

**POLITYKA BEZPIECZEŃSTWA PROJEKTU
pn. „Nasi Mistrzowie”**

**Realizowanego z środków
EUROPEJSKIEGO FUNDUSZU SPOŁECZNEGO
W RAMACH RPO WD 2014-2020**

u Beneficjenta RPO WD 2014-2020

Rozdział 1 Postanowienia ogólne

§ 1.

Na podstawie:

- ✓ 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)
- ✓ Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);

przyjmuje się Politykę Bezpieczeństwa dla Projektu „Nasi Mistrzowie” RPO WD 2014-2020, zwaną dalej „Polityką”, określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorze danych osobowych uczestników projektu oraz w systemie SL2014 w ramach realizowanego projektu pn. „Nasi Mistrzowie”

§ 2.

Użyte w Polityce określenia oznaczają:

- 1) **Administrator Danych** - Instytucję Zarządzającą RPO WD;
- 2) **ustawa** - ustawę z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.);
- 3) **rozporządzenie** - rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024);
- 4) **użytkownik** - osobę upoważnioną do przetwarzania danych osobowych w systemie SL 2014;
- 5) **Administrator Bezpieczeństwa Informacji** - osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL 2014;

- 6) **Administrator Bezpieczeństwa Informacji SL 2014 w IP** - osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL 2014w IP;
- 7) **Administrator Bezpieczeństwa Informacji SL 2014u Beneficjenta** - osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL 2014u Beneficjenta;
- 8) **Administrator Systemu u Beneficjenta** - osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych w SL2014u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;
- 9) **naruszenie zabezpieczenia SL 2014** - jakiegokolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności SL 2014;
- 10) **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
- 11) **przetwarzanie danych osobowych** - jakiegokolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
- 12) **usuwanie danych osobowych** - zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
- 13) **zbiór danych osobowych** - posiadający strukturę zestaw danych o charakterze danych osobowych, które są dostępne według określonych kryteriów, niezależnie od tego czy zestaw ten jest rozproszony lub podzielony funkcjonalnie;

- 14) 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;
- 15) Instrukcja** - Instrukcję Zarządzania Systemem Informatycznym dla systemu Podsystem Monitorowania Europejskiego Funduszu Społecznego 2007 u Beneficjenta;
- 16) Pracownik** - osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub innego stosunku prawnego;
- 17) Ministerstwo** - Ministerstwo Infrastruktury i Rozwoju

Rozdział 2

Zakres oraz zasady zabezpieczania danych osobowych

§ 3.

Niniejszą politykę stosuje się do zbioru danych osobowych SL2014znajdującego się u Beneficjenta.

§ 4.

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 Instrukcji, oraz nad wykonywaniem zadań związanych z ochroną danych osobowych w SL2014u Beneficjenta, sprawuje Administrator Bezpieczeństwa Informacji SL2014 u Beneficjenta.

§ 5.

Dane osobowe przetwarzane w SL2014podlegają ochronie zgodnie z przepisami ustawy.

§ 6.

Przetwarzanie danych osobowych w SL2014jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach RPO WD 2014-2020

§ 7.

Przetwarzanie danych osobowych w SL2014nie może naruszać praw i wolności osób, których dane osobowe dotyczą, a w szczególności zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność wyznaniową, partyjną lub związkową, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń

wydanym w postępowaniu sądowym lub administracyjnym.

§ 8.

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby SL2014 bezpośrednio od osoby, której dane dotyczą, osoba zbierająca dane osobowe jest zobowiązana do przekazania tej osobie informacji o:

- 1) pełnej nazwie Ministerstwa oraz jego adresie;
- 2) celu zbierania danych osobowych;
- 3) prawie dostępu do treści swoich danych osobowych oraz ich poprawiania;
- 4) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym w ramach RPO WD 2014-2020

§ 9.

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 przetwarzanych w SL2014, po wstępnym rozpatrzeniu przez Administratora Bezpieczeństwa Informacji, są rozpatrywane przez Administratora Danych.

