ZARZĄDZENIE

DYREKTORA ŻORSKIEGO CENTRUM ORGANIZACJI POZARZĄDOWYCH

0120.6.2022 Z DNIA 14.02.2022 r.

W sprawie wprowadzenia Polityki bezpieczeństwa danych osobowych

Na podstawie: wymagań 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) oraz w związku ze zmianami wprowadzonymi Ustawą z dnia 21 lutego 2019 r. o zmianie niektórych ustaw w związku z zapewnieniem stosowania 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).

ZARZĄDZAM

§ 1

1. Wprowadzić do stosowania w Żorskim Centrum Organizacji Pozarządowych Politykę bezpieczeństwa danych osobowych w brzmieniu stanowiącym Załącznik do niniejszego zarządzenia.
2. Do stosowania zasad określonych w Polityce Bezpieczeństwa danych osobowych zobowiązani są wszyscy pracownicy oraz inne osoby mające dostęp do informacji podlegających ochronie.

§ 2

Od dnia wejścia w życie niniejszego Zarządzenia przestaje obowiązywać dotychczasowa Polityka bezpieczeństwa danych osobowych.

§ 3

Zarządzenie wchodzi w życie z dniem podpisania.

Podpisano:

Dyrektor Żorskiego Centrum Organizacji Pozarządowych

Adam Grześkiewicz

Adam Grześkiewicz
DYREKTOR
Żorskiego Centrum
Organizacji Pozarządowych

Załącznik do Zarządzenia Dyrektora Żorskiego Centrum Organizacji Pozarządowych 0120.6.2022 z dnia 14.02.2022 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Administrator danych:

ŻORSKIE CENTRUM ORGANIZACJI POZARZĄDOWYCH

Osiedle Władysława Sikorskiego 52

44-240 Żory

Polityką objęte jest

Centrum Integracji Społecznej w Żorach

z siedzibą w Żorach (44-240), ul. Dworcowa 35

- dla którego Administrator danych jest „ instytucją tworzącą" .

1. Wstęp

Administratorem Danych, który wdraża Politykę Bezpieczeństwa jest **Żorskie Centrum Organizacji Pozarządowych w Żorach.** Niniejsza Polityka jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora danych w celu spełnienia wymagań 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) oraz ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (tj. Dz. U. z 2019 r. poz. 1781).Dokument niniejszy stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z ogólnym rozporządzeniem o ochronie danych, a także usprawnienie i usystematyzowanie organizacji pracy w zakresie zapewnienia bezpieczeństwa danych osobowych przetwarzanych przez Administratora danych.

2. Definicje.

W Polityce przyjmuje się następującą terminologię:

Administrator (danych) - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. W ramach niniejszego dokumentu jest to **Żorskie Centrum Organizacji Pozarządowych w Żorach.**

RODO – 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).

Dane osobowe - to wszelkie informacje związane ze zidentyfikowaną lub możliwą do zidentyfikowania osobą fizyczną. Osoba jest uznawana za osobę bezpośrednio lub pośrednio identyfikowalną przez odniesienie do identyfikatora, takiego jak nazwa, numer identyfikacyjny, dane dotyczące lokalizacji, identyfikator internetowy lub jeden oraz więcej czynników specyficznych określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej o których mowa w art. 4 pkt 1 RODO.

Przetwarzanie oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub

zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie o których mowa w art. 4 pkt 2 RODO.

Ograniczenie przetwarzania - polega na oznaczeniu przetwarzanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania.

Anonimizacja - zmiana danych osobowych, w wyniku której dane te tracą charakter danych osobowych. Jest to proces nieodwracalny.

Pseudonimizacja - oznacza przetwarzanie danych osobowych w taki sposób (np. przez zastępowanie imienia i nazwiska liczbami lub innymi pseudonimami), że danych osobowych nie można już przypisać do określonego podmiotu danych bez użycia dodatkowych informacji (np. listy referencyjnej nazwisk i numerów), pod warunkiem, że takie dodatkowe informacje są przechowywane oddzielnie i podlegają środkom technicznym i organizacyjnym zapewniającym brak dostępu dla osób, które nie mają uprawnień nadanych przez administratora.

Zgoda osoby, której dane dotyczą - oznacza w pełni świadome i dobrowolne oświadczenie lub wyraźne działanie potwierdzające wyrażenie zgody na przetwarzanie danych osobowych przez osobę, której dane dotyczą, przy czym to Administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych. Oceniając, czy zgodę wyrażono dobrowolnie, w jak największym stopniu uwzględnia się, czy między innymi od zgody na przetwarzanie danych nie jest uzależnione wykonanie umowy, w tym świadczenie usługi, jeśli przetwarzanie danych osobowych nie jest niezbędne do wykonania tej umowy.

Ocena skutków w ochronie danych - to proces przeprowadzany przez Administratora, jeśli jest wymagany przez obowiązujące prawo (wykaz rodzajów operacji przetwarzania wymagających oceny skutków opublikowany w Monitorze Polskim), lub w przypadku kiedy ryzyko naruszenia praw i wolności będzie wysokie.

Podmiot danych - osoba fizyczna, której dane dotyczą.

Odbiorca - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią.

Podmiot przetwarzający (procesor) - osoba fizyczna lub prawna, organ publiczny, agencja lub

jakikolwiek inny organ przetwarzający dane osobowe w imieniu Administratora.

Inspektor Ochrony Danych (IOD) - osoba wyznaczona przez Administratora w celu informowania i doradzania Administratorowi w zakresie obowiązującego prawa o ochronie danych oraz w celu monitorowania przestrzegania przepisów o ochronie danych oraz działająca jako punkt kontaktowy dla podmiotów danych, a także organu nadzorczego.

Szczególne kategorie danych osobowych oznaczają informacje na temat pochodzenia rasowego lub etnicznego, poglądów politycznych, przekonań religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, stanu zdrowia, kodu genetycznego, nałogów lub życia seksualnego, skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym.

Profilowanie – jest dowolną formą zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.

Zbiór danych - oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Naruszenie ochrony danych osobowych - jest to przypadkowy lub niezgodny z prawem incydent prowadzący do zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

Organ nadzorczy – Urząd Ochrony Danych Osobowych.

