



Fundusze Europejskie
dla Kujaw i Pomorza

Dofinansowane przez
Unię Europejską



Samorząd Województwa
Kujawsko-Pomorskiego

POLITYKA BEZPIECZEŃSTWA

na cele realizacji Projektu SILVERS CLUB

realizowanego przez

Kujawsko-Pomorskie Centrum Edukacji Prawno-Obywatelskiej „PUBLICORUM”

z siedzibą w Bydgoszczy przy ul. Grunwaldzkiej 18A

Bydgoszcz, 01.10.2026 r.



Rozdział 1 – Postanowienia ogólne – słownik pojęć

Użyte w Polityce Bezpieczeństwa określenia:

- a) **Beneficjent** – Kujawsko-Pomorskie Centrum Edukacji Prawno-Obywatelskiej „PUBLICORUM”
- b) **Siedziba Beneficjenta** – Bydgoszcz, ul. Grunwaldzkiej 18A.
- c) **Projekt** – SILVERS CLUB w ramach Programu Regionalnego Fundusze Europejskie dla Kujaw i Pomorza 2021-2027 (FEKP), w ramach projektu “Wspieranie integracji społecznej LGD “Dwie Rzeki””
- d) **Administrator Danych** – Kujawsko-Pomorskie Centrum Edukacji Prawno-Obywatelskiej „PUBLICORUM” z siedzibą w Bydgoszczy, przy ul. Grunwaldzkiej 18a
- e) **Współadministratorzy:**
 - Zarząd Województwa Kujawsko-Pomorskiego pełniący funkcję Instytucji zarządzającej FEKP,
 - Minister właściwy ds. rozwoju regionalnego, pełniący funkcję Instytucji Koordynującej Umowę Partnerstwa,
 - Stowarzyszenie Bydgoska Lokalna Grupa Działania “Dwie Rzeki”.
- f) **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),
 - a) **ustawa** – ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U.2019 poz.1781),
 - b) **ustawa wdrożeniowa** – ustawa z dnia 28 kwietnia 2022 r. o zasadach realizacji zadań finansowanych ze środków europejskich w perspektywie finansowej 2021-2027 (Dz. U. 2022 poz. 1079),
 - c) **dostęp do danych osobowych zgodny z ustawą wdrożeniową** – dostęp do danych przysługujący zgodnie z art. 89 ustawy wdrożeniowej:
 - ministrowi właściwemu do spraw rozwoju regionalnego wykonującemu zadania państwa członkowskiego,
 - ministrowi właściwemu do spraw finansów publicznych,
 - instytucji zarządzającej,
 - instytucji audytowej,
 - Prezesowi Zakładu Ubezpieczeń Społecznych,
 - podmiotom związanym z realizacją zadań w ramach programu regionalnego, w szczególności zaangażowanym w proces audytu, ewaluacji, kontroli, oceny i ekspertyzy,
 - podmiotom, które wykonują usługi związane z obsługą i rozwojem systemów teleinformatycznych, a także zapewnieniem łączności, np. dostawcom rozwiązań IT i operatorom telekomunikacyjnym, operatorom pocztowym lub kurierskim w zakresie niezbędnym w celu prawidłowej realizacji projektu,
 - podmiotom, którym Beneficjent i w/w wymienione podmioty powierzają realizację zadań na podstawie odrębnej umowy, w zakresie niezbędnym do realizacji ich zadań wynikających z przepisów ustawy wdrożeniowej,
 - innym podmiotom upoważnionym na mocy prawa.
 - d) **użytkownik** – osoba upoważniona do przetwarzania danych osobowych w ramach Centralnego Systemu Teleinformatycznego CST2021,
 - e) **Centralny System Teleinformatyczny CST2021** – system teleinformatyczny wykorzystywany na potrzeby wdrażania funduszy strukturalnych w Polsce w perspektywie finansowej 2021-2027,
 - f) **Inspektor Ochrony Danych (dawniej Administrator Bezpieczeństwa Informacji)** – osoba wyznaczona przez Administratora Danych, odpowiedzialna za nadzór nad zapewnieniem bezpieczeństwa danych osobowych pełniąc zadania określone w art. 39 rozporządzenia,





