BURMISTRZ PIĄTKU

Zarządzenie Nr 81/2022
Burmistrza Piątku
z dnia 24 listopada 2022 roku

w sprawie wprowadzenia Polityki Bezpieczeństwa dla Centralnego Systemu Teleinformatycznego SL2014 w Gminie Piątek

Na podstawie art. 33 ust. 3 ustawy z dnia 8 marca 1990 r. o samorządzie gminnym (t.j. Dz. U. z 2022 r. poz. 559 ze zm.) w związku z art. 24 ust. 1 i 2 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) **zarządza się co następuje:**

§ 1. Zarządzam wprowadzenie „Polityki Bezpieczeństwa dla Centralnego Systemu Teleinformatycznego SL2014 w Gminie Piątek", stanowiącą załącznik do zarządzenia.

§ 2. Zobowiązuję pracowników do przestrzegania „Polityki Bezpieczeństwa dla Centralnego Systemu Teleinformatycznego SL2014 w Gminie Piątek".

§ 3. Wykonanie i wdrożenie zarządzenia powierzam Sekretarzowi Gminy.

§ 4. Zarządzenie wchodzi w życie z dniem podpisania.

BURMISTRZ PIĄTKU

BURMISTRZ
mgr Krzysztof Lisiecki

BURMISTRZ PIĄTKU

Załącznik
do Zarządzenia Nr 81/2022
Burmistrza Piątku
z dnia 24 listopada 2022 r.

POLITYKA BEZPIECZEŃSTWA
DLA CENTRALNEGO SYSTEMU TELEINFORMATYCZNEGO
SL2014
W GMINIE PIĄTEK

Rozdział 1
Postanowienia ogólne

§ 1.

Polityka Bezpieczeństwa dla Centralnego Systemu Teleinformatycznego SL2014 u Beneficjenta RPO WŁ zwana dalej „Polityką", określa zasady i tryb oraz wprowadza jednolite standardy zarządzania bezpieczeństwem danych osobowych przetwarzanych w Centralnym Systemie Teleinformatycznym SL2014, zwanym dalej SL 2014, w **Gminie Piątek, Rynek 16, 99-120 Piątek**, zwanym dalej „Beneficjentem".

§ 2.

Użyte w Polityce określenia oznaczają:

1) **Administrator Danych**	Instytucję Zarządzającą Programem Operacyjnym;
2) **RODO**	Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE ;
3) **użytkownik**	osobę upoważnioną do przetwarzania danych osobowych w SL2014;
4) **Inspektor Ochrony Danych Osobowych**	osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL2014;
5) **Inspektor Ochrony Danych Osobowych SL2014 w IP/IP2**	osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL2014 w IP/IP2;
6) **Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta**	osobę wyznaczoną przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL2014 u Beneficjenta;
7) **Administrator Systemu u Beneficjenta**	osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych w SL2014 u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Inspektora Ochrony Danych Osobowych SL2014 u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;

8) naruszenie zabezpieczenia SL2014	jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności SL2014 skutkujące przypadkowym lub bezprawnym zniszczeniem, utratą, zmianą, nieuprawnionym ujawnieniem lub dostępem do danych osobowych;
9) dane osobowe	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;
10) przetwarzanie danych osobowych	jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;
11) usuwanie danych osobowych	zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
12) 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;
13) 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;
14) Instrukcja	Instrukcję Zarządzania Systemem Informatycznym dla Centralnego systemu teleinformatycznego SL2014 u Beneficjenta;
15) Pracownik	osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub innego stosunku prawnego;
16) Ministerstwo	Ministerstwo Inwestycji i Rozwoju.

Rozdział 2
Zakres oraz zasady zabezpieczania danych osobowych

§ 3.

Niniejszą politykę stosuje się do zbioru danych osobowych SL2014 znajdującego się u Beneficjenta. Celem jest zdefiniowanie ogólnych standardów i wymagań dla systemu informatycznego służącego do przetwarzania danych osobowych, utrzymywanego z zamiarem osiągnięcia takiego poziomu organizacyjnego i technicznego, które zapewnią ochronę systemu przed włamaniem i złośliwym oprogramowaniem, ochronę przed szpiegostwem komputerowym, ochronę przed przestępstwami komputerowymi, ochronę przed kradzieżami danych i oprogramowania.

§ 4.