3. Obszar przetwarzania danych osobowych.

1. Żorskie Centrum Organizacji Pozarządowych w Żorach przetwarza dane osobowe gromadzone w zbiorach danych.
2. Dane osobowe domyślnie przetwarzane są na obszarze obejmującym pomieszczenia biurowe, zlokalizowane w Żorach, Osiedle Władysława Sikorskiego 52, oraz w innych budynkach, jeżeli wymagają tego odrębne projekty realizowane przez Administratora.
3. Zgodnie ze statutem Żorskiego Centrum Organizacji Pozarządowych dane osobowe z zakresu reintegracji zawodowej i społecznej przetwarza na rzecz Żorskiego Centrum Organizacji Pozarządowych Centrum Integracji Społecznej.

4. Dodatkowy obszar, w którym przetwarzane są dane osobowe, stanowią wszystkie komputery przenośne oraz inne nośniki danych znajdujące się poza obszarem wskazanym w zdaniu poprzedzającym.

4. Upoważnienia.

1. Administrator upoważnia na piśmie wszystkie osoby, które w zakresie swoich czynności służbowych oraz realizowanych na polecenie administratora zadań mają dostęp do danych osobowych.
2. Osoby upoważnione oraz wszystkie inne osoby, którym udostępnia się dane osobowe zobowiązane są do przetwarzania danych osobowych zgodnie z wymogami prawa oraz zgodnie z postanowieniami Polityki, jak również innych regulaminów lub procedur wewnętrznych związanych z przetwarzaniem danych osobowych.
3. Przy zatrudnianiu Pracowników oraz nadawaniu uprawnień Administrator zapewnia, że:
1) Pracownicy przed przystąpieniem do wykonywania obowiązków służbowych otrzymują należytą wiedzę w zakresie zasad przetwarzania i ochrony danych osobowych;
2) Każda z osób przetwarzających dane osobowe w imieniu i na polecenie Administratora zostaje upoważniona na piśmie do przetwarzania danych osobowych w niezbędnym zakresie, zgodnie z wzorem stanowiącym **załączniki nr 1a lub 1b** do Polityki.
3) Osobom, które mają dostęp do danych osobowych pracowników, w tym danych szczególnej kategorii w związku z realizacją art. 22^{1b} Kodeksu Pracy nadaje się upoważnienie zgodnie ze wzorem stanowiącym **załącznik nr 2** do Polityki;
4) Pracownicy mający dostęp do danych osobowych osób korzystających ze świadczeń w ramach zakładowego funduszu świadczeń socjalnych o których mowa w art. 9 ust. 1 rozporządzenia 2016/679 zgodnie z Art. 8 ust. 1b Ustawy z dnia 4 marca 1994 r. o zakładowym funduszu świadczeń socjalnych, muszą posiadać pisemne upoważnienie do przetwarzania takich danych wydane przez pracodawcę. Osoby dopuszczone do przetwarzania takich danych są obowiązane do zachowania ich w tajemnicy. Wzór upoważnienia stanowi **załącznik nr 3** do Polityki.
4. Administrator odpowiada za nadawanie oraz odbieranie upoważnień do przetwarzania danych osobowych.
5. Każda osoba upoważniona może przetwarzać dane wyłącznie na polecenie Administratora lub na podstawie przepisu prawa.

6. Upoważnienia nadawane są pracownikom, zleceniobiorcom, stażystom oraz innym osobom, które w ramach wykonywania czynności służbowych na rzecz Administratora mają dostęp do danych osobowych.

7. Administrator prowadzi Ewidencję nadanych uprawnień, w której zamieszcza się następujące informacje: imię i nazwisko osoby upoważnionej, zajmowane stanowisko, identyfikator w systemie informatycznym, datę nadania oraz ustania upoważnienia.

8. Nadane upoważnienia do przetwarzania danych osobowych przechowywane są w części B akt osobowych pracownika lub w dokumentacji prowadzonej dla osób wykonujących inne czynności na rzecz administratora (np. dokumentacja praktyk, stażów).

9. Osoba, która przetwarza dane osobowe w systemie informatycznym uzyskuje dostęp do tego systemu poprzez nadanie loginu, jako indywidualnego identyfikatora służącego rozliczalności tego dostępu oraz hasło zabezpieczające.

10. Hasło dostępu należy bezwzględnie chronić i utrzymywać w tajemnicy.

11. Uprawnienie dostępu do systemu informatycznego może uzyskać wyłącznie osoba upoważniona przez administratora do przetwarzania danych osobowych.

12. Loginy podlegają wpisaniu do ewidencji nadanych uprawnień. Dopuszcza się ewidencjonowanie uprawnień z danych środowisk systemowych jako odrębne rejestry.

13. Osoby nie posiadające upoważnienia do przetwarzania danych osobowych, a wykonujące zlecone czynności w fizycznym obszarze przetwarzania (np. sprzątaczka, konserwator) podpisują oświadczenie o poufności według wzoru stanowiącego **załącznik nr 7** do niniejszej Polityki ochrony danych osobowych.

5. Rejestr czynności przetwarzania.

1. Za pośrednictwem rejestru Administrator dokumentuje czynności przetwarzania danych osobowych oraz inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe. Poprzez wskazanie w rejestrze ogólnych środków ochrony danych osobowych objętych wyodrębnioną czynnością przetwarzania, Administrator dąży również do wykazania zgodności przetwarzania danych osobowych z wymogami prawa.

2. Prowadzenie **rejestru czynności przetwarzania** danych ma na celu zapewnienie zgodności z zasadami i warunkami przetwarzania danych osobowych. Dzięki danym zebranym w tym rejestrze administrator może ocenić, w jakim zakresie dotyczą go inne obowiązki wynikające z RODO np. obowiązek przeprowadzenia oceny skutków przetwarzania dla ochrony danych.

3. Rejestr pozwala zatem na stałą weryfikację działalności w zakresie przetwarzania danych osobowych oraz poddawanie ocenie każdego nowo wprowadzanego lub modyfikowanego procesu już na jego najwcześniejszym etapie.

4. W przypadku podjęcia się przez Administratora zadań procesora i przetwarzania danych osobowych powierzonych przez innych administratorów, Administrator prowadzi dodatkowo **rejestr wszystkich kategorii czynności przetwarzania.**

6. Analiza ryzyka.

1. Celem analizy ryzyka jest zastosowanie środków technicznych i organizacyjnych zapewniających stopień bezpieczeństwa odpowiadający ryzyku wynikającemu z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.

