Polityka bezpieczeństwa danych osobowych

Fundacja Animacji Społecznej i Ekonomii Społecznej
ul. Władysława Sobocińskiego 4,
40-687 Katowice

Rozdział 1

Postanowienia ogólne

§1

Polityka bezpieczeństwa dla zbiorów danych osobowych u Beneficjenta Programów Operacyjnych (dalej PO), zwaną „Polityką", określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w Fundacji Animacji Społecznej i Ekonomii Społecznej, zwanej dalej „Beneficjentem".

§2

Użyte w Polityce określenia oznaczają:

1) Administrator Danych - Instytucję Zarządzającą PO,

2) Ustawa - Ustawę z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. Nr 2018,poz.1000),

3) 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) (Dz. Urz. UE L 119 z dnia 04.05.2019 r., str.1);

4) Użytkownik - osobę upoważnioną do przetwarzania danych osobowych,

5) Inspektor Danych Osobowych - osobę wyznaczoną przez Administratora Danych, odpowiedzialną za nadzór nad zapewnieniem bezpieczeństwa danych osobowych;

6) Administrator Systemu u Beneficjenta - osobę odpowiedzialną za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń systemu informatycznego służącego do przetwarzania danych u Beneficjenta, o ile zadania te zostały wyłączone z zakresu kompetencji Administratora Bezpieczeństwa Informacji u Beneficjenta i powierzone przez osobę upoważnioną do podejmowania decyzji u Beneficjenta innemu pracownikowi;

7) Naruszenie zabezpieczenia bazy danych - jakiekolwiek naruszenie bezpieczeństwa, niezawodności, integralności, lub poufności bazy danych;

8) Dane osobowe - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej;

9) Przetwarzanie danych osobowych - jakiekolwiek operacje wykonywane na danych osobowych polegające na: zbieraniu, utrwalaniu, opracowywaniu, zmienianiu, przechowywaniu, analizowaniu, raportowaniu, aktualizowaniu, udostępnianiu lub usuwaniu danych osobowych;

10) Usuwanie danych osobowych - czynność, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;

11) 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;

12) Zabezpieczenie danych osobowych - środki administracyjne, techniczne i fizyczne wdrożone w celu zabezpieczenia zasobów technicznych oraz ochrony przed zniszczeniem, nieuprawionym dostępem i modyfikacją, ujawnieniem lub pozyskaniem danych osobowych bądź ich utratą;

13) Pracownik - osobę zatrudnioną u Beneficjenta na podstawie stosunku pracy lub innego stosunku prawnego;

14) Ministerstwo - Ministerstwo Rozwoju Regionalnego;

Rozdział 2

Zakres oraz zasady zabezpieczenia danych osobowych

§1

Niniejszą Politykę stosuje się do zbioru danych osobowych znajdującego się u Beneficjenta.

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

§3

Dane osobowe przetwarzane podlegają ochronie zgodnie z przepisami ustawy.

§4

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

§5

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 orientacji seksualnej oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym
lub administracyjnym.

§6

W przypadku zbierania jakichkolwiek danych osobowych na potrzeby bazy danych osobowych 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 Programu Operacyjnego.

§7

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

§8

Przetwarzanie danych osobowych 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.

§9

Każdej osobie, której dane osobowe są przetwarzane 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 udostępnione;
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.

§10

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 te dane są przetwarzane;
5. W jakim zakresie oraz komu te dane osobowe zostały udostępnione.

§11

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, 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 Administratora Bezpieczeństwa Informacji u Beneficjenta

§1

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

§2

Do zadań Administratora Bezpieczeństwa Informacji u Beneficjenta należy w szczególności:

1. Współdziałanie z Administratorem Bezpieczeństwa Informacji w IZ/IP PO lub innym podmiotem upoważnionym w zakresie zapewniającym wypełnianie przez Beneficjenta obowiązków wynikających z ustawy i rozporządzenia;

2. Prowadzenie i aktualizacja rejestru, o którym mowa §2 Rozdział 5, który stanowi załącznik nr 1 do Polityki lub na wzorze dostarczonym przez IZ/ IP PO lub podmiot upoważniony;

3. Prowadzenie i aktualizacja wykazu budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe u Beneficjenta, który stanowi załącznik 2 do Polityki lub na wzorze dostarczonym przez IZ/IP PO lub podmiot upoważniony;

4. Analiza i identyfikacja zagrożeń i ryzyka, na które może być narażone przetwarzanie danych osobowych w ramach u Beneficjenta oraz pisemne informowanie o wynikach analizy osoby upoważnione do podejmowania decyzji w imieniu Beneficjenta;

5. Inicjowanie i realizację szkoleń osób zajmujących się przetwarzaniem oraz ochroną danych osobowych u Beneficjenta.

§3

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

§4

1. Obowiązki Administratora Bezpieczeństwa Informacji u Beneficjenta wykonywane są przez osobę upoważnioną do podejmowania decyzji w imieniu Beneficjenta.

2. W przypadku powołania Administratora Systemu u Beneficjenta, nadzór nad wykonywaniem obowiązków Administratora Systemu u Beneficjenta, pełni osoba upoważniona do podejmowania decyzji w imieniu Beneficjenta.

§5

W razie konieczności, w kwestiach związanych z zastosowaniem środków technicznych i organizacyjnych zapewniających ochronę przetwarzania u Beneficjenta danych osobowych, Administrator Bezpieczeństwa Informacji u Beneficjenta konsultuje się i współpracuje z Administratorem Bezpieczeństwa Informacji w IZ/IP PO lub podmiocie upoważnionym.

Rozdział 5

Przetwarzanie danych osobowych

§1

1. Administrator Bezpieczeństwa Informacji u Beneficjenta jest osobą upoważnioną do przetwarzania danych osobowych na mocy pełnionej funkcji.

