POLITYKA OCHRONY DANYCH OSOBOWYCH

Dotyczy projektu **„DOBRY KURS - rozwój kompetencji w sektorze motoryzacyjnym”**
nr projektu: **POWR.02.21.00-00-R125/21**

Rozdział 1
Postanowienia ogólne

§ 1

Polityka Ochrony Danych Osobowych zwana dalej „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w zbiorach danych przetwarzanych przez Marcin Rokoszewski MARSOFT, w ramach projektu **„DOBRY KURS - rozwój kompetencji w sektorze motoryzacyjnym"** nr projektu: **POWR.02.21.00-00-R125/21**

§ 2

Użyte w Polityce określenia oznaczają:

Administrator Danych Osobowych	Minister właściwy do spraw rozwoju regionalnego pełniący funkcję Instytucji Zarządzającej dla Programu Operacyjnego Wiedza Edukacja Rozwój 2014-2020, mający siedzibę przy ul. Wspólnej 2/4, 00-926 Warszawa
Instytucja Pośrednicząca	Polska Agencja Rozwoju Przedsiębiorczości z siedzibą w Warszawie przy ul. Pańskiej 81/83, NIP 526-25-01-444, REGON 017181095
Beneficjent	Marcin Rokoszewski MARSOFT ul. Turystyczna 36, 20-207 Lublin, NIP 9462304058
Ustawa	Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.) oraz Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.
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. 2004 Nr 100, poz. 1024);
Użytkownik	Osobę upoważnioną do przetwarzania danych osobowych;
Administrator Systemu	Osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych;

Naruszenie zabezpieczenia	Jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności lub poufności zbiorów danych;
Dane osobowe	Wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej; dane osobowe w rozumieniu ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 poz. 1000 z późn. zm.) oraz Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w zakresie określonym w załączniku do umowy o dofinansowanie (tj. zakres danych osobowych powierzonych Beneficjentowi do przetwarzania)
Przetwarzanie danych osobowych	Jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie a zwłaszcza te, które wykonuje się w systemie informatycznym;
Usuwanie danych osobowych	Zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
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;
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;
Instrukcja	Instrukcję Zarządzania Systemem Informatycznym;
Pracownik	Osobę zatrudnioną na podstawie stosunku pracy lub innego stosunku prawnego;

Rozdział 2
Zakres oraz zasady zabezpieczania danych osobowych

§ 3

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

§ 4

1. Nadzór ogólny nad realizacją przepisów wynikających z ustawy oraz rozporządzenia pełni Administrator Danych Osobowych.
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, sprawuje osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta.

§ 5

Dane osobowe przetwarzane przez Beneficjenta podlegają ochronie zgodnie z przepisami ustawy.

§ 6

1. Przetwarzanie danych osobowych jest dopuszczalne wyłącznie w celu udzielania wsparcia uczestnikom projektu, z uwzględnieniem rekrutacji, działań informacyjnych, monitorowania, sprawozdawczości, waluacji, kontroli i audytu prowadzonych w zakresie projektu oraz zarządzania, kontroli, audytu, ewaluacji, sprawozdawczości i raportowania w ramach projektu.
2. Pracownik Beneficjenta jest zobowiązany odebrać od uczestnika projektu oświadczenie, którego wzór stanowi załącznik nr 9 do Polityki. Oświadczenia przechowywane są w siedzibie Beneficjenta lub w innym miejscu, w którym są zlokalizowane dokumenty związane z Projektem.

§ 7

Przetwarzanie danych osobowych nie 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 wskazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym, z wyjątkiem sytuacji o których mowa w art. 27 ust. 2 ustawy.

§ 8

W przypadku zbierania jakichkolwiek danych osobowych bezpośrednio od osoby, której dane dotyczą, Pracownik Beneficjenta jest zobowiązany do przekazania tej osobie informacji o:

1. pełnej nazwie instytucji gromadzących dane osobowe oraz ich adresach;
2. celu zbierania danych osobowych, a w szczególności o znanych mu w czasie udzielania informacji przewidywanych odbiorcach lub kategoriach odbiorców danych,
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, szkoleniu lub innych zajęciach.

§ 9

Jakiekolwiek udostępnianie danych osobowych może odbywać się wyłącznie w trybie określonym w ustawie oraz w pełnej zgodności z przepisami prawa.

§ 10

Przetwarzanie danych osobowych może zostać powierzone innym podmiotom wykonującym zadania związane z udzieleniem wsparcia i realizacją Projektu, wyłącznie w celach określony w § 6, pod warunkiem zawarcia z tym podmiotem pisemnej umowy powierzenia przetwarzania danych osobowych.