2. Administrator musi samodzielnie analizować ryzyko, uwzględniając wiele specyficznych dla niego czynników, takich jak: wielkość, struktura organizacyjna, możliwości techniczne, zakres i rodzaj danych, cel przetwarzania danych.

3. Analiza ryzyka przeprowadzana jest według określonej procedury, która opisuje sposób przeprowadzenia analizy w celu zabezpieczenia danych osobowych adekwatnie do zidentyfikowanych zagrożeń.

7. Zasady ochrony danych.

1. Administrator danych stosuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych, odpowiednie do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności zabezpiecza dane przed ich udostępnianiem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

2. Administrator danych zobowiązany jest do zapewnienia, aby dane osobowe były:

1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu");

3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

4) prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania,

aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

5) przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania");

6) przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

3. Przy zapewnieniu przetwarzania danych osobowych zgodnie z zasadami wskazanymi wyżej Administrator opiera przetwarzanie na następujących podstawach:

1) Legalność – Administrator dba o ochronę prywatności i przetwarza dane osobowe zgodnie z wymogami prawa;

2) Bezpieczeństwo – Administrator zapewnia odpowiedni poziom bezpieczeństwa danych osobowych podejmując stale działania w tym zakresie;

3) Prawa Jednostki – Administrator umożliwia osobom, których dane osobowe przetwarza, wykonywanie swoich praw i prawa te realizuje;

4) Rozliczalność – Administrator zapewnia należyte udokumentowanie sposobu spełniania obowiązków w zakresie ochrony danych osobowych.

8. Bezpieczeństwo danych osobowych.

Administrator zapewnia odpowiedni poziom bezpieczeństwa danych, w tym:

1) przeprowadza analizy ryzyka dla czynności przetwarzania danych lub ich kategorii;

2) przeprowadza oceny skutków dla ochrony danych tam, gdzie ryzyko naruszenia praw i wolności osób jest wysokie;

3) dostosowuje środki ochrony danych do ustalonego ryzyka;

4) stosuje procedury pozwalające na identyfikację, ocenę i zgłoszenie zidentyfikowanego naruszenia ochrony danych Urzędowi Ochrony Danych – zarządza incydentami;

5) dokonuje aktualizacji uprawnień dostępowych przy zmianach w składzie personelu i zmianach ról osób, oraz zmianach podmiotów przetwarzających;

6) wprowadza regulaminy i instrukcje postępowania z danymi osobowymi;

7) stosuje techniki anonimizacji i pseudonimizacji.

9. Zadania oraz status Inspektora Ochrony Danych.

1. Do zadań Inspektora ochrony danych należy w szczególności:

1)informowanie Dyrektora oraz pracowników, którzy przetwarzają dane osobowe o obowiązkach wynikających z rozporządzenia RODO oraz innych przepisów Unii Europejskiej lub państw członkowskich o ochronie danych i doradzanie im w tych sprawach;

2)monitorowanie przestrzegania RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

3)udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

4)współpraca z organem nadzorczym, tj. Urzędem Ochrony Danych Osobowych;

5)pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Administrator jest zobowiązany zgłosić do rejestracji w UODO powołanie i odwołanie Inspektora ochrony danych w terminie 14 dni od jego powołania lub odwołania, jeśli odrębne przepisy nie stanowią inaczej.

3. Administrator publikuje na swojej stronie internetowej dane Inspektora Ochrony Danych, tj. imię i nazwisko oraz adres e-mail do kontaktu.

4. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

5. Administrator zapewnia, by inspektor ochrony danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

6. Administrator wspiera inspektora ochrony danych w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania.

7. Administrator zapewnia, by inspektor ochrony danych nie otrzymywał instrukcji dotyczących wykonywania swoich zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. Inspektor ochrony danych bezpośrednio podlega najwyższemu kierownictwu administratora.

8. Osoby, których dane dotyczą, mogą kontaktować się z inspektorem ochrony danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

9. Inspektor ochrony danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań – zgodnie z prawem Unii lub prawem państwa członkowskiego.

10. Jeżeli Inspektor ochrony danych miałby wykonywać inne zadania i obowiązki, niż wymienione w ust. 1 to Administrator zapewnia, by te zadania i obowiązki nie powodowały konfliktu interesów.

10. Postępowanie z incydentami oraz naruszeniami ochrony danych osobowych

Postępowanie Administratora danych osobowych lub osoby przez niego upoważnionej w przypadku stwierdzenia wystąpienia zagrożenia bezpieczeństwa danych osobowych:

1) ustalenie zakresu i przyczyn zagrożenia oraz jego ewentualnych skutków,
2) w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
3) w razie konieczności zainicjowanie działań dyscyplinarnych,
4) zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
5) udokumentowanie prowadzonego postępowania w rejestrze incydentów i naruszeń bezpieczeństwa danych osobowych zgodnie ze wzorem stanowiącym **załącznik nr 6** do niniejszej Polityki.

Administrator opracowuje szczegółową instrukcję postępowania na wypadek wystąpienia zagrożenia dla bezpieczeństwa przetwarzanych danych osobowych oraz w przypadku naruszenia.

11. Szkolenia.

1. Osoby zatrudnione w obszarze przetwarzania przed dopuszczeniem do pracy z danymi osobowymi zostają zobowiązane przez Administratora do zachowania w tajemnicy przetwarzanych przez siebie danych osobowych. Poufność obowiązuje w trakcie zatrudnienia jak i po jego ustaniu.

2. Osoby zatrudnione w obszarze przetwarzania przed dopuszczeniem do pracy z danymi osobowymi zostają zapoznane z zasadami ochrony danych osobowych - **załącznik nr 4** do Polityki.

3. W przypadku przeprowadzenia szkolenia wewnętrznego z zasad ochrony danych osobowych przez Inspektora Ochrony Danych, wskazane jest udokumentowanie odbycia tego szkolenia.

4. Wewnętrzne szkolenie przypominające zostaje zakończone podpisaniem przez pracownika listy uczestników szkolenia.

12. Audyty

1. Zgodnie z art. 32 RODO, Administrator powinien regularnie testować, mierzyć i oceniać skuteczność środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Audyt przeprowadza Inspektor Ochrony Danych wraz z pracownikiem wyznaczonym przez Administratora.

