

Świętochłowice, dnia 21.09.2018 r.

Zarządzenie nr 6 / 2018

Dyrektora Centrum Integracji Społecznej w Świętochłowicach

W sprawie: **wprowadzenia/zmiany Polityki Bezpieczeństwa Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach**

§ 1

W związku z przetwarzaniem danych osobowych w zakresie określonym w art. 2 i art. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1), zwanego dalej „rozporządzeniem 2016/679”.

ZARZĄDZAM:

W celu realizacji postanowień Ustawy wprowadzenie dokumentu: „Polityka Bezpieczeństwa Danych Osobowych w Centrum Integracji Społecznej Świętochłowicach ” wraz z załącznikami.

§ 2

Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR
Centrum Integracji Społecznej
w Świętochłowicach

Kamil Wójcik
podpis

Polityka Bezpieczeństwa Przetwarzania Danych Osobowych w Centrum Integracji Społecznej w Świętochłowicach.

Wersja: 1.0	Funkcja	Imię i Nazwisko	Data /podpis
Opracował	Inspektor Ochrony Danych	Mirosław Karwot	<i>Mirosław Karwot</i> Inspektor Ochrony Danych
Zatwierdził	Administrator Danych	Kamil Wójcik	<i>Kamil Wójcik</i> DYREKTOR Centrum Integracji Społecznej w Świętochłowicach
Właściciel:	Centrum Integracji Społecznej w Świętochłowicach	Obowiązuje od:	01.10.2018 <i>Kamil Wójcik</i>

oat niesobow
gp

Spis treści

I.	Postanowienia ogólne	3
II.	Cel powstania dokumentu.....	3
III.	Podstawa prawna oraz zakres obowiązywania	4
IV.	Definicje.....	4
V.	Sposób przechowywania, udostępniania i modyfikacji polityki	7
VI.	Podstawowe zasady przetwarzania danych osobowych.....	8
VII.	Przetwarzanie szczególnych kategorii danych osobowych	9
VIII.	Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa ...	10
IX.	Zgodność przetwarzania z prawem	11
X.	Zasady przetwarzania danych.....	11
XI.	Warunki wyrażenia zgody.....	13
XII.	Odpowiedzialność za bezpieczeństwo danych osobowych, obowiązki Administratora Danych oraz Inspektora Danych Osobowych	13
XIII.	Wymogi i informacje dotyczące ochrony i przetwarzania danych osobowych.....	15
XIV.	Postępowanie w przypadkach stwierdzenia naruszenia ochrony danych osobowych	15
XV.	Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych	16
XVI.	Zmiany i udostępnianie tekstu polityki.....	16
XVII.	Znajomość polityki.....	16
XVIII.	Pozostałe informacje dotyczące systemów informatycznych i baz danych	16
XIX.	Załączniki	16

I. Postanowienia ogólne

1. Polityka bezpieczeństwa zwana dalej „Polityką”, określa środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych oraz sposób przepływu danych pomiędzy poszczególnymi systemami. Zawiera wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe, wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych oraz opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi, a także tryb postępowania w przypadku stwierdzenia naruszenia ochrony danych osobowych w systemach informatycznych lub kartotekach albo w sytuacji zaistnienia podejrzenia o powstaniu takiego naruszenia.
2. Szczegółowe zestawienie przetwarzanych zbiorów osobowych wraz z ich charakterystyką i zawartością merytoryczną, a także opisem pól informacyjnych i wzajemnych zależności występujących pomiędzy poszczególnymi zbiorami, stanowi załącznik nr 17 do Polityki.
3. Obszar fizyczny przetwarzania danych określa szczegółowo załącznik nr 9 do Polityki, zawierający wykaz budynków i pomieszczeń wraz z opisem zabezpieczenia pomieszczenia.
4. Zbiory osobowe przetwarzane są z wykorzystaniem:
 - a) systemu informatycznego oraz informacji udostępnianych z jego wykorzystaniem;
 - b) informacji zgromadzonych i przetwarzanych w formie tradycyjnej.
5. Dostęp do Internetu realizowany jest poprzez stałe łącze.
6. Każde naruszenie zasad Polityki może być uznane za poważne naruszenie podstawowych obowiązków pracowniczych lub wynikających z umów cywilnych o współpracy i może skutkować konsekwencjami, zgodnie z Kodeksem Pracy lub odpowiednimi przepisami regulującymi zasady współpracy, jak również odpowiedzialnością przewidzianą w ustawie o ochronie danych osobowych