1. Nadzór ogólny nad realizacją przepisów wynikających z przepisów dotyczących ochrony danych osobowych pełni Administrator Danych.
2. Nadzór nad poprawnością realizacji przepisów o ochronie danych osobowych, w szczególności zasad opisanych w **Polityce** oraz **Instrukcji,** która stanowiącej **załączniku nr 5 do Polityki** oraz nad wykonywaniem zadań związanych z ochroną danych osobowych w SL2014 u Beneficjenta, sprawuje Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta.

§ 5.

Dane osobowe przetwarzane w SL2014 podlegają ochronie zgodnie z przepisami dotyczącymi ochrony danych osobowych, a w szczególności Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związanych z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE.

§ 6.

Przetwarzanie danych osobowych w SL2014 jest dopuszczalne wyłącznie w zakresie niezbędnym do udzielenia wsparcia, realizacji projektów, ewaluacji, monitoringu, sprawozdawczości i kontroli, w ramach RPO WŁ.

§ 7.

Przetwarzanie danych osobowych w SL2014 nie może naruszać praw i wolności osób, i może być realizowane na zasadzie dobrowolności zgodnie z wymaganiami, o których mowa w art. 9 RODO.

§ 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 do bycia informowanym, dostępu do swoich danych osobowych oraz ich poprawiania, prawie do usuwania danych, prawie do ograniczenia przetwarzania danych, prawie do przenoszenia danych, prawie do wniesienia sprzeciwu;
4) dobrowolności podania danych osobowych, z zastrzeżeniem, że odmowa zgody na ich przetwarzanie skutkuje niemożnością wzięcia udziału w projekcie realizowanym w ramach RPO WŁ.

§ 9.

1. Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w pełnej zgodności z przepisami prawa dotyczącymi ochrony danych osobowych.
2. Wnioski o udostępnienie danych osobowych przetwarzanych w SL2014, po wstępnym rozpatrzeniu przez Inspektora Ochrony Danych Osobowych, 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 dotyczące ochrony danych osobowych oraz umowy o dofinansowanie projektu.
2. Umowy lub porozumienia o powierzeniu przetwarzania danych osobowych w SL2014 powinny zostać przed podpisaniem, w zakresie dotyczącym zasad przetwarzania danych osobowych, zaopiniowane przez Inspektora ochrony Danych osobowych SL2014 u Beneficjenta.

§ 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 przepisów dotyczących ochrony danych osobowych 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 przepisów dotyczących ochrony danych osobowych 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 Inspektora Ochrony Danych Osobowych Informacji SL2014 u Beneficjenta

§ 14.

Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych w SL2014 u Beneficjenta.

§ 15.

Do zadań Inspektora Ochrony Danych Osobowych u Beneficjenta należy w szczególności:

1) współdziałanie z Inspektorem Ochrony Danych Osobowych SL2014 w Instytucji Pośredniczącej w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z przepisów dotyczących ochrony danych osobowych;
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 SL2014 u 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 SL2014 u 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 SL2014 podmiotowi zewnętrznemu wobec Beneficjenta.

§ 16.

W doborze i stosowaniu środków ochrony danych osobowych w SL2014 Inspektor ochrony Danych Osobowych SL2014 u Beneficjenta zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 17.

1. Obowiązki Inspektora Ochrony Danych Osobowych SL2014 u Beneficjenta wykonywane są przez wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta Pracownika.
2. Nadzór nad wykonywaniem obowiązków Inspektora Ochrony Danych Osobowych SL2014 u 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, Inspektor Ochrony danych Osobowych SL2014 u Beneficjenta konsultuje się i współpracuje z Inspektorem Ochrony Danych Osobowych SL2014 w Instytucji Pośredniczącej.

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 Inspektora Ochrony Danych Osobowych SL2014 u 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 Inspektora Ochrony Danych Osobowych SL2014 u Beneficjenta, którego wzór jest określony w **załączniku nr 1 do Polityki**.
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 Inspektora Ochrony Danych Osobowych SL 2014 u Beneficjenta potwierdzający przyznanie uprawnień;
   6) datę odebrania uprawnień
   7) podpis Inspektora Ochrony Danych Osobowych SL2014 u 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 Inspektora Ochrony Danych Osobowych SL2014 u 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 odpowiedzialnego za te osoby.