13. Wykaz podstawowych zabezpieczeń stosowanych przez Administratora danych:

1. Środki organizacyjne:

1) Opracowano i wdrożono Politykę bezpieczeństwa danych osobowych.

2) Do przetwarzania danych dopuszczono wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych.

3) Prowadzona jest ewidencja osób uprawnionych do dostępu do systemów informatycznych.

4) Osoby zatrudnione przy przetwarzaniu danych zaznajomiono z przepisami dotyczącymi ochrony danych osobowych.

5) Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązano do zachowania ich w tajemnicy.

6) Monitory komputerów, na których przetwarzane są dane osobowe, ustawione są w sposób uniemożliwiający wgląd osobom postronnym w przetwarzane dane.

7) Pliki edytorów tekstu lub arkuszy kalkulacyjnych należy traktować jako kopie zbiorów, z których pochodzą przetwarzane w nich dane i odpowiednio zabezpieczać stosując wytyczne zawarte w Polityce bezpieczeństwa.

8) Kopie zapasowe zbioru danych osobowych przechowywane są w innym pomieszczeniu niż to, w którym znajduje się serwer, na którym dane osobowe przetwarzane są na bieżąco.

9) Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane

przed dostępem osób nieupoważnionych.

10) Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.

11) Stosuje się pisemne umowy powierzenia przetwarzania danych dla współpracy z podwykonawcami (procesorami) przetwarzającymi dane osobowe.

12) W każdym przypadku budzącym wątpliwości co do legalności udostępnienia danych osobowych podmiotowi upoważnionemu do otrzymania Administrator udostępnia dane wyłącznie na pisemny wniosek tego podmiotu.

13) W podmiocie prowadzi się zasadę czystego biurka i ekranu oraz zostały określone zasady korzystania z kluczy.

2. Środki ochrony fizycznej danych

1) Dane osobowe przechowywane są w pomieszczeniach zamykanych na klucz.

2) Dane osobowe w formie papierowej są przechowywane w zamkniętych niemetalowych lub metalowych szafach.

3) Po zakończeniu pracy, przed opuszczeniem pomieszczenia stanowiącego obszar przetwarzania danych zamykane są okna oraz wszystkie dokumenty i nośniki informacji umieszczane są w zamykanych szafach bądź biurkach.

4) Kopie zapasowe/archiwalne zbioru danych osobowych przechowywane są w zamkniętej szafie.

5) Zastosowano system ochrony przeciwpożarowej zgodny z instrukcją bezpieczeństwa przeciwpożarowego.

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

3. Środki sprzętowe infrastruktury informatycznej i telekomunikacyjnej

1) Wprowadzono procedurę nadawania i odbierania uprawnień.

2) Dostęp do internetu oraz sieci lokalnej zabezpieczony jest hasłem.

3) Zastosowano urządzenia typu UPS oraz listwy przepięciowe, połączone pomiędzy siecią zasilania a komputerami chroniący system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

4) Dostęp do systemu operacyjnego komputera, w którym przetwarzane są dane osobowe, jest zabezpieczony za pomocą procesu uwierzytelnienia z wykorzystaniem identyfikatora

użytkownika oraz hasła.

5) Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

6) Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

7) Zastosowano programy antywirusowe.

8) Użyto system Firewall do ochrony dostępu do sieci komputerowej.

9) Użytkownicy sytemu przetwarzania danych mający dostęp do zbiorów danych prowadzonych w systemie informatycznym przy użyciu komputerów przenośnych, na których przetwarzane są dane osobowe, zobowiązani są do zabezpieczenia tych komputerów hasłem oraz do stosowania środków ochrony kryptograficznej. Ponadto użytkownicy ci zobowiązani są do zachowania szczególnej ostrożności podczas transportu i użytkowania komputerów przenośnych poza wyznaczonym obszarem przetwarzania danych osobowych.

4. Postępowanie w przypadku klęski żywiołowej

1. Klęską żywiołową jest katastrofa spowodowana działaniem sił przyrody takich jak ogień, huragan, woda lub ich przejawami.

2. W przypadku wystąpienia zagrożenia powodującego konieczność przeprowadzenia ewakuacji osób lub mienia z pomieszczeń, w których przetwarzane są dane osobowe mają zastosowanie przepisy niniejszego rozdziału oraz innych przepisów szczególnych.

3. Każda osoba, która będzie świadkiem zbliżania się lub działania zagrożeń związanych z klęską żywiołową zobowiązana jest powiadomić Administratora w każdy możliwy sposób.

4. Osoby biorące udział w akcji ratunkowej, mają prawo wejść do pomieszczeń, w których przetwarzane są dane osobowe.

5. W przypadku ogłoszenia alarmu ewakuacyjnego użytkownicy przebywający w pomieszczeniach, w których przetwarzane są dane osobowe obowiązani są do przerwania pracy, a w miarę możliwości przed opuszczeniem tych pomieszczeń do:

1)zamknięcia systemu informatycznego;

2) zabezpieczenia danych osobowych przetwarzanych tradycyjnie.

6. W czasie trwania akcji ratunkowej i po jej zakończeniu Administrator Danych Osobowych, oraz obecni użytkownicy powinni w miarę możliwości zabezpieczać dane osobowe przed nieuprawnionym do nich dostępem, o ile nie stoi to w sprzeczności z poleceniami wydanymi przez służby ratunkowe.

14. Polityka czystego biurka

1. Polityka czystego biurka obowiązuje wszystkich pracowników, przy czym za pracownika uważa się każdą osobę zatrudnioną na podstawie umowy o pracę, a także osobę fizyczną wykonującą pracę na innej podstawie niż stosunek pracy.
2. Każdy pracownik zobowiązany jest do przechowywania na biurku tylko tych dokumentów, które są pracownikowi niezbędne w danym momencie pracy do wykonania bieżących zadań.
3. Każdy Pracownik zobowiązany jest do ograniczenia dostępu osób postronnych do danych poufnych, w tym danych osobowych zawartych na nośnikach papierowych wykorzystywanych przez Pracownika przy wykonywaniu obowiązków służbowych.
4. W przypadku opuszczenia przez pracownika – choćby chwilowo – biurka lub stanowiska pracy Pracownik zobowiązany jest do odłożenia i schowania wszystkich wykorzystywanych dokumentów zawierających dane poufne lub dane osobowe do zamykanej szuflady lub szafy, celem uniemożliwienia dostępu do dokumentów osobom postronnym.
5. Na biurku nie mogą znajdować się napoje w pojemnikach grożących rozlaniem płynu.
6. Po zakończonej pracy pracownik zobowiązany jest odłożyć wszystkie dokumenty do zamykanej na klucz szafy.
7. Po zakończonej pracy na biurku mogą znajdować się jedynie telefon i przybory biurowe, takie jak: zszywacz, dziurkacz, długopis, itp.
8. Pracownik zobowiązany jest do niszczenia dokumentów niepotrzebnych w taki sposób, aby nie było możliwe odtworzenie zawartych w nich informacji, np. w niszczarce.