§ 10.

1. Przetwarzanie danych osobowych znajdujących się w SL2014 może zostać powierzone innemu podmiotowi, wyłącznie w celu określonym w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy lub porozumienia, w pełni respektujących przepisy ustawy, rozporządzenia oraz umowy o dofinansowanie projektu.

§ 11.

Każdej osobie, której dane osobowe są przetwarzane w SL2014 przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:

- 1) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych;
- 2) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
- 3) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
- 4) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
- 5) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
- 6) żądania uzupełnienia, uaktualnienia, sprostowania danych osobowych, czasowego lub stałego wstrzymania ich przetwarzania lub ich usunięcia, jeżeli są one niekompletne, nieaktualne, nieprawdziwe lub zostały zebrane z naruszeniem ustawy albo są już zbędne do realizacji celu, dla którego zostały zebrane.

§ 12.

Na wniosek osoby, której dane osobowe dotyczą, Beneficjent jest zobowiązany, w terminie maksymalnie 30 dni od dnia wpłynięcia wniosku do Beneficjenta, wskazać w powszechnie zrozumiałej formie:

- 1) jakie dane osobowe dotyczące zapytującej osoby są przetwarzane przez Beneficjenta w SL2014;
- 2) w jaki sposób zebrano te dane osobowe;
- 3) w jakim celu i zakresie te dane osobowe są przetwarzane;
- 4) od kiedy są przetwarzane te dane osobowe;

5) w jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§ 13.

W razie wykazania przez osobę, której dane osobowe dotyczą, że jej dane osobowe, przetwarzane przez Beneficjenta w SL2014 są niekompletne, nieaktualne, nieprawdziwe, lub zostały zebrane z naruszeniem ustawy albo są zbędne do realizacji celu, w jakim zostały zebrane, 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 4

Obowiązki Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta

§ 14.

Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych w SL2014u Beneficjenta.

§ 15.

Do zadań Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta należy w szczególności:

- 1) współdziałanie z Administratorem Bezpieczeństwa Informacji SL2014 w IP w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z ustawy i rozporządzenia;
- 2) prowadzenie i aktualizacja rejestru, o którym mowa w § 20, który stanowi załącznik nr 1 do Polityki;
- 3) prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe w SL2014u Beneficjenta, który stanowi załącznik nr 2 do Polityki;
- 4) analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach SL2014u Beneficjenta oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta;
- 5) opiniowanie umów, których przedmiotem jest powierzenie przetwarzania danych osobowych w SL2014u podmiotowi zewnętrznemu wobec Beneficjenta;
- 6) inicjowanie szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych w SL2014u Beneficjenta.

§ 16.

W doborze i stosowaniu środków ochrony danych osobowych w SL2014 Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 17.

1. Obowiązki Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta Pracownika.
2. Nadzór nad wykonywaniem obowiązków Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta i, o ile został powołany, Administratora Systemu u Beneficjenta pełni osoba upoważniona do podejmowania decyzji w imieniu Beneficjenta.

§ 18.

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania u Beneficjenta danych osobowych w SL2014, Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta konsultuje się i współpracuje z Administratorem Bezpieczeństwa Informacji SL2014w IP.

Rozdział 5 Przetwarzanie danych osobowych

§ 19.

1. Do przetwarzania danych osobowych w SL2014 mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do umowy o dofinansowanie projektu.
2. Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych w SL2014, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją.
3. Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta, której wzór jest określony w załączniku nr 3 do Polityki.

§ 20.

1. Każdy pracownik mający dostęp do danych osobowych w SL2014 jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji SL2014 u Beneficjenta.
2. Rejestr, o którym mowa w ust. 1, zawiera:
 - 1) imię i nazwisko pracownika;
 - 2) jego identyfikator w systemie informatycznym służącym przetwarzaniu danych w SL2014;
 - 3) zakres przydzielonego uprawnienia;
 - 4) datę przyznania uprawnień;
 - 5) podpis Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta potwierdzający przyznanie uprawnień;
 - 6) datę odebrania uprawnień
 - 7) podpis Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta potwierdzający odebranie uprawnień.

