstawie:
 - 1) rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 2021/1060 z 24 czerwca 2021 r. ustanawiającego wspólne przepisy dotyczące Europejskiego Funduszu Rozwoju Regionalnego, Europejskiego Funduszu Społecznego Plus, Funduszu Spójności, Funduszu na rzecz Sprawiedliwej Transformacji i Europejskiego Funduszu Morskiego, Rybackiego i Akwakultury, a także przepisy finansowe na potrzeby tych funduszy oraz na potrzeby Funduszu Azylu, Migracji i Integracji, Funduszu Bezpieczeństwa Wewnętrznego i Instrumentu Wsparcia Finansowego na rzecz Zarządzania Granicami i Polityki Wizowej (Dz. Urz. UE L 231 z 30.06.2021, str. 159, z późn. zm.);
 - 2) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/1057 z dnia 24 czerwca 2021 r. ustanawiające Europejski Fundusz Społeczny Plus (EFS+) oraz uchylające rozporządzenie (UE) nr 1296/2013 (Dz. Urz. UE L 231 z 30.06.2021, str. 21, z późn. zm.);
 - 3) ustawy z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. poz. 1079), w szczególności art. 87-93.

²⁾ 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) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.).

³⁾ Ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz.U. poz. 1079).

4. Cel przetwarzania danych:
 - 1) dane osobowe będą przetwarzane w celu realizacji projektów „Mazowiecki program stypendialny dla uczniów szkół zawodowych – Region Warszawski Stołeczny” oraz „Mazowiecki program stypendialny dla uczniów szkół zawodowych – Region Mazowiecki Regionalny” dofinansowanych ze środków Unii Europejskiej w ramach programu Fundusze Europejskie dla Mazowsza 2021-2027, Priorytet VII „Fundusze Europejskie dla nowoczesnej i dostępnej edukacji na Mazowszu”, Działanie 7.2 „Wzmocnienie kompetencji uczniów”, w związku z realizacją FEM 2021-2027, w szczególności w celu monitorowania, sprawozdawczości, komunikacji, publikacji, ewaluacji, zarządzania finansowego, weryfikacji i audytów oraz do celów określania kwalifikowalności uczestników;
 - 2) podanie danych jest dobrowolne, ale konieczne do realizacji wyżej wymienionego celu. Odmowa ich podania jest równoznaczna z brakiem możliwości podjęcia stosownych działań. Niepodanie danych wskazanych we Wniosku o udzielenie pomocy stypendialnej jako dane obowiązkowe uniemożliwi otrzymanie wsparcia w ramach projektów.
5. Dane pozyskujemy bezpośrednio od osób, których one dotyczą, w szczególności od Wnioskodawców.
6. Dostęp do Państwa danych osobowych mają pracownicy i współpracownicy Administratora, podmioty, które na zlecenie Beneficjenta uczestniczą w realizacji projektów – Mazowieckie Samorządowe Centrum Doskonalenia Nauczycieli, ul. Świętojerska 9, 00-236 Warszawa, Ośrodek Edukacji Informatycznej i Zastosowań Komputerów w Warszawie ul. Raszyńska 8/10, 02-026 Warszawa oraz *wykonawcy dostarczającego i utrzymującego system informatyczny do obsługi wniosków*. Ponadto Państwa dane osobowe mogą być powierzane lub udostępniane organom Komisji Europejskiej, ministrowi właściwemu do spraw rozwoju regionalnego, ministrowi właściwemu do spraw finansów publicznych oraz innym podmiotom upoważnionym na podstawie przepisów prawa. Dane osobowe mogą być również przekazane podmiotom realizującym określone zadania w ramach FEM 2021-2027 na zlecenie Instytucji Zarządzającej, Instytucji Pośredniczącej lub Beneficjenta oraz podmiotom wykonującym określone czynności powierzone przez Beneficjenta w ramach projektów, w tym podmiotom świadczącym obsługę administracyjno-organizacyjną Urzędu Marszałkowskiego Województwa Mazowieckiego w Warszawie.
7. Podanie danych osobowych dotyczących niepełnosprawności, statusie rodziny, przynależności do mniejszości narodowych lub etnicznych jest dobrowolne. Podstawę prawną przetwarzania tych danych osobowych stanowi art. 9 ust. 2 lit. a RODO. Dane te są zbierane w celu ustalenia kolejności Wnioskodawców na Liście rankingowej Wnioskodawców, którzy uzyskali jednakową liczbę punktów oraz w celu ustalenia spełnienia warunku dochodowego. Odmowa podania tych danych osobowych jest równoznaczna z brakiem możliwości zastosowania dodatkowych kryteriów, o których mowa w § 4 ust. 6 Regulaminu przyznawania pomocy stypendialnej dla uczniów szkół zawodowych w ramach programu Fundusze Europejskie dla Mazowsza 2021-2027 w roku szkolnym 2023/2024, ale nie ma wpływu na ubieganie się o przyznanie stypendium. Niepodanie danych o niepełnosprawności przy ustaleniu warunku dochodowego jest równoznaczne z brakiem możliwości zastosowania wyższego progu dochodowego, o którym mowa w § 3 ust. 1 pkt 4 Regulaminu przyznawania pomocy stypendialnej dla uczniów szkół zawodowych w ramach programu Fundusze Europejskie dla Mazowsza 2021-2027.
8. Dane osobowe są przechowywane przez okres niezbędny do realizacji celów określonych w punkcie 4.
9. Przysługują Państwu następujące prawa:
 - 1) prawo dostępu do swoich danych oraz otrzymania ich kopii (art. 15 RODO);