15. Prawa osób, których dane dotyczą.

1. Administrator wdraża metody zarządzania zgodami umożliwiające rejestrację i weryfikację posiadania zgody osoby na przetwarzanie jej konkretnych danych w konkretnym celu, zgody na komunikację na odległość (email, telefon, sms, in.) oraz rejestrację odmowy zgody, cofnięcia zgody i podobnych czynności, takich jak zgłoszenie sprzeciwu lub ograniczenie przetwarzania.
2. Administrator dba o czytelność i styl przekazywanych informacji i komunikacji z osobami, których dane osobowe przetwarza.
3. W przypadku zbierania danych osobowych od osoby, której dane dotyczą oraz w przypadku pozyskiwania ich w sposób inny niż od osoby, której dane dotyczą Administrator wypełnia obowiązek informacyjny zgodnie z art. 13 i 14 RODO.

4. Administrator realizuje również obowiązek informacyjny o przetwarzaniu danych wobec osób niezidentyfikowanych, tam gdzie to jest możliwe poprzez wywieszenie informacji o objęciu obszaru monitoringiem wizyjnym.

5. W celu realizacji praw osoby, której dane osobowe dotyczą Administrator zapewnia procedury i mechanizmy pozwalające zidentyfikować dane konkretnych osób przetwarzane przez Administratora, zintegrować te dane, wprowadzać do nich zmiany i usuwać w sposób zintegrowany.

6. Administrator bez zbędnej zwłoki zawiadamia osobę o naruszeniu ochrony danych osobowych, jeżeli może ono powodować wysokie ryzyko naruszenia praw lub wolności tej osoby.

7. Na żądanie osoby dotyczące dostępu do jej danych, Administrator informuje osobę, czy przetwarza jej dane oraz informuje osobę o szczegółach przetwarzania, zgodnie z art. 15 RODO, a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych.

8. Administrator wydaje osobie, której dane osobowe dotyczą kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych.

9. Administrator dokonuje sprostowania nieprawidłowych danych na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić sprostowania danych chyba, że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga.

10. Administrator uzupełnia i aktualizuje dane na żądanie osoby, której dane osobowe dotyczą. Administrator ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych. Administrator może polegać na oświadczeniu osoby, co do uzupełnianych danych chyba, że będzie to niewystarczające w świetle przyjętych przez Administratora procedur, prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

11. Z uwzględnieniem ust. 12 niżej, na żądanie osoby, Administrator usuwa dane, gdy:

1) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach,

2) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania,

3) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych,

4) dane były przetwarzane niezgodnie z prawem,

5) konieczność usunięcia wynika z obowiązku prawnego,

6) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.

12. Administrator przy usuwaniu danych osobowych uwzględnia, aby zapewnić efektywną realizację tego prawa przy poszanowaniu wszystkich zasad ochrony danych, w tym bezpieczeństwa, a także weryfikację, czy nie zachodzą wyjątki, o których mowa w art. 17. ust. 3 RODO.

13. Administrator dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

1) osoba kwestionuje prawidłowość danych – na okres pozwalający sprawdzić ich prawidłowość,

2) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,

3) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń,

4) osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją – do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

14. W trakcie ograniczenia przetwarzania Administrator przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą chyba, że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego. Administrator informuje osobę przed uchyleniem ograniczenia przetwarzania. W przypadku ograniczenia przetwarzania danych Administrator informuje osobę o odbiorcach danych, na żądanie tej osoby.

15. Sposób realizacji praw osób, których dane dotyczą opisany jest szczegółowo w procedurze obsługi żądań podmiotów danych.

16. Postanowienia końcowe.

1. Polityka jest przechowywana i udostępniana w wersji papierowej w siedzibie Administratora.

2. Administrator w uzupełnieniu do niniejszej Polityki bezpieczeństwa danych osobowych , w celu uszczegółowienia niektórych procedur w niej zawartych, opracowuje i udostępnia do

zapoznania się przez pracowników wyznaczonych do realizowania tych procedur, instrukcje określające szczegółowe zasady postępowania.

3. Wdrożenie odrębnych instrukcji oraz procedur w zakresie przetwarzania danych osobowych wymaga wprowadzenia zarządzeniem dyrektora jednostki.

4. Dopuszcza się prowadzenie rejestrów (np. rejestr nadanych uprawnień, rejestr naruszeń w wersji elektronicznej).

Załączniki do Polityki:

Nr załącznika	Opis załącznika
Załącznik nr 1a	Wzór upoważnienia do przetwarzania danych osobowych - pracownik
Załącznik nr 1b	Wzór upoważnienia do przetwarzania danych osobowych - inna osoba
Załącznik nr 2	Wzór upoważnienia do danych osobowych pracowników
Załącznik nr 3	Wzór upoważnienia do danych osobowych w ramach ZFŚS
Załącznik nr 4	Zasady ochrony danych osobowych
Załącznik nr 5	Wzór ewidencji nadanych uprawnień
Załącznik nr 6	Wzór rejestru incydentów i naruszeń bezpieczeństwa danych osobowych
Załącznik nr 7	Klauzula poufności dla pracowników bez nadanego upoważnienia

Podpisano:

Dyrektor Żorskiego Centrum Organizacji Pozarządowych

Adam Grześkiewicz

Adam Grześkiewicz
DYREKTOR
Żorskiego Centrum
Organizacji Pozarządowych

.....
(Administrator danych)

Upoważnienie do przetwarzania danych osobowych - pracownik

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, zwane dalej RODO, upoważniam Panią / Pana :

imię i nazwisko:.....
zatrudnioną/ ego na stanowisku : .....
do przetwarzania od dnia ..... r. danych osobowych wyłącznie w zakresie wykonywania obowiązków służbowych na stanowisku pracy oraz poleceń przełożonego

Upoważnienie jest ważne do: dnia ustania zatrudnienia / ..... (*)

.....
(Administrator Danych Osobowych)

Ja niżej podpisana/y oświadczam że :

1) przed przystąpieniem do pracy przy przetwarzaniu danych osobowych zostałam/em zaznajomiona/y z przepisami dotyczącymi ochrony danych osobowych, w szczególności z polityką i procedurami obowiązującymi u Administratora;

2) zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w załączniku nr 4 do dokumentacji przetwarzania danych osobowych obowiązującej u Administratora Danych Osobowych oraz zobowiązuje się do ich przestrzegania. Ponadto zobowiązuje się zachować w tajemnicy dane osobowe, które będę przetwarzał/a oraz znane mi sposoby zabezpieczenia danych osobowych przez cały okres zatrudnienia u Administratora Danych Osobowych, jak również po ustaniu zatrudnienia.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów o ochronie danych osobowych.