§ 11

1. Każdej osobie, której dane osobowe są przetwarzane, przysługuje prawo do kontroli przetwarzania jej danych osobowych, a w szczególności prawo do:
   a) uzyskania wyczerpującej informacji, czy jej dane osobowe są przetwarzane oraz do otrzymania informacji o pełnej nazwie i adresie siedziby Administratora Danych Osobowych, Instytucji Pośredniczącej i Beneficjenta;
   b) uzyskania informacji o celu, zakresie i sposobie przetwarzania danych osobowych;
   c) uzyskania informacji, od kiedy są przetwarzane jej dane osobowe, oraz podania w powszechnie zrozumiałej formie treści tych danych;
   d) uzyskania informacji o źródle, z którego pochodzą dane osobowe jej dotyczące;
   e) uzyskania informacji o sposobie udostępniania danych osobowych, a w szczególności informacji o odbiorcach lub kategoriach odbiorców, którym te dane osobowe są udostępniane;
   f) 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;
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 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 3
Obowiązki osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta

§ 14

Osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta poza realizacją zadań wynikających z Polityki, sprawuje ogólny nadzór nad realizacją czynności dotyczących przetwarzania danych osobowych.

§ 15

Do zadań osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta należy w szczególności:

1. współdziałanie z osobą odpowiedzialną za ochronę danych osobowych instytucji zewnętrznych 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, który stanowi załącznik nr 2 do Polityki;
4. analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta;
5. opiniowanie umów powierzenia przetwarzania danych osobowych podmiotowi zewnętrznemu;
6. zapewnianie zapoznania użytkowników z przepisami o ochronie danych osobowych.

§ 16

W doborze i stosowaniu środków ochrony danych osobowych osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta zwraca szczególną uwagę na ich należyte zabezpieczenie przed udostępnieniem osobom nieuprawnionym, kradzieżą, uszkodzeniem lub nieuprawnioną modyfikacją.

§ 17

1. Obowiązki osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta wykonywane są przez Pracownika wyznaczonego przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta.
2. Nadzór nad wykonywaniem obowiązków osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta pełni kierownik jednostki organizacyjnej Beneficjenta.

§ 18

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania danych osobowych, osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta konsultuje się i współpracuje z osoba odpowiedzialna za ochronę danych osobowych instytucji zewnętrznych.

Rozdział 4
Przetwarzanie danych osobowych

§ 19

1. Do przetwarzania danych osobowych mogą być dopuszczeni jedynie Pracownicy posiadający odpowiednie upoważnienie wydane przez osobę odpowiedzialnę za ochronę danych osobowych ze strony Beneficjenta. Wzór upoważnienia do przetwarzania danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach nr 6 i 7.

2. Każdy Pracownik, przed dopuszczeniem go do przetwarzania danych osobowych, 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, której wzór jest określony w załączniku nr 3 do Polityki.

§ 20

1. Każdy Pracownik mający dostęp do danych osobowych jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez osobę odpowiedzialną za ochronę danych osobowych ze strony Beneficjenta.
2. Rejestr, o którym mowa w ust. 1, zawiera:
   a) imię i nazwisko osoby upoważnionej;
   b) datę nadania i ustania oraz zakres upoważnienia do przetwarzania danych osobowych;
   c) identyfikator, jeżeli dane są przetwarzane w systemie informatycznym.

§ 21

1. Dopuszczenie do przetwarzania danych osobowych przez osoby niebędące Pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po uzyskaniu pozytywnej opinii osoby odpowiedzialnej za ochronę danych osobowych ze strony 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 Pracownika Beneficjenta.

§ 22

Wszyscy użytkownicy 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.

§ 23

Użytkownicy są w szczególności zobowiązani do:

1. bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji, określonych w Polityce, Instrukcji i innych procedurach, dotyczących zarządzania 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 oraz jego obsługi;
4. niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
5. nieudzielania informacji o przetwarzanych 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;
6. bezzwłocznego zawiadamiania osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych, 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 5
Postępowanie w przypadku naruszenia ochrony danych osobowych

§ 25

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

1. stwierdzono naruszenie zabezpieczeń;
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 przetwarzanych danych osobowych.

§ 26

1. Każdy użytkownik w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych, jest zobowiązana do niezwłocznego poinformowania o tym bezpośredniego przełożonego oraz osoby odpowiedzialnej za ochronę danych osobowych ze strony Beneficjenta.
2. Osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta, która stwierdziła lub uzyskała informację wskazującą na naruszenie ochrony danych osobowych jest zobowiązana niezwłocznie:
   a) poinformować pisemnie o zaistniałym zdarzeniu Instytucję Pośrednicząca i stosować się do jej 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. Osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta, który stwierdziła lub uzyskała informację wskazującą na naruszenie zabezpieczenia systemu informatycznego służącego przetwarzaniu danych osobowych jest zobowiązana 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.
f) Czynności opisane w ust. 3 wykonuje Administrator Systemu, o ile został powołany.

§ 27

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

§ 28

1. Osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczeń i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczeń przekazuje go osoba odpowiedzialna za ochronę danych osobowych instytucji zewnętrznej.
2. Jeżeli naruszenie zabezpieczeń nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta przygotowując raport, o którym mowa w ust. 1 współpracuje z Administratorem Systemu, o ile został powołany.