- 2) prawo do sprostowania swoich danych (art. 16 RODO);
 - 3) prawo do usunięcia swoich danych (art. 17 RODO) - jeśli nie zaistniały okoliczności, o których mowa w art. 17 ust. 3 RODO;
 - 4) prawo do żądania od administratora ograniczenia przetwarzania swoich danych (art. 18 RODO);
 - 5) prawo do przenoszenia swoich danych (art. 20 RODO) - jeśli przetwarzanie odbywa się na podstawie umowy: w celu jej zawarcia lub realizacji (w myśl art. 6 ust. 1 lit. b RODO), oraz w sposób zautomatyzowany;
 - 6) prawo wniesienia skargi do organu nadzorczego, którym jest Prezes Urzędu Ochrony Danych Osobowych na adres: ul. Stawki 2, 00-193 Warszawa (art. 77 RODO) - w przypadku, gdy osoba uzna, iż przetwarzanie jej danych osobowych narusza przepisy RODO lub inne krajowe przepisy regulujące kwestię ochrony danych osobowych, obowiązujące w Polsce;
 - 7) w zakresie danych przetwarzanych na podstawie zgody – prawo do cofnięcia zgody w dowolnym momencie, co pozostanie jednak bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody, przed jej wycofaniem.
10. Dane nie będą przetwarzane w sposób zautomatyzowany, w celu podjęcia decyzji w sprawie indywidualnej, w tym nie będą podlegały profilowaniu i nie będą przekazywane do państwa trzeciego.
11. Kontakt z administratorem danych i Inspektorem Ochrony Danych:
- 1) Jeśli mają Państwo pytania dotyczące przetwarzania danych przez Województwo Mazowieckie – Beneficjenta projektów, prosimy kontaktować się pod adresem: Urząd Marszałkowski Województwa Mazowieckiego w Warszawie, ul. Jagiellońska 26, 03-719 Warszawa, tel. (22) 5979-100, email: urząd_marszalkowski@mazovia.pl, ePUAP: /umwm/SkrytkaESP. Administrator wyznaczył inspektora ochrony danych (IOD), z którym można skontaktować się pod adresem e-mail: iod@mazovia.pl;
 - 2) Jeśli mają Państwo pytania dotyczące przetwarzania danych przez Instytucję Pośredniczącą tj. Mazowiecką Jednostkę Wdrażania Programów Unijnych w ramach FEM 2021-2027, prosimy kontaktować się z Inspektorem Ochrony Danych (IOD) w następujący sposób: pocztą tradycyjną na adres: ul. Inflanckiej 4, 00-189 Warszawa, elektronicznie: na adres e-mail: iod@mazowia.eu;
 - 3) Jeśli mają Państwo pytania dotyczące przetwarzania danych przez Instytucję Zarządzającą FEM 2021-2027, prosimy kontaktować się pod adresem: Urząd Marszałkowski Województwa Mazowieckiego w Warszawie, ul. Jagiellońska 26, 03-719 Warszawa, tel. (22) 5979-100, email: urząd_marszalkowski@mazovia.pl, ePUAP: /umwm/SkrytkaESP. Administrator wyznaczył inspektora ochrony danych (IOD), z którym można skontaktować się pod adresem e-mail: iod@mazovia.pl.

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,
 - c) 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.

§ 3 Elementy zawiadomienia

1. Zawiadomienie, o którym mowa w § 2 ust. 1 pkt 2, musi zawierać co najmniej:
 - 1) wyraźne wskazanie, że dane osobowe, których poufność, integralność lub dostępność została naruszona, są danymi osobowymi przetwarzanymi w imieniu Administratora Danych Osobowych, o którym mowa w § 1;
 - 2) elementy określone w art. 33 ust. 3 RODO:
 - a) charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