.....
(osoba upoważniona do przetwarzania danych
- data i podpis)

(*) jeżeli upoważnienie ustaje w innym terminie należy wskazać datę ustania upoważnienia

.....

(Administrator Danych)

Upoważnienie do przetwarzania danych osobowych zlecenie/dzieło/staż/wolontariat/praktyka (*)

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, zwane dalej RODO, upoważniam:

Panią/Pana:.....

wykonującą/cego czynności: .....

.....

do przetwarzania od dnia ..... danych osobowych w zakresie związanym z wykonywaniem wyżej wymienionych czynności .

Upoważnienie udzielane jest na czas realizowania czynności / do dnia ..... (**).

(*) właściwe podkreślić
(**) w razie potrzeby należy wpisać inną datę ustania upoważnienia.

.....
(podpis Administratora)

Ja niżej podpisana/y oświadczam, że :

Zapoznałam/em się i rozumiem zasady dotyczące ochrony danych osobowych opisane w załączniku nr 4 do dokumentacji przetwarzania danych osobowych obowiązującej u Administratora Danych Osobowych oraz zobowiązuje się do ich przestrzegania.

Zobowiązuje się zachować w tajemnicy dane osobowe, które będę przetwarzał/a oraz znane mi sposoby zabezpieczenia danych osobowych przez cały okres obowiązywania upoważnienia oraz po jego ustaniu. Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższymi zobowiązaniami, może być uznane za naruszenie przepisów o ochronie danych osobowych.

.....
(osoba upoważniona do przetwarzania danych

-data i podpis)

.....
(Administrator danych)

UPOWAŻNIENIE DO PRZETWARZANIA DANYCH OSOBOWYCH PRACOWNIKÓW

Data nadania upoważnienia : .....

Data ważności upoważnienia : do ustania stosunku pracy lub odebrania upoważnienia.

Na podstawie art.22^{1b} Kodeksu pracy upoważniam :

Panią/Pana : .....

Stanowisko : .....

do przetwarzania danych osobowych pracowników , w tym danych osobowych o których mowa w art. 9 ust.1 rozporządzenia 2016/679, tj. danych osobowych ujawniających poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia.

Upoważnienie do przetwarzania danych udzielone jest w związku z Pani/Pana zakresem obowiązków służbowych oraz zadań realizowanych w ramach stosunku pracy.

.....
(podpis administratora danych)

Zobowiązuję się do zastosowania zabezpieczających dane osobowe środków technicznych i organizacyjnych stosowanych u administratora danych. Jednocześnie zobowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie wykonywania pracy/realizowania zadań, jak i po jej/ich ustaniu.

.....
(data i podpis osoby upoważnionej)

Załącznik nr 3 do Polityki

.....
(Administrator danych)

UPOWAŻNIENIE
DO PRZETWARZANIA DANYCH OSOBOWYCH

Zakładowy Fundusz Świadczeń Socjalnych

Data nadania upoważnienia : .....

Data ważności upoważnienia : do momentu ustania obsługi ZFŚS / członkostwa w Komisji Socjalnej / lub odebrania upoważnienia.

Niniejszym upoważniam :

Panią/Pana : .....

Stanowisko : .....

do przetwarzania danych osobowych, w tym dotyczących zdrowia, o których mowa w art.9 ust.1 rozporządzenia 2016/679.

Upoważnienie do przetwarzania danych udzielone jest do przetwarzania danych udostępnionych przez osoby uprawnione do korzystania ze świadczeń Zakładowego Funduszu Świadczeń Socjalnych.

.....

(podpis administratora danych)

Zobowiązuję się do zastosowania zabezpieczających dane osobowe środków technicznych i organizacyjnych stosowanych przez administratora danych.

Jednocześnie obowiązuję się do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, zarówno w trakcie wykonywania pracy/realizowania zadań, jak i po jej/ich ustaniu.

.....

(data i podpis osoby upoważnionej)

Zasady ochrony danych osobowych

Osoba, która przetwarza dane osobowe w systemie informatycznym zapoznaje się z zasadami przetwarzania danych osobowych zawartych w części pierwszej i drugiej. Osoby przetwarzające dane w sposób tylko tradycyjny (wersja papierowa) zapoznają się z zasadami przetwarzania zawartymi w części drugiej.