- g) **Inspektor Ochrony Danych w projekcie (w skrócie: IOD w projekcie; dawniej Administrator Bezpieczeństwa Informacji w projekcie, w skrócie: ABI w projekcie)** – osoba wyznaczona przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta, odpowiedzialna za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w projekcie,
- h) **Administrator Systemu w projekcie** – osoba odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Inspektora Ochrony Danych w projekcie i powierzone przez osobę upoważnioną do podejmowania decyzji w projekcie innej osobie,
- i) **naruszenie zabezpieczenia** – naruszenie ochrony danych osobowych w rozumieniu art. 4 pkt. 12 rozporządzenia tj. 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,
- j) **dane osobowe** – dane osobowe w rozumieniu art. 4 pkt. 1 rozporządzenia tj. wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej,
- k) **przetwarzanie danych osobowych** – przetwarzanie w rozumieniu art. 4 pkt. 2 rozporządzenia tj. operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takich 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,
- l) **usuwanie danych osobowych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą,
- m) **zbiór danych osobowych** – zbiór danych w rozumieniu art. 4 pkt. 6 rozporządzenia tj. uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie,
- n) **zabezpieczenie danych osobowych** – środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawnionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą w tym środki o których mowa w art. 32 rozporządzenia,
- o) **pracownik Projektu** – osoba zaangażowana w realizację Projektu jako personel projektu lub stanowiąca kadrę zarządzającą Projektu
- p) **Polityka** – Polityka Bezpieczeństwa na cele realizacji Projektu.

Rozdział 2 – Zakres oraz zasady zabezpieczania danych osobowych

§ 1.

Niniejszą Politykę Bezpieczeństwa stosuje się do zbioru danych osobowych w odniesieniu do Projektu znajdującego się w Siedzibie Beneficjenta i pomieszczeniach, tworzących obszar, w którym są przetwarzane dane osobowe zgodnie z załącznikiem nr 1 do Polityki.



§ 2.

1. Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych.
2. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w Polityce oraz nad wykonywaniem zadań związanych z ochroną danych osobowych w Projekcie, sprawuje Inspektor Ochrony Danych w Projekcie.

§ 3.

Dane osobowe przetwarzane w Projekcie podlegają ochronie zgodnie z przepisami ustawy oraz rozporządzenia.

§ 4.

Przetwarzanie danych osobowych jest dopuszczalne wyłącznie w zakresie niezbędnym do aplikowania o środki europejskie i realizacji Projektu, w szczególności celu przeprowadzenia rekrutacji, potwierdzenia kwalifikowalności wydatków, udzielenia wsparcia, monitoringu, ewaluacji, kontroli, audytu i sprawozdawczości, działań informacyjno-promocyjnych i archiwizacji w ramach FEdKP.

§ 5.

Przetwarzanie danych osobowych nie może naruszać praw i wolności osób, których dane osobowe dotyczą.

§ 6.

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby Projektu bezpośrednio od osoby, której dane dotyczą, osoba ta zostanie poinformowana o zakresie danych i celu ich wykorzystania.

§ 7.

1. Jakiegokolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.
2. Wnioski o udostępnienie danych osobowych, po wstępnym rozpatrzeniu przez Inspektora Ochrony Danych, są rozpatrywane przez Beneficjenta.

§ 8.

1. Przetwarzanie danych osobowych może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 4, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia (w szczególności art. 28) oraz umowy o dofinansowanie Projektu.
2. Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych powinny zostać przed podpisaniem, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Inspektora Ochrony Danych w Projekcie.

§ 9.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane przez Beneficjenta są niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane przez Beneficjenta, Beneficjent jest zobowiązany do uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania przetwarzania kwestionowanych danych osobowych lub ich usunięcia, zgodnie z żądaniem osoby, której dane osobowe dotyczą.

Rozdział 3 – Obowiązki Inspektora Ochrony Danych u Beneficjenta



§ 10.

Inspektor Ochrony Danych w Projekcie poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych u Beneficjenta.

§ 11.

Do zadań Inspektora Ochrony Danych w Projekcie, wynikających z art. 39 rozporządzenia, należy w szczególności:

- a) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez: sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowanie w tym zakresie sprawozdania dla Administratora Danych, nadzorowanie opracowania i aktualizowania dokumentacji (zgodnie z załącznikami do niniejszej Polityki) oraz przestrzegania zasad w niej określonych, zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
- b) prowadzenie i aktualizacja rejestru zbiorów danych,
- c) prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w Projekcie, który stanowi załącznik nr 1 do Polityki,
- d) analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w Projekcie oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta,
- e) opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu wobec Beneficjenta,
- f) inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych w Projekcie.

§ 12.

W doborze i stosowaniu środków ochrony danych osobowych Inspektor Ochrony Danych w Projekcie zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 13.