§ 21.

1. Dopuszczenie do przetwarzania danych osobowych znajdujących się w SL2014 przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta oraz podpisaniu z tą osobą umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku § 19 i 20 stosuje się odpowiednio.
2. Osoby trzecie mogą przebywać na obszarze, w którym są przetwarzane dane osobowe jedynie w obecności co najmniej jednego użytkownika posiadającego uprawnienia do przetwarzania danych osobowych.

§ 22.

Wszyscy pracownicy oraz osoby, o których mowa w § 21 ust. 1, pod groźbą sankcji dyscyplinarnych, mają

obowiązek zachowania tajemnicy o przetwarzanych w SL2014 danych osobowych oraz o stosowanych sposobach zabezpieczeń danych osobowych. Obowiązek zachowania tajemnicy istnieje również po ustaniu zatrudnienia lub współpracy.

§ 23.

Użytkownicy są w szczególności zobowiązani do:

- 1) bezwzględne przestrzegania zasad bezpieczeństwa przetwarzania informacji w SL2014, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania SL2014 oraz jego obsługi;
- 2) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
- 3) zabezpieczania zbioru danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcji i innych procedurach dotyczących zarządzania SL2014 oraz jego obsługi;
- 4) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
- 5) nieudzielania informacji o danych osobowych przetwarzanych w SL2014 innym podmiotom, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
- 6) bezwzględnego zawiadomiania Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych w SL2014, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§ 24.

Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzania danych osobowych są określone w załączniku nr 4 do Polityki.

Rozdział 6

Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 25.

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

- 1) stwierdzono naruszenie zabezpieczenia SL2014;
- 2) 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;
- 3) inne okoliczności wskazują, że mogło nastąpić nieuprawnione udostępnienie danych osobowych przetwarzanych w SL2014.

§ 26.

1. Każdy użytkownik, w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych w SL2014, jest zobowiązany do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz Administratora Bezpieczeństwa Informacji SL2014u Beneficjenta.

Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:

- 1) poinformować pisemnie o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji SL2014 w IP i stosować się do jego zaleceń;
- 2) 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. Administrator Bezpieczeństwa Informacji u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych w SL2014 jest zobowiązany niezwłocznie:
 - 1) wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i podpisać;
 - 2) 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 w SL2014;
 - 3) 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:
 - a) fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie niepowołanej,
 - b) wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
 - c) zmianę hasła użytkownika, przez którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu;
 - 4) szczegółowo analizować stan systemu informatycznego służącego przetwarzaniu danych osobowych w SL2014 w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;
 - 5) przywrócić normalne działanie systemu informatycznego służącego przetwarzaniu danych osobowych w SL2014.
4. Czynności opisane w ust. 3 wykonuje Administrator Systemu u Beneficjenta, o ile został powołany.

§ 27.

1. Po przywróceniu normalnego stanu SL2014 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 w SL2014.
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 Beneficjenta, a w przypadku gdy użytkownik nie jest pracownikiem, konsekwencje wynikające z umowy, o której mowa w § 21 ust. 1.

§ 28.

1. Administrator Bezpieczeństwa Informacji SL2014 u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia SL2014 i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia SL2014 przekazuje go Administratorowi Bezpieczeństwa Informacji w IP/IP2.
2. Jeżeli naruszenie zabezpieczenia SL2014 nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych w SL2014 Administrator Bezpieczeństwa Informacji SL2014 u Beneficjenta przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu u Beneficjenta, o ile został powołany.

Rozdział 7

Kontrola nad przestrzeganiem ochrony danych osobowych

§ 29.

1. Bieżąca kontrola nad przetwarzaniem danych osobowych w SL2014 u Beneficjenta jest dokonywana przez Administratora Bezpieczeństwa Informacji SL2014 u Beneficjenta.
2. W ramach kontroli, o której mowa w ust. 1 Administrator Bezpieczeństwa Informacji SL2014 u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30.

1. Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych, z czego sporządza odpowiedni raport.
2. Przygotowując raport, o którym mowa w ust. 1, Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta uwzględnia informacje zawarte w raportach, o których mowa w § 28.

§ 31.

Kontrola, o której mowa w § 30, polega w szczególności na sprawdzeniu:

- 1) którzy pracownicy mają dostęp do danych osobowych;
- 2) czy dane osobowe nie zostały udostępnione nieupoważnionym pracownikom lub osobom;
- 3) czy pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych w SL2014 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 8

Postanowienia końcowe

§ 32.

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

§ 33.

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

§ 34.

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia SL2014.

§ 35.

1. Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta.

2. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych Administrator Bezpieczeństwa Informacji SL2014u Beneficjenta, zaś w zakresie środków technicznych Administrator Systemu u Beneficjenta, o ile został powołany.

§ 36.

Integralną część niniejszej Polityki stanowią następujące załączniki:

- 1) Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych w SL2014u Beneficjenta RPO WD 2014-20;
- 2) Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe w SL2014;
- 3) Załącznik nr 3 – Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych;
- 4) Załącznik nr 4 -Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w SL2014u Beneficjenta;
- 5) Załącznik nr 5 – Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach SL2014;
- 6) Załącznik nr 6 – Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych.

Załącznik nr 1
do Polityki Bezpieczeństwa

**Rejestr osób upoważnionych do przetwarzania danych osobowych w SL2014
u Beneficjenta RPO WD 2014-2020**

Lp.	Imię i nazwisko	Zakres przydzielonych uprawnień	Data przyznania uprawnień
1	Kamila Wróblewska Carter		
2	Ewelina Grybuś		
3	Joanna Zatylna		
4			
5			
6			
7			
8			
9			
10			
11			
12			
13			
14			
15			
16			
17			
18			
19			
20			

Załącznik nr 2
do Polityki Bezpieczeństwa

**Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym
są przetwarzane dane osobowe w SL2014**

Lp.	Budynek – dane adresowe	Pomieszczenie
1.	ul. Szkolna 3, 59-600 Lwówek Śląski	Wszystkie pomieszczenia Szkoły Master's Academy
2.	Ul. Piekarska 1, 59-600 Lwówek Śląski	j.w

Załącznik nr 3
do Polityki Bezpieczeństwa

Lista oświadczeń użytkowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych

Oświadczam, iż zapoznałem/am się z:

- przepisami ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. z 2002 r. Nr 101, poz. 926, z późn. zm.) oraz przepisami wykonawczymi do niniejszej ustawy,
- Polityką Bezpieczeństwa.

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1	Kamila Wróblewska-Cetler		
2	Ewelina Grybuś		
3	Joanna Zatylna		
4			
5			
6			