Część I

1. **Zasady bezpiecznego użytkowania komputerów.**
   1) Należy mieć świadomość, że dane osobowe mogą znajdować się na twardych dyskach komputerów stacjonarnych i komputerów przenośnych.
   2) Każdy pracownik zobowiązany jest do zabezpieczenia komputerów przed dostępem osób nieupoważnionych.
   3) Osoba upoważniona ma obowiązek natychmiast zgłosić zagubienie, utratę lub zniszczenie powierzonego mu komputera.
   4) Samowolne zmiany (montaż, demontaż) w wyposażeniu komputera są zabronione.
2. **Zasady korzystania z oprogramowania:**
   1) Osoba upoważniona zobowiązuje się do korzystania wyłącznie z oprogramowania objętego prawami autorskimi.
   2) Instalowanie jakiegokolwiek oprogramowania na komputerach może być dokonane wyłącznie przez osobę upoważnioną lub za jej zgodą.
   3) Zabroniona jest samowolna zmiana parametrów systemu operacyjnego komputera.
   4) Pliki z danymi osobowymi nie powinny być trwale zapisywane na twardych dyskach komputerów, jeżeli komputery nie zapewniają indywidualnego logowania się wszystkich użytkowników. Pliki te powinny być usunięte (skasowane) po ich wykorzystaniu np. do wydruku.
3. **Zasady korzystania z internetu:**
   1) Korzystać z internetu można wyłącznie w celach służbowych, chyba że Administrator wyrazi zgodę na inne cele.
   2) Zabrania się zapisywania na dysk twardy komputera oraz uruchamiania nielegalnych/nielicencjonowanych programów oraz plików pobranych z niewiadomego źródła. Pliki takie powinny być pobierane tylko za każdorazową zgodą Administratora i tylko w uzasadnionych przypadkach.
   3) Osoba upoważniona ponosi odpowiedzialność za szkody spowodowane przez oprogramowanie instalowane z internetu.
   4) Zabrania się wchodzenia na strony, na których prezentowane są informacje o charakterze przestępczym, hakerskim, pornograficznym lub innym zakazanym przez prawo (na większości stron tego typu jest zainstalowane szkodliwe oprogramowanie, infekujące w sposób automatyczny system operacyjny komputera szkodliwym oprogramowaniem).
   5) Nie należy w opcjach przeglądarki internetowej włączać opcji autouzupełniania formularzy i zapamiętywania haseł.
   6) W przypadku korzystania z szyfrowanego połączenia przez przeglądarkę, należy zwracać uwagę na pojawienie się odpowiedniej ikonki (kłódka) oraz adresu www rozpoczynającego się frazą "https:".
   7) Należy zachować szczególną ostrożność w przypadku żądania lub prośby podania kodów, PIN-ów, numerów kart płatniczych przez internet.

4. Zasady korzystania z poczty elektronicznej:
   1) Przesyłanie danych osobowych z użyciem maila może odbywać się tylko przez osoby upoważnione.
   2) W przypadku wysyłania danych osobowych mailem, pliki należy zabezpieczyć hasłem. Hasło należy przesłać odrębnym mailem lub innym kanałem. Rekomendowane jest hasło co najmniej 12 znakowe.
   3) Użytkownicy powinni zwracać szczególną uwagę na poprawność adresu odbiorcy dokumentu.
   4) Nie należy otwierać załączników (np. plików z rozszerzeniem .exe) w mailach nadesłanych przez nieznanego lub znanego nadawcę.
   5) Nie wolno rozsyłać za pośrednictwem maila informacji, które mogą zagrażać systemowi informatycznemu tzw. "łańcuszków szczęścia" itp.
   6) Należy okresowo usuwać niepotrzebne maile ze swoich skrzynek pocztowych.
   7) Podczas wysyłania maili do wielu adresatów jednocześnie, należy użyć metody " ukryte do wiadomości - UDW".
   8) Mail jest przeznaczony wyłącznie do wykonywania obowiązków służbowych, chyba że pracodawca zdecyduje o innych celach użycia.
5. Ochrona antywirusowa:
   1) Zaleca się, aby pracownicy skanowali pliki wprowadzane z zewnętrznych nośników programem antywirusowym.
   2) Zakazane jest wyłączanie systemu antywirusowego podczas pracy systemu informatycznego przetwarzającego dane osobowe.
   3) W przypadku stwierdzenia zainfekowania systemu, Pracownik zobowiązany jest poinformować niezwłocznie o tym fakcie Administratora.
6. Polityka haseł:
   1) Hasło dostępu do programu lub do systemu operacyjnego komputera zawierającego dane osobowe składa się co najmniej z 8 znaków (dużych i małych liter oraz cyfr lub znaków specjalnych). Zalecane jest użycie min. 12 znaków.
   2) Zmiana hasła następuje nie rzadziej, niż co 30 dni oraz niezwłocznie w przypadku podejrzenia, że hasło mogło zostać ujawnione.
   3) Jeżeli zmiany hasła nie wymusza system, wówczas do zmiany hasła zobowiązany jest użytkownik.
   4) Hasła nie mogą być powszechnie używanymi słowami. W szczególności nie należy jako haseł wykorzystywać: dat, imion, nazwisk, inicjałów, numerów telefonów.
   5) Użytkownik zobowiązuje się do zachowania hasła w poufności, nawet po utracie przez nie ważności.
7. Procedura rozpoczęcia, zawieszenia i zakończenia pracy.
   1) Użytkownik rozpoczyna pracę z systemem informatycznym przetwarzającym dane osobowe z użyciem identyfikatora i hasła.
   2) Użytkownik jest zobowiązany do uniemożliwienia osobom niepowołanym odczytanie danych wyświetlanych na monitorach- tzw. Polityka czystego ekranu.
   3) Przed czasowym opuszczeniem stanowiska pracy, użytkownik zobowiązany jest wywołać blokowany hasłem wygaszacz ekranu lub wylogować się z systemu.
   4) Po zakończeniu pracy, użytkownik zobowiązany jest:
      a) wylogować się z systemu informatycznego, a następnie wyłączyć sprzęt komputerowy,
      b) zabezpieczyć stanowisko pracy, w szczególności wszelka dokumentację oraz nośniki, na których znajdują sie dane osobowe.

8. Zasady użytkowania laptopów oraz dysków przenośnych (w tym tablety i smartfony)
   1) Wyłącznie za zgodą Administratora można wynosić laptopy oraz dyski przenośne poza organizację.
   2) Wynoszone poza organizację dane osobowe lub inne dane poufne znajdujące się w laptopie lub dysku przenośnym muszą zostać zaszyfrowane hasłem.
   3) Laptopy oraz dyski przenośne powinny być wykorzystywane tylko do prac służbowych. W przypadku korzystania z komputera przenośnego w innym celu wszystkie dane osobowe przetwarzane na polecenie ADO muszą być zabezpieczone hasłem.
   4) W przypadku kradzieży/zgubienia laptopa lub dysku przenośnego, a także naruszenia ochrony danych osobowych osoba upoważniona zobowiązana jest zgłosić niezwłocznie to zdarzenie ADO.
   5) Osoba upoważniona zobowiązana jest do zabezpieczenia laptopa oraz dysku przenośnego w czasie transportu, a przede wszystkim:
   a) zaleca się przenoszenie laptopa oraz dysku przenośnego w teczce lub aktówce,
   b) zabrania się pozostawiania laptopa oraz dysku przenośnego w samochodzie podczas nieobecności osoby upoważnionej.
   6) Użytkownik laptopa oraz dysku przenośnego jest zobowiązany do regularnego tworzenia kopii bezpieczeństwa danych. Nośniki z takimi kopiami powinny być przechowywane w miejscu zabezpieczonym przed dostępem osób nieupoważnionych.
   7) Pracując na laptopie oraz dysku przenośnym w miejscach publicznych i środkach transportu, osoba upoważniona zobowiązana jest do chronienia wyświetlanych danych osobowych na monitorze przed wglądem osób nieupoważnionych.
   8) Zabrania się logowania do nie zabezpieczonej sieci.
   9) W przypadku uszkodzenia lub zużycia nośnika zawierającego dane osobowe, należy dokonać jego fizycznego zniszczenia lub trwałego usunięcia znajdujących się na nim danych.
   10) Komputery przenośne należy zabezpieczyć przed dostępem osób nieupoważnionych (np. schować w szafach zamykanych na klucz).