- b) imię i nazwisko oraz dane kontaktowe osoby, od której można uzyskać więcej informacji,
 - c) możliwe konsekwencje naruszenia ochrony danych osobowych,
 - d) środki zastosowane lub proponowane przez podmiot przetwarzający w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków;
- 3) informacje umożliwiające określenie czy naruszenie skutkuje wysokim ryzykiem naruszenia praw lub wolności osób fizycznych;
 - 4) w przypadku wysokiego ryzyka naruszenia praw lub wolności osób fizycznych wykaz osób, których to naruszenie dotyczyło wraz z danymi umożliwiającymi ich powiadomienie o naruszeniu ochrony danych osobowych;
 - 5) w przypadku naruszenia ochrony danych osobowych niepodlegającego zgłoszeniu do organu nadzoru informacje umożliwiające określenie czy naruszenie wiąże się z brakiem ryzyka lub małym prawdopodobieństwem naruszenia praw i wolności osób fizycznych;
 - 6) w przypadku naruszenia terminu, o którym mowa w § 2 ust. 2, wyjaśnienie przyczyn opóźnienia.
2. Elementy określone w ust. 1 pkt 2-5 należy przesłać poprzez wypełnienie tabeli określonej w załączniku do instrukcji.

§ 4 Ocena zawiadomienia

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

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

Zgłoszenie naruszenia ochrony danych osobowych

1. Czas naruszenia

A. Wykrycie naruszenia i powiadomienie organu nadzorczego

Data stwierdzenia naruszenia

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

Kliknij tutaj, aby wprowadzić datę.

Sposób stwierdzenia naruszenia

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

Kliknij tutaj, aby wprowadzić tekst.

Data powiadomienia przez podmiot przetwarzający
(opcjonalnie)

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Powody opóźnienia powiadomienia organu nadzorczego o naruszeniu

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

Kliknij tutaj, aby wprowadzić tekst.

B. Czas naruszenia

Data i czas zaistnienia/rozpoczęcia naruszenia

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

Trwające naruszenie

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

Data i czas zakończenia naruszenia

(opcjonalnie)

Jeśli nie znasz dokładnego terminu, podaj czas przybliżony.

Kliknij tutaj, aby wprowadzić tekst.

C. Komentarz do czasu naruszenia (opcjonalnie)

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

Kliknij tutaj, aby wprowadzić tekst.

2. Charakter naruszenia

A. Charakter

Naruszenie poufności danych

Nieuprawnione lub przypadkowe ujawnienie bądź udostępnienie danych

Naruszenie integralności danych

Wprowadzenie nieuprawnionych zmian podczas odczytu, zapisu, transmisji lub przechowywania

Naruszenie dostępności danych

Brak możliwości wykorzystania danych na żądanie, w założonym czasie, przez osobę do tego uprawnioną

B. Na czym polegało naruszenie?

Zgubienie lub kradzież nośnika/urządzenia

Dokumentacja papierowa (zawierająca dane osobowe) zgubiona, skradziona lub pozostawiona w niezabezpieczonej lokalizacji

Korespondencja papierowa utracona przez operatora pocztowego lub otwarta przed zwróceniem jej do nadawcy

Nieuprawnione uzyskanie dostępu do informacji

Nieuprawnione uzyskanie dostępu do informacji poprzez złamanie zabezpieczeń

Złośliwe oprogramowanie ingerujące w poufność, integralność i dostępność danych

Uzyskanie poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail czy komunikator internetowy (phishing)

Nieprawidłowa anonimizacja danych osobowych w dokumencie

Nieprawidłowe usunięcie/zniszczenie danych osobowych z nośnika/urządzenia elektronicznego przed jego zbyciem przez administratora

Niezamierzona publikacja

Dane osobowe wysłane do niewłaściwego odbiorcy

Ujawnienie danych niewłaściwej osoby

Ustne ujawnienie danych osobowych

Opisz szczegółowo na czym polegało naruszenie.

Kliknij tutaj, aby wprowadzić tekst.

C. Dzieci

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

D. Przyczyna naruszenia

Wewnętrzne działanie niezamierzone

Wewnętrzne działanie zamierzone

Zewnętrzne działanie niezamierzone

Zewnętrzne działanie zamierzone

Inne przyczyny (w tym nieznanne)

Kliknij tutaj, aby wprowadzić tekst.

2.1. Kategorie danych osobowych

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

A. Kategorie danych

Szczegółowy opis kategorii danych, których dotyczy naruszenie

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

Kliknij tutaj, aby wprowadzić tekst.

B. Dane podstawowe

Dane identyfikacyjne

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

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.

Wykaz podwykonawców przetwarzania

Administrator zezwolił na korzystanie z usług następujących podwykonawców przetwarzania:

- 1) Imię, nazwisko lub nazwa:
- 2) Adres:
- 3) Imię i nazwisko i dane kontaktowe osoby wyznaczonej do kontaktu:
- 4) *Opis przetwarzania (w tym wyraźnie rozgraniczenie obowiązków, jeżeli upoważnionych jest kilku podwykonawców przetwarzania tj. opis za jakie operacje przetwarzania odpowiada dany podwykonawca):