Rozdział 6
Kontrola nad przestrzeganiem ochrony danych osobowych

§ 29

1. Bieżąca kontrola nad przetwarzaniem danych osobowych jest dokonywana przez osobę odpowiedzialną za ochronę danych osobowych ze strony Beneficjenta.
2. W ramach kontroli, o której mowa w ust. 1 osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta jest zobowiązana do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§ 30

1. Osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta przeprowadza w pierwszym kwartale roku kalendarzowym kontrolę w zakresie przestrzegania przez użytkowników Polityki, Instrukcji oraz innych przepisów prawa w zakresie ochrony danych osobowych.

§ 31

Kontrola, o której mowa w § 30, polega w szczególności na sprawdzeniu:
a) którzy pracownicy mają dostęp do danych osobowych;

b) czy dane osobowe nie zostały udostępnione nieupoważnionym Pracownikom lub osobom;
c) czy Pracownicy i inne osoby mające dostęp do danych osobowych przetwarzanych w ramach projektu posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

§ 32

1. Beneficjent umożliwia Administratorowi danych osobowych lub podmiotom przez niego upoważnionym, w miejscach, w których są przetwarzane powierzone dane osobowe, dokonanie kontroli:
   a) zawiadomienie o zamiarze przeprowadzenia kontroli powinno być przekazane podmiotowi kontrolowanemu co najmniej 5 dni roboczych przed rozpoczęciem kontroli.
   b) W przypadku powzięcia przez Administratora danych osobowych wiadomości o rażącym naruszeniu przez Beneficjenta obowiązków wynikających z ustawy o ochronie danych osobowych, rozporządzenia MSWiA lub niniejszej umowy, Beneficjent umożliwi Administratorowi danych osobowych lub podmiotom prze niego upoważnionym dokonanie niezapowiedzianej kontroli.
2. Kontrolerzy Administratora danych osobowych lub podmiotów przez niego upoważnionych, mają w szczególności prawo:
   a) Wstępu, w godzinach pracy Beneficjenta, za okazaniem imiennego upoważnienia, do pomieszczenia, w którym jest zlokalizowany zbiór powierzonych do przetwarzania danych osobowych oraz pomieszczenia, w którym są przetwarzane powierzone dane osobowe i przeprowadzenia niezbędnych badań lub innych czynności kontrolnych w celu oceny zgodności przetwarzania danych osobowych z ustawą o ochronie danych osobowych, rozporządzeniem MSWiA oraz niniejszą umową;
   b) żądać złożenia pisemnych lub ustnych wyjaśnień przez osoby upoważnione do przetwarzania danych osobowych w zakresie niezbędnym do ustalenia stanu faktycznego;
   c) wglądu do wszystkich dokumentów i wszelkich danych mających bezpośredni związek z przedmiotem kontroli oraz sporządzania ich kopii;
   d) przeprowadzania oględzin urządzeń, nośników oraz systemu informatycznego służącego do przetwarzania danych osobowych;
3. Beneficjent zobowiązuje się zastosować zalecenia dotyczące poprawy jakości zabezpieczenia danych osobowych oraz sposobu ich przetwarzaniu sporządzone w wyniku kontroli przeprowadzonych przez Administratora danych osobowych lub podmioty przez niego upoważnione albo przez inne instytucje upoważnione do kontroli na podstawie odrębnych przepisów.
4. Beneficjent zobowiązuje się do usunięcia z elektronicznych nośników informacji wielokrotnego zapisu w sposób trwały i nieodwracalny oraz zniszczenia nośników papierowych i elektronicznych nośników informacji jednokrotnego zapisu, na których utrwalone zostały powierzone do przetwarzania dane osobowe, po zakończeniu obowiązywania okresu archiwizowania wynikającego z przepisów obowiązującego prawa.

Rozdział 7
Postanowienia końcowe

§ 33

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

§ 34

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

§ 35

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczeń.

§ 36

1. Wykazy i rejestry znajdujące się w załącznikach nr 1-3 do Polityki, prowadzi osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta.
2. Wykaz znajdujący się w załączniku nr 4 do Polityki prowadzi w zakresie środków organizacyjnych osoba odpowiedzialna za ochronę danych osobowych ze strony Beneficjenta, zaś w zakresie środków technicznych Administrator Systemu, o ile został powołany.

Integralną część niniejszej Polityki stanowią następujące załączniki:

1. Załącznik nr 1 – Rejestr osób upoważnionych do przetwarzania danych osobowych z podziałem na zadania;
2. Załącznik nr 2 – Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym są przetwarzane dane osobowe;
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;
5. Załącznik nr 5 – Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych
6. Załącznik nr 6 – Wzór upoważnienia do przetwarzania danych osobowych uczestników projektu
7. Załącznik nr 7 - Wzór odwołania upoważnienia do przetwarzania danych osobowych uczestników projektu
8. Załącznik nr 8 – Sposób przepływu danych pomiędzy narzędziami do przetwarzania danych osobowych w ramach systemu SL2014;
9. Załącznik nr 9 – wzór oświadczenia uczestnika projektu potwierdzającego zgodę na przetwarzanie danych osobowych.
10. Załącznik nr 10 – Rejestr czynności przetwarzania