Część II

9. Postępowanie z danymi osobowymi w wersji papierowej:
   1) Za bezpieczeństwo dokumentów i wydruków zawierających dane osobowe odpowiedzialne są osoby upoważnione oraz kierownicy właściwych jednostek organizacyjnych.
   2) Dokumenty i wydruki zawierające dane osobowe przechowuje się w pomieszczeniach zabezpieczonych fizycznie przed dostępem osób nieupoważnionych.
   3) Należy stosować " politykę czystego biurka". Polega ona na zabezpieczeniu dokumentów np. w szafach, biurkach, pomieszczeniach przed kradzieżą lub wglądem osób nieupoważnionych.
   4) Niepotrzebne dokumenty oraz tymczasowe wydruki należy niszczyć w niszczarkach niezwłocznie po ustaniu celu ich przetwarzania.
   5) Po zakończeniu pracy należy zabezpieczyć (zamykać na klucz w szafach) dokumenty zawierające dane osobowe oraz zabezpieczyć system informatyczny (wyłączyć komputery).
10. Zapewnienie poufności danych osobowych:
   1) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych, do których ma lub będzie miał dostęp wskazanych w nadanym upoważnieniu.

2) Osoba upoważniona zobowiązana jest do nie wykorzystywania danych osobowych w celach pozasłużbowych bądź niezgodnych ze zleceniem, o ile nie są one jawne.
3) Osoba upoważniona zobowiązana jest do zachowania w tajemnicy sposobów zabezpieczania danych osobowych o ile nie są one jawne.
4) Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym.
5) Zakazuje się przekazywania informacji o danych osobowych osobom nieupoważnionym, np. sytuacjach towarzyskich, pozazawodowych.
6) Zakazuje się wynoszenia dokumentów zawierających dane osobowe poza teren placówki.

11. Postępowanie w przypadku naruszenia ochrony danych osobowych:

1) W przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych należy niezwłocznie powiadomić Administratora.
2) Typowe sytuacje stwierdzenia lub podejrzenia naruszenia ochrony danych:
   a) ślady na drzwiach, oknach i szafach wskazują na próbę włamania,
   b) dokumentacja jest niszczona bez użycia niszczarki,
   c) fizyczna obecność w budynku lub pomieszczeniach osób zachowujących sie podejrzanie,
   d) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
   e) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz organizacji bez pozwolenia Administratora,
   f) udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej,
   g) telefoniczne próby wyłudzenia danych,
   h) kradzież komputerów lub CD/DVD, twardych dysków, pendrive-ów z danymi osobowymi,
   i) maile zachęcające do ujawnienia identyfikatora i/lub hasła,
   j) pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów,
   k) hasła do systemów przyklejone są w pobliżu komputera.

12. Odpowiedzialność porządkowa

Za nieprzestrzeganie zapisów niniejszej Polityki pracownicy podlegają odpowiedzialności porządkowej uregulowanej w przepisach kodeksu pracy, a w przypadku pracowników mianowanych odpowiedzialność za naruszenie obowiązków w zakresie ochrony danych osobowych może podlegać odpowiedzialności porządkowej bądź dyscyplinarnej.

13. Postanowienia końcowe:

Z powyższymi zasadami osoby przetwarzające dane osobowe zostają zapoznane przed dopuszczeniem do przetwarzania, co zostaje potwierdzone oświadczeniem w treści upoważnienia.

Załącznik nr 5 do Polityki

Żorskie Centrum Organizacji Pozarządowych

EWIDENCJA NADANYCH UPRAWNIEŃ DO SYSTEMÓW INFORMATYCZNYCH

LP	IMIĘ I NAZWISKO PRACOWNIKA ZAJMOWANE STANOWISKO	NAZWA PROGRAMU/ APLIKACJAI	NADANY LOGIN	DATA NADANIA	DATA ODEBRANIA

REJESTR INCYDENTÓW I NARUSZEŃ OCHRONY DANYCH OSOBOWYCH

L.P.	Naruszenie bezpieczeństwa – opis incydentu/naruszenia	Źródło zgłoszenia – osoba/podmiot zgłaszający incydent/naruszenie	Data zgłoszenia	Przyczyna	Odpowiedzialny za błąd/naruszenie lub informacja o braku takiej osoby	Działanie zapobiegawcze i korygujące wraz ze wskazaniem osoby odpowiedzialnej za wykonanie	Data zakończenia i ocena skuteczności podjętych działań	Czy naruszenie podlegało zgłoszeniu do UODO (TAK/NIE) oraz data zgłoszenia
1.								
2.								
3.								
4.								
5.								

.....
(imię i nazwisko)

.....
(miejscowość, data)

.....
(zajmowane stanowisko)

OŚWIADCZENIE O POUFNOŚCI

Oświadczam, iż zobowiązuję się do:

- zachowania w tajemnicy danych osobowych, do których mam lub będę miał/a dostęp w trakcie wykonywania zleconych czynności w fizycznym obszarze przetwarzania, a których administratorem/procesorem jest Żorskie Centrum Organizacji Pozarządowych w Żorach.

- zgłaszania wszelkich zauważonych incydentów naruszenia zasad ochrony danych osobowych pracownikowi Żorskiego Centrum Organizacji Pozarządowych w Żorach.

Przyjmuję do wiadomości, iż postępowanie sprzeczne z powyższym zobowiązaniem, może być uznane za naruszenie przepisów o ochronie danych osobowych.

.....
(podpis)