§ 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) bezwzględnego 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) bezzwłocznego zawiadamiania Inspektora Ochrony Danych Osobowych SL2014 u 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 fizyczne, 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 Inspektora Ochrony Danych Osobowych SL2014 u Beneficjenta.
2. Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązany niezwłocznie:
   1) poinformować pisemnie o zaistniałym zdarzeniu Inspektora Ochrony Danych Osobowych SL2014 w Instytucji Pośredniczącej 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. Inspektora Ochrony Danych Osobowych 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;
   6) 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. Inspektor Ochrony Danych Osobowych 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 Instytucji Pośredniczącej.
2. Jeżeli naruszenie zabezpieczenia SL2014 nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych w SL2014 Inspektor Ochrony Danych Osobowych 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 Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta.
2. W ramach kontroli, o której mowa w ust. 1 Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30.

1. Inspektor Ochrony Danych Osobowych SL2014 u 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, Inspektor Ochrony Danych Osobowych SL2014 u 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 Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta.
2. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych Inspektor Ochrony Danych Osobowych SL2014 u 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 SL2014 u Beneficjenta;
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 fizycznych, technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w SL2014 u Beneficjenta;
5) Załącznik nr 5 – Instrukcja Zarządzania Centralnym Systemem Informatycznym SL2014 u Beneficjenta;
6) Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych;
7) Załącznik nr 7 – Wzór odwołania upoważnienia do przetwarzania danych osobowych.

BURMISTRZ
mgr Krzysztof Lisiecki

Załącznik nr 1
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

Rejestr osób upoważnionych do przetwarzania danych osobowych w SL 2014 u Beneficjenta

Lp.	Imię I nazwisko	Identyfikator użytkownika	Zakres przydzielonych uprawnień	Data przyznania uprawnień	Podpis Inspektora ochrony Danych Osobowych	Data odebrania uprawnień	Podpis Inspektora Ochrony Danych Osobowych
1.							
2.							
3.							
4.							

Załącznik nr 2
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

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

Lp.	Budynek – dane adresowe	Pomieszczenie

Załącznik nr 3
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

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

Oświadczam, iż zapoznałem/am się z:

- przepisami ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych;
- Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związanych z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;
- Polityką Bezpieczeństwa dla zbioru SL2014 u Beneficjenta RPO WŁ oraz z Instrukcją Zarządzania Systemem Informatycznym dla systemu SL2014.

Lp.	Imię i nazwisko	Data	Podpis potwierdzający zapoznanie się z ww. dokumentami
1.			
2.			
3.			
4.			
5.			
6.			
7.			

Załącznik nr 4
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

Określenie środków fizycznych, technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności ochrony danych osobowych w SL2014 u Beneficjenta

I. Środki ochrony fizycznej danych:

a) budynek Urzędu podlega ochronie polegającej na całodobowym monitorowaniu przez system alarmowy wraz z czujnikami ruchu i system monitoringu wizyjnego;

b) drzwi wejściowe do Urzędu wyposażone w zamek patentowy;

c) pomieszczenia, w których przetwarzany jest zbiór danych osobowych wyposażone są w system alarmowy przeciwwłamaniowy;

d) pomieszczenie, w którym przetwarzane są zbiory danych osobowych, zabezpieczone jest przed skutkami pożaru za pomocą wolnostojącej gaśnicy;

e) klucze do pomieszczeń wydawane wyłącznie osobom upoważnionym;

f) podczas nieobecności osób uprawnionych pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz;

g) 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;

h) 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;

i) zbiór danych osobowych w formie papierowej jest przechowywany w zamkniętej szafie;

j) kopie zapasowe/archiwalne zbioru danych osobowych są przechowywane w zamkniętej metalowej szafie;

k) dokumenty zawierające dane osobowe po ustaniu przydatności są niszczone w sposób mechaniczny za pomocą niszczarek dokumentów.

II. Środki techniczne (sprzętowe, informatyczne i telekomunikacyjne):

a) sieć komputerowa jest zabezpieczona przed nieuprawnionym dostępem z sieci Internet poprzez zastosowanie Firewall 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 zbioru danych osobowych, który przetwarzany jest na wydzielonej stacji komputerowej zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą hasła BIOS;

d) dostęp do systemu operacyjnego komputera, w którym są przetwarzane dane osobowe jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

e) dostęp do zbioru danych osobowych wymaga uwierzytelnienia z wykorzystaniem identyfikatora użytkownika oraz hasła;

f) zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł;

g) zastosowano macierz dyskową w celu ochrony danych osobowych przed skutkami awarii pamięci dyskowej;

h) zainstalowano wygaszacze ekranów na stanowiskach, na których są przetwarzane dane osobowe;

i) zastosowano urządzenia typu UPS, chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

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;

e) przeszkolono osoby zatrudnione przy przetwarzaniu danych osobowych w zakresie zabezpieczeń systemu informatycznego.