Załącznik nr 4
do Polityki Bezpieczeństwa

Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w SL2014u Beneficjenta

I. 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.

II. Środki sprzętowe, informatyczne i telekomunikacyjne:

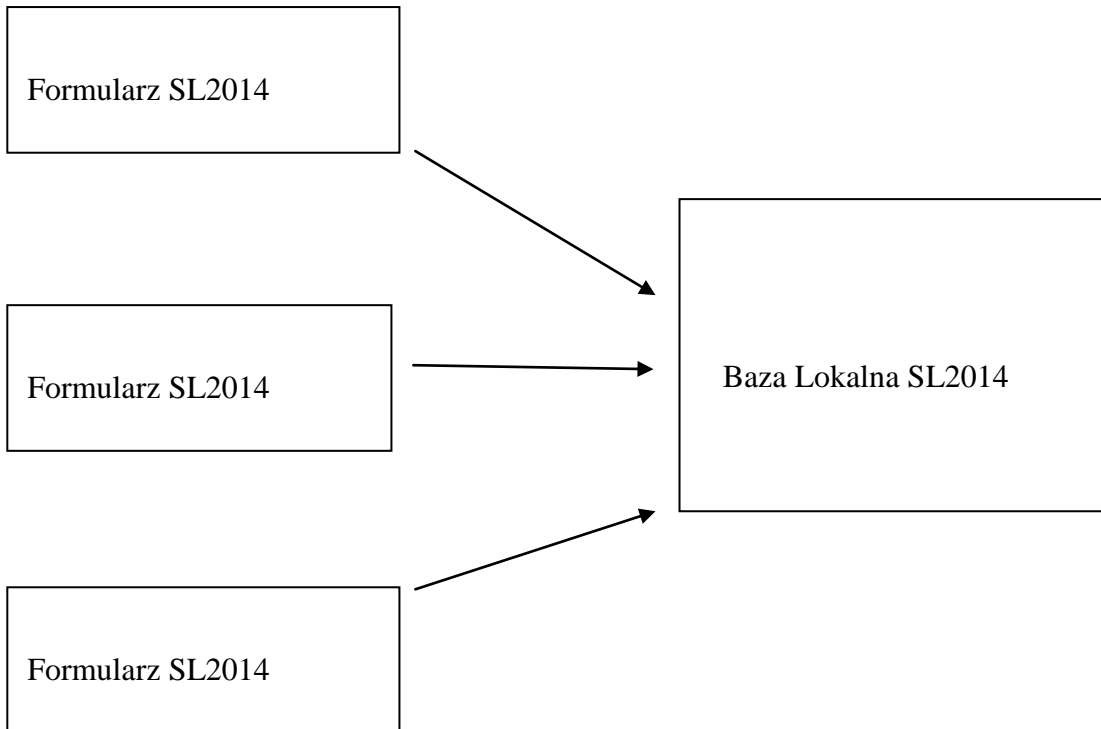
- a) Sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie firewalla programowego chroniącego zasoby beneficjenta.
- b) Oprogramowanie antywirusowe działające w czasie rzeczywistym na wszystkich komputerach wykrywa i eliminuje wirusy, konie trojańskie, 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.
- e) Zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe.

III Środki organizacyjne:

- a) Osoby zatrudnione przy przetwarzaniu danych osobowych zostały zaznajomione z przepisami dotyczącymi ochrony danych osobowych.
- b) Osoby zatrudnione 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.

Załącznik nr 5
do Polityki Bezpieczeństwa

Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach SL2014



Procedura przekazywania do IP Formularza SL2014 przez Beneficjentów

Formularz SL2014 powinien zostać dostarczony wyłącznie w systemie SL

Przekazywanie plików pomiędzy pracownikami - Przekazywane dane powinny zostać uprzednio skompresowane do jednego z formatów: ZIP, TAR, GZ lub RAR oraz zabezpieczone hasłem z wykorzystaniem programu 7-Zip lub Win RAR. Użycie innego programu kompresującego

Niestosowanie się do w/w procedury będzie uznawane przez IZ za rażące naruszenie przepisów o ochronie danych osobowych.

Załącznik nr 6
do Polityki Bezpieczeństwa

Wzór oświadczenia

Lwówek Śl., dnia

UPOWAŻNIENIE NR / 2018
DO PRZETWARZANIA DANYCH OSOBOWYCH

Na podstawie przepisów art. 37 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (j.t. z 2002 r. Dz. U. NR 101, poz. 926, z późn. zm.)

u p o w a ż n i a m

Panią/Pana

do przetwarzania danych osobowych zawartych w zbiorze/zbiorach danych o nazwie:

zgodnie z uprawnieniami wynikającymi z ustalonego zakresu czynności.

Zobowiązuję Panią/Pana do zachowania tajemnicy o danych znajdujących się w w/w zbiorach, jak i sposobach ich zabezpieczenia. Obowiązek ten istnieje również po ustaniu zatrudnienia.

Upoważnienie ważne jest na czas nieokreślony.

Upoważnienie może zostać odwołane lub utracić ważność wskutek wcześniejszego ustania zatrudnienia.

Oryginał upoważnienia należy zwrócić po jego odwołaniu lub ustaniu zatrudnienia.