II. Cel powstania dokumentu

1. Celem powstania niniejszej Polityki jest realizacja obowiązków wynikających z przepisów dotyczących ochrony danych osobowych, jak również spełnienie wymagań chroniących prywatność i godność osób, których dane osobowe są przetwarzane przez Administratora Danych.
2. Przedmiotem Polityki jest określenie, opisanie i zawarcie w tym i załączonych dokumentach, zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych osobowych objętych ochroną, a w szczególności zabezpieczeń danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniami przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.

III. Podstawa prawna oraz zakres obowiązywania

1. Polityka została przygotowana, aby spełnić wymogi:
 - a. 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) zwane dalej RODO.
 - b. Ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. 2018 poz. 1000).
2. Polityka obowiązuje przy przetwarzaniu wszelkich danych osobowych w Centrum Integracji Społecznych w Świętochłowicach.
3. Sposób postępowania przy przetwarzaniu danych opisany jest w osobnych procedurach i instrukcjach.
4. Podmioty zewnętrzne, które będą przetwarzać dane osobowe na zlecenie Administratora Danych, zobowiązane są opracować własną dokumentację i zabezpieczyć przetwarzane dane osobowe zgodnie z wymogami prawa.

IV. Definicje

1. „Dane osobowe” oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
2. „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;
3. „Ograniczenie przetwarzania” oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
4. „Profilowanie” oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które 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;
5. „Pseudonimizacja” oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych

informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

6. „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;
7. „Administrator” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;
8. „Podmiot przetwarzający” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
9. „Odbiorca” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania;
10. „Strona trzecia” oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
11. „Zgoda” osoby, której dane dotyczą oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
12. „Naruszenie ochrony danych osobowych” oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych;
13. „Dane genetyczne” oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
14. „Dane biometryczne” oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;

15. „Dane dotyczące zdrowia” oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
16. „Główna jednostka organizacyjna” oznacza:
- a) jeżeli chodzi o administratora posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii, a jeżeli decyzje co do celów i sposobów przetwarzania danych osobowych zapadają w innej jednostce organizacyjnej tego administratora w Unii i ta jednostka organizacyjna ma prawo nakazać wykonanie takich decyzji, to za główną jednostkę organizacyjną uznaje się jednostkę organizacyjną, w której zapadają takie decyzje;
 - b) jeżeli chodzi o podmiot przetwarzający posiadający jednostki organizacyjne w więcej niż jednym państwie członkowskim – miejsce, w którym znajduje się jego centralna administracja w Unii lub, w przypadku gdy podmiot przetwarzający nie ma centralnej administracji w Unii – jednostkę organizacyjną podmiotu przetwarzającego w Unii, w której odbywają się główne czynności przetwarzania w ramach działalności jednostki organizacyjnej podmiotu przetwarzającego, w zakresie w jakim podmiot przetwarzający podlega szczególnym obowiązkom na mocy niniejszego rozporządzenia;
17. „Przedstawiciel” oznacza osobę fizyczną lub prawną mającą miejsce zamieszkania lub siedzibę w Unii, która została wyznaczona na piśmie przez administratora lub podmiot przetwarzający na mocy art. 27 do reprezentowania administratora lub podmiotu przetwarzającego w zakresie ich obowiązków wynikających z niniejszego rozporządzenia;
18. „Przedsiębiorca” oznacza osobę fizyczną lub prawną prowadzącą działalność gospodarczą, niezależnie od formy prawnej, w tym spółki osobowe lub zrzeczenia prowadzące regularną działalność gospodarczą;
19. „Grupa przedsiębiorstw” oznacza przedsiębiorstwo sprawujące kontrolę oraz przedsiębiorstwa przez nie kontrolowane;
20. „Wiążące reguły korporacyjne” oznaczają polityki ochrony danych osobowych stosowane przez administratora lub podmiot przetwarzający, którzy posiadają jednostkę organizacyjną na terytorium państwa członkowskiego, przy jednorazowym lub wielokrotnym przekazaniu danych osobowych administratorowi lub podmiotowi przetwarzającemu w co najmniej jednym państwie trzecim w ramach grupy przedsiębiorstw lub grupy przedsiębiorców prowadzących wspólną działalność gospodarczą;
21. „Organ nadzorczy” oznacza niezależny organ publiczny ustanowiony przez państwo członkowskie zgodnie z art. 51;
22. „Organ nadzorczy, którego sprawa dotyczy” oznacza organ nadzorczy, którego dotyczy przetwarzanie danych osobowych, ponieważ:
- a) administrator lub podmiot przetwarzający posiadają jednostkę organizacyjną na terytorium państwa członkowskiego tego organu nadzorczego;