1. Obowiązki Inspektora Ochrony Danych w Projekcie wykonywane są przez osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta.
2. Nadzór nad wykonywaniem obowiązków Inspektora Ochrony Danych w Projekcie i Administratora Systemu w projekcie pełni osoba upoważniona do podejmowania decyzji w imieniu Beneficjenta.

§ 14.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania u Beneficjenta danych osobowych, Inspektor Ochrony Danych w Projekcie konsultuje się i współpracuje z osobą upoważnioną do reprezentowania Beneficjenta.

§ 15.

Inspektor Ochrony Danych w Projekcie może być osoba, która:

- a) ma pełną zdolność do czynności prawnych oraz korzysta z pełni praw publicznych,
- b) posiada odpowiednią wiedzę w zakresie ochrony danych osobowych,
- c) nie była karana za umyślne przestępstwo.

Rozdział 4 – Przetwarzanie danych osobowych

§ 16.



1. Do przetwarzania danych osobowych w Projekcie mogą być dopuszczeni jedynie pracownicy Projektu posiadający odpowiednie upoważnienie wydane przez posiadającą umocowanie do tego osobę. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do niniejszej Polityki.
2. Każdy pracownik Projektu, przed dopuszczeniem go do przetwarzania danych osobowych musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką.
3. Pracownik Projektu potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych w Projekcie składając podpis pod informacją zawartą w upoważnieniu do przetwarzaniu danych osobowych.

§ 17.

1. Każdy pracownik Projektu mający dostęp do danych osobowych jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Beneficjenta.

§ 18.

1. Dopuszczenie do przetwarzania danych osobowych w Projekcie przez osoby niebędące pracownikami Projektu, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Inspektora Ochrony Danych w Projekcie oraz uzyskaniu odpowiedniego upoważnienia.
2. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 19.

Wszyscy pracownicy Projektu oraz osoby, o których mowa w § 18, pod groźbą sankcji dyscyplinarnych, mają obowiązek zachowania tajemnicy o przetwarzanych danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 20.

Pracownicy Projektu (oraz osoby o których mowa w § 18) są w szczególności zobowiązani do:

- a) bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji, określonych w Polityce i innych procedurach,
- b) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach (lub wyznaczonych ich częściach), służbowych
- c) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce,
- d) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie,
- e) nieudzielania informacji o danych osobowych innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,
- f) bezwzględnego zawiadamiania Inspektora Ochrony Danych w Projekcie o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 21.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 2 do Polityki.



Rozdział 5 – Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 22.

Za naruszenie ochrony danych osobowych uznaje się w szczególności przypadki, gdy:

- a) stwierdzono naruszenie zabezpieczenia systemu informatycznego dedykowanego przetwarzaniu danych,
- b) stan sprzętu komputerowego, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakość komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych,
- c) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych.

§ 23.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Inspektora Ochrony Danych w Projekcie.
2. Inspektor Ochrony Danych w Projekcie, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
 - a) poinformować pisemnie o zaistniałym zdarzeniu Administratora Danych oraz Beneficjenta i stosować się do zaleceń,
 - b) zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a w szczególności dokładny czas uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu.
3. Inspektor Ochrony Danych w Projekcie, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych jest zobowiązany niezwłocznie:
 - a) wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać,
 - b) przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby niepowołanej do danych osobowych w systemie informatycznym służącym przetwarzaniu danych osobowych,
 - c) podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem ślady naruszenia ochrony danych osobowych, w szczególności przez:
 - fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
 - wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu,
 - d) szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych,
 - e) przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
4. Czynności opisane w ust. 3 wykonuje Administrator Systemu w Projekcie.

§ 24.

1. Po przywróceniu normalnego stanu systemu informatycznego należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.





2. Jeżeli przyczyną zdarzenia był błąd użytkownika, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych osobowych.
3. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym niebezpiecznym oprogramowaniem, należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne, wykluczające powtórzenie się podobnego zdarzenia w przyszłości.
4. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z przepisów prawa pracy oraz wewnętrznych uregulowań u Beneficjenta, a w przypadku gdy użytkownik nie jest pracownikiem Projektu, konsekwencje wynikające z umowy, o której mowa w § 18 ust. 1.

§ 25.

1. Inspektor Ochrony Danych w Projekcie przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia przekazuje go Administratorowi Danych.
2. Jeżeli naruszenie zabezpieczenia nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych Inspektor Ochrony Danych w Projekcie przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu w Projekcie.
3. W przypadku naruszenia zabezpieczenia Inspektor Ochrony Danych dokonuje analizy zasadności dokonania zgłoszenia, o którym mowa w art. 33 rozporządzenia.