2. Ponadto do przetwarzania danych osobowych mogą być dopuszczeni jedynie pracownicy posiadający odpowiednie upoważnienie wydane przez upoważnioną do tego osobę. Wzór upoważnienia do upoważnienia danych osobowych oraz wzór odwołania upoważnienia do przetwarzania danych osobowych określone są w załącznikach do umowy o dofinansowanie projektu.

3. Każdy pracownik, przed dopuszczeniem go do przetwarzania danych osobowych, musi być zapoznany z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją.

4. Pracownik potwierdza zapoznanie się z przepisami dotyczącymi ochrony danych osobowych oraz Polityką i Instrukcją przez złożenie podpisu na liście prowadzonej przez Administratora Bezpieczeństwa Informacji u Beneficjenta, której wzór jest określony w załączniku nr 3 do Polityki lub na wzorze dostarczonym przez IZ/IP PO lub podmiot upoważniony.

§2

1. Każdy pracownik mający dostęp do danych osobowych jest wpisywany do rejestru osób upoważnionych do przetwarzania danych osobowych, prowadzonego przez Administratora Bezpieczeństwa Informacji u Beneficjenta.

2. Rejestr, o którym mowa w ust. 1, zawiera:

a) imię i nazwisko pracownika;

b) jego identyfikator w systemie informatycznym służącym przetwarzaniu danych (o ile dotyczy)

c) zakres przydzielonego uprawnienia;

d) datę przyznania uprawnień;

e) podpis Administratora Bezpieczeństwa Informacji u Beneficjenta potwierdzający przyznanie uprawnień;

f) datę odebrania uprawnień;

g) podpis Administratora Bezpieczeństwa Informacji u Beneficjenta potwierdzający odebranie uprawnień.

§3

1. Dopuszczenie do przetwarzania danych osobowych przez osoby niebędące pracownikami, jest możliwe tylko w wyjątkowych przypadkach, po podpisaniu z tą osoby umowy zapewniającej przestrzeganie przepisów dotyczących ochrony danych osobowych. W takim przypadku §1 i 2 Rozdziału 5 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.

§4

1. Wszyscy pracownicy oraz osoby, o których mowa w §3 ust.1 Rozdziału 5, 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.

§5

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. Zabezpieczenia 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 danych osobowych przetwarzanych innym podmiotów, chyba że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
6. Bezzwłocznego zawiadamiania Administratora Bezpieczeństwa Informacji u Beneficjenta o wszelkich przypadkach naruszenia bezpieczeństwa danych, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających te dane osobowe.

§6

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

§1

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

1. Stwierdzono naruszenie zabezpieczenie bazy tych danych;
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 nieuprawione danych osobowych.

§2

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

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

a) poinformować pisemnie o zaistniałym zdarzeniu Administratora Bezpieczeństwa Informacji IZ/IP PO lub podmiot upoważniony i stosować się do jego zaleceń;

b) zapisać wszelkie informacje i okoliczności związane z danym zdarzeniem, a 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 jest zobowiązany niezwłocznie:

a) wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opisać ją 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:

- 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 Bezpieczeństwa Informacji u Beneficjenta lub Administrator Systemu u Beneficjenta, o ile został powołany.

§3

1. Po przywróceniu normalnego stanu bazy 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.

§4

1. Administrator Bezpieczeństwa Informacji u Beneficjenta przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach z naruszenia zabezpieczenia bazy danych i w terminie 21 dni od daty powzięcia wiedzy o naruszeniu zabezpieczenia bazy danych przekazuje go Administratorowi Bezpieczeństwa Informacji u Beneficjenta w IP/IZ PO lub upoważnionym podmiocie.
2. Jeżeli naruszenie zabezpieczenia bazy danych nastąpiło na skutek naruszenia zabezpieczeń systemu informatycznego służącego do przetwarzania danych, Administrator Bezpieczeństwa Informacji 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

§1

1. Bieżąca kontrola nad przetwarzaniem danych osobowych u Beneficjenta jest dokonywana przez Administratora Bezpieczeństwa Informacji u Beneficjenta.

2. W ramach kontroli, o której mowa w ust.1 Administrator Bezpieczeństwa Informacji u Beneficjenta jest zobowiązany do nadzorowania, przestrzegania przez użytkowników wymagań Polityki i Instrukcji.

§2

1. Administrator Bezpieczeństwa Informacji 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 Administrator Bezpieczeństwa Informacji u Beneficjenta uwzględnia informacje zawarte w raportach, o których mowa w §4 Rozdziału 7.

§3

Kontrola, o której mowa w §2, 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 posiadają odpowiednie upoważnienia do przetwarzania danych osobowych wydane przez upoważnioną do tego osobę.

Rozdział 8

Postanowienia końcowe

§1

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

§2

Do spraw nieuregulowanych w Polityce stosuje się przepisy o ochronie danych osobowych zawarte w ustawie i rozporządzeniu.

§3

Polityka nie wyłącza stosowania innych instrukcji dotyczących zabezpieczenia danych osobowych.

§4

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

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

§5

Integralną część niniejszej Polityki stanowią następujące załączniki:

1. Załącznik nr 1 - Rejestr osób upoważnionych do przetwarzania danych osobowych u Beneficjenta;
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 u Beneficjenta.
5. Załącznik nr 5 - Wykaz zbiorów danych wraz ze wskazaniem programów zastosowanych do przetwarzania danych.
6. Załącznik nr 6 - Wzór upoważnienia do przetwarzania danych osobowych
7. Załącznik nr 7 - Wzór odwołania upoważnienia do przetwarzania danych osobowych.
8. Załącznik nr 8 - Rejestr czynności przetwarzania danych.