Załącznik nr 5
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

Instrukcja Zarządzania Centralnym Systemem Informatycznym SL2014 u Beneficjenta

Rozdział 1
Postanowienia ogólne

§ 1.

Instrukcja Zarządzania Systemem Informatycznym dla systemu SL2014 u Beneficjenta RPO WŁ, zwana dalej ,,Instrukcją", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w Centralnym systemie teleinformatycznym SL2014, zwanym dalej „SL2014", w Gminie Piątek zwanym/ej dalej „Beneficjentem".

§ 2.

Użyte w Instrukcji określenia oznaczają:

1) **Administrator Danych** – Instytucję Zarządzającą Realizację Programów Operacyjnych Województwa Łódzkiego;
2) **Użytkownik** – osobę upoważnioną do przetwarzania danych osobowych w SL2014;
3) **Inspektor Ochrony Danych Osobowych SL2014 w Jednostce Pośredniczącej (IP)** – osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL2014 we właściwej Instytucji Pośredniczącej RPO WŁ;
4) **Inspektor ochrony Danych Osobowych SL2014 u Beneficjenta** – osobę odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych w SL2014 u Beneficjenta;
5) **Administrator Systemu Informatycznego u Beneficjenta** – osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń SL2014 u Beneficjenta, o ile zadanie te zostały wyłączone z zakresu kompetencji Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;
6) **naruszenie zabezpieczenia SL2014** – jakiekolwiek zdarzenie lub działanie, które może stanowić przyczynę utraty zasobów, niezawodności, integralności lub poufności SL2014.

Rozdział 2
Przydział haseł i identyfikatorów

§ 3.

Podstawową metodą logowania do systemu jest uwierzytelnienie za pomocą elektronicznej platformy usług administracji publicznej ePUAP.

§ 4.

Identyfikator użytkownika jest niepowtarzalny, a po wyrejestrowaniu użytkownika z S2014 nie jest przydzielany innej osobie.

§ 5.

Hasło użytkownika:

1) jest przydzielane indywidualnie dla każdego z użytkowników;
2) nie jest zapisane w systemie komputerowym w postaci jawnej.

§ 6.

Osobą odpowiedzialną za przydział identyfikatorów i pierwszych haseł dla użytkowników u Beneficjenta jest Administrator Systemów Informatycznych SL2014 u Beneficjenta.

§ 7.

1. Użytkownik jest odpowiedzialny za wszystkie czynności wykonane przy użyciu identyfikatora, który został mu przyznany.
2. Użytkownik jest zobowiązany utrzymywać hasło, którym się posługuje lub posługiwał, w ścisłej tajemnicy, w szczególności dołożyć wszelkich starań w celu uniemożliwienia zapoznania się przez osoby trzecie z hasłem, nawet po ustaniu jego ważności.

Rozdział 3
Rejestrowanie i wyrejestrowywanie użytkowników

§ 8.

1. Rejestracji i wyrejestrowywania użytkowników z systemu dokonuje Administrator Systemu Informatycznego SL2014 u Beneficjenta.
2. Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta prowadzi rejestr użytkowników, który stanowi **załącznik nr 1 do Polityki** Bezpieczeństwa dla zbioru Centralnego systemu teleinformatycznego SL2014 u Beneficjenta.
3. Jakakolwiek zmiana informacji ujawnionych w rejestrze podlega natychmiastowemu odnotowaniu i uaktualnieniu.

§ 9.

W SL2014 może zostać zarejestrowany jedynie użytkownik, któremu upoważniona do tego osoba wydała upoważnienie do przetwarzania danych osobowych w SL2014.

§ 10.