Rozdział 6 – Kontrola nad przestrzeganiem ochrony danych osobowych

§ 26.

1. Bieżąca kontrola nad przetwarzaniem danych osobowych w Projekcie jest dokonywana przez Inspektora Ochrony Danych w Projekcie.
2. W ramach kontroli, o której mowa w ust. 1 Inspektor Ochrony Danych w Projekcie jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki.

§ 27.

1. Inspektor Ochrony Danych w Projekcie przeprowadza raz w roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.
2. Przygotowując raport, o którym mowa w ust. 1, Inspektor Ochrony Danych w Projekcie uwzględnia informacje zawarte w raportach, o których mowa w § 25.

§ 28.

Kontrola, o której mowa w § 27, polega w szczególności na sprawdzeniu:

- a) którzy pracownicy Projektu mają dostęp do danych osobowych,
- b) czy dane osobowe nie zostały udostępnione nieupoważnionym osobom,
- c) czy pracownicy Projektu i inne osoby mające dostęp do danych osobowych przetwarzanych w Projekcie posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 7 – Postanowienia końcowe

§ 29.

Polityka jest dokumentem wewnętrznym Beneficjenta i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.

§ 30.

Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych.



§ 31.

1. Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia przetwarzania danych osobowych w Projekcie.
2. Polityka obowiązuje od dnia rozpoczęcia realizacji Projektu.

§ 32.

1. Wykazy i rejestry znajdujące się w załącznikach do Polityki, prowadzi Inspektor Ochrony Danych w Projekcie.
2. Wykaz znajdujący się w załączniku nr 2 do Polityki prowadzi w zakresie środków organizacyjnych Inspektor Ochrony Danych w Projekcie, zaś w zakresie środków technicznych Administrator Systemu w Projekcie.

§ 33.

Integralną część niniejszej Polityki stanowią następujące załączniki:

- Załącznik nr 1 Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe
- Załącznik nr 2 Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w Projekcie
- Załącznik nr 3 Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w Projekcie



Załącznik nr 1 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe

Lp.	Adres	Pomieszczenie
1.	adres – Młyny Rothera , ul. Mennica 10	Salę zajęć
2.	adres – Młyny Rothera , ul. Mennica 10; ul. Grunwaldzka 18A, 85-236 Bydgoszcz	Biuro Projektu



Załącznik nr 2 – Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w Projekcie

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych

1. Środki ochrony fizycznej danych:

- a) klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym,
- b) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz,
- c) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do likwidacji, pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie,
- d) urządzenia, dyski lub inne informatyczne nośniki, zawierające dane osobowe przeznaczone do przekazania innemu podmiotowi, nieuprawnionemu do otrzymywania danych osobowych, pozbawia się wcześniej zapisu tych danych,
- e) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie,
- f) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej szafie,
- g) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

2. Środki sprzętowe, informatyczne i telekomunikacyjne:

- a) sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby Beneficjenta,
- b) oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, robaki komputerowe, oprogramowanie szpiegujące i kradnące hasła oraz inne niebezpieczne oprogramowanie,
- c) dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła,
- d) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła i jeśli to możliwe za pomocą dodatkowego czynnika uwierzytelnienia,
- e) zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

3. Środki organizacyjne:

- a) osoby zaangażowane przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych,
- b) osoby zaangażowane przy przetwarzaniu danych osobowych zostały zobowiązane do zachowania ich w tajemnicy,
- c) monitory komputerów, na których są przetwarzane dane osobowe ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane,
- d) kopie zapasowe zbioru danych osobowych są przechowywane w innym pomieszczeniu niż to, w którym znajduje się komputer, na którym dane osobowe są przetwarzane na bieżąco.



Fundusze Europejskie
dla Kujaw i Pomorza

Dofinansowane przez
Unię Europejską



Samorząd Województwa
Kujawsko-Pomorskiego

Załącznik nr 3 – Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w Projekcie

Przekazywane drogą elektroniczną (poza Centralnym Systemem Informatycznym CST2021) dane osobowe powinny zostać uprzednio skompresowane do jednego z formatów: ZIP, TAR, GZ lub RAR oraz zabezpieczone hasłem z wykorzystaniem programu 7-Zip lub WinRAR przed przekazaniem. Hasło, przy użyciu którego zostaną zabezpieczone dane, powinno zostać przekazane do podmiotu/użytkownika, do którego dane będą kierowane w odrębnej formie niż dane osobowe.