1. Po zarejestrowaniu w SL2014 użytkownik jest informowany przez Administratora Systemu Informatycznego SL2014 u Beneficjenta o ustalonym dla niego identyfikatorze i konieczności posługiwania się hasłami.
2. Inspektor Ochrony Danych Osobowych SL2014 u Beneficjenta jest odpowiedzialny za zapoznanie każdego nowego użytkownika z Instrukcją oraz Polityką Bezpieczeństwa dla zbioru Centralnego systemu teleinformatycznego SL2014 u Beneficjenta, a także z przepisami dotyczącymi ochrony danych osobowych, co użytkownik potwierdza swoim podpisem na liście, stanowiącej **załącznik nr 3 do Polityki** Bezpieczeństwa dla zbioru Centralnego systemu teleinformatycznego SL2014 u Beneficjenta.

§ 11.

Użytkownik jest wyrejestrowywany z SL2014 w każdym przypadku utraty przez niego uprawnień do przetwarzania danych osobowych w SL2014, co ma miejsce szczególnie w przypadku:

1) ustania zatrudnienia tego użytkownika u Beneficjenta lub zakończeniu przez tego użytkownika współpracy z Beneficjentem na podstawie umowy cywilno-prawnej;
2) zmiany zakresu obowiązków użytkownika powodujących utratę uprawnień do przetwarzania danych osobowych w SL2014.

Rozdział 4
Rozpoczęcie, zawieszenie i zakończenie pracy w SL2014

§ 12.

Użytkownik rozpoczynając pracę jest zobowiązany zalogować się do SL2014 posługując się swoim hasłem i loginem w celu podpisania dokumentu.

§ 13.

1. W przypadku, gdy użytkownik planuje przerwać pracę, jest zobowiązany do zabezpieczenia dostępu do komputera za pomocą wygaszacza ekranu z aktywnym hasłem.
2. W przypadku, gdy użytkownik planuje przerwać pracę na dłuższy okres, a także kończąc pracę, jest zobowiązany wylogować się z SL2014 oraz sprawdzić, czy nie zostały pozostawione bez zamknięcia nośniki zawierające dane osobowe.

§ 26.

Osoby nieuprawnione do dostępu do danych osobowych w SL2014 mogą przebywać w pomieszczeniach, w których są przetwarzane dane osobowe w SL2014 wyłącznie w obecności co najmniej jednego użytkownika odpowiedzialnego za te osoby.

§ 27.

Decyzję o instalacji na stacji roboczej obsługującej przetwarzanie danych osobowych w SL2014 jakiegokolwiek oprogramowania systemowego lub użytkowego podejmuje Administrator Systemu Informatycznego SL2014 u Beneficjenta.

Rozdział 9
Postanowienia końcowe

§ 28.

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

§ 29.

Instrukcja nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia SL201.

Załącznik nr 6
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

UPOWAŻNIENIE Nr _____

DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... r., na podstawie art. 29 w związku z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 04.05.2016 r., **upoważniam** Pana/Panią* ..... do przetwarzania danych osobowych w zbiorze **„Realizacja programów operacyjnych i projektów współfinansowanych z Funduszy Europejskich"** w ramach Regionalnego Programu Operacyjnego Województwa Łódzkiego na lata 2014-2020. Upoważnienie wygasa z chwilą ustania Pana/Pani* stosunku prawnego z Gminą Piątek lub z chwilą jego odwołania.

Czytelny podpis osoby upoważnionej do
wydawania i odwoływania upoważnień.

Upoważnienie otrzymałem

(miejscowość, data) (podpis osoby upoważnionej)

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

Zobowiązuję się do zachowania w tajemnicy przetwarzanych danych osobowych, z którymi zapoznałem/am się oraz sposobów ich zabezpieczania, zarówno w okresie trwania umowy jak również po ustania stosunku prawnego łączącego mnie z Gminą Piątek.

Czytelny podpis osoby składającej oświadczenie

* Niepotrzebne skreślić

BURMISTRZ PIĄTKU

Załącznik nr 7
do Polityki Bezpieczeństwa dla
systemu SL2014 u Beneficjenta

ODWOŁANIE UPOWAŻNIENIA Nr ____
DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem ..... r., na podstawie art. 29 w związku z art. 28 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L 119 z 04.05.2016 r., **odwołuję upoważnienie** Pana/Pani* ..... Nr ..... do przetwarzania danych osobowych wydane w dniu .....

Czytelny podpis osoby upoważnionej do
wydawania i odwoływania upoważnień.

Odwołanie upoważnienia otrzymałem

(miejscowość, data) (podpis osoby upoważnionej)

* Niepotrzebne skreślić