b) przetwarzanie znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, mające miejsce zamieszkania w państwie członkowskim tego organu nadzorczego; lub

c) wniesiono do niego skargę;

23. „Transgraniczne przetwarzanie” oznacza:

a) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności jednostek organizacyjnych w więcej, niż jednym państwie członkowskim administratora lub podmiotu przetwarzającego w Unii posiadającego jednostki organizacyjne w więcej niż jednym państwie członkowskim; albo

b) przetwarzanie danych osobowych, które odbywa się w Unii w ramach działalności pojedynczej jednostki organizacyjnej administratora lub podmiotu przetwarzającego w Unii, ale które znacznie wpływa lub może znacznie wpłynąć na osoby, których dane dotyczą, w więcej niż jednym państwie członkowskim;

24. „Mający znaczenie dla sprawy i uzasadniony sprzeciw” oznacza sprzeciw wobec projektu decyzji dotyczącej tego, czy doszło do naruszenia niniejszego rozporządzenia lub czy planowane działanie wobec administratora lub podmiotu przetwarzającego jest zgodne z niniejszym rozporządzeniem, który to sprzeciw musi jasno wskazywać wagę wynikającego z projektu decyzji ryzyka naruszenia podstawowych praw lub wolności osób, których dane dotyczą, oraz gdy ma to zastosowanie – wagę ryzyka zakłócenia swobodnego przepływu danych osobowych w Unii;

25. „Usługa społeczeństwa informacyjnego” oznacza usługę w rozumieniu art. 1 ust. 1 lit. b) dyrektywy Parlamentu Europejskiego i Rady (UE) 2015/1535 ⁽¹⁾;

26. „Organizacja międzynarodowa” oznacza organizację i organy jej podlegające działające na podstawie prawa międzynarodowego publicznego lub inny organ powołany w drodze umowy między co najmniej dwoma państwami lub na podstawie takiej umowy.

V. Sposób przechowywania, udostępniania i modyfikacji polityki

1. Polityka została zatwierdzona w Centrum Integracji Społecznych w Świętochłowicach w dniu 01.10.2018 jako dokument obowiązujący.
2. Niniejszy dokument powinien być regularnie przeglądany i aktualizowany przez Inspektora Ochrony Danych lub przez Administratora Danych.
3. Zmiany w dokumencie Polityki oraz załącznikach wprowadzane są w chwili pojawienia się ważnych okoliczności lub nowego przepisu, istotnego dla spójności i aktualności Polityki, bądź aktualizacji dotychczasowych przepisów dotyczących ochrony lub przetwarzania danych osobowych. Zmiany zatwierdzane są przez Administratora Danych.
4. Informacje o zmianach podawane są do wiadomości osób uczestniczących w przetwarzaniu danych osobowych poprzez publikację w intranecie lub dokumentach formalnych udostępnianych w ustalony wewnętrznie sposób.
5. W przypadku zatwierdzenia nowej wersji Polityki jest ona drukowana, a wydruk dołączany jest do prowadzonej dokumentacji ochrony danych osobowych. Załączniki są

przechowywane wyłącznie w formie elektronicznej. Ich wydruk następuje tylko w razie zaistnienia takiej konieczności, na zlecenie Administratora Danych lub Inspektora Ochrony Danych.

6. Dokument Polityki, wraz z załącznikami, stanowi tajemnicę Centrum Integracji Społecznej w Świętochłowicach i jest klasyfikowany jako dokument wewnętrzny.

VI. Podstawowe zasady przetwarzania danych osobowych

1. Dane osobowe muszą być:
 - a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
 - b) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane w myśl art. 89 ust. 1 za niezgodne z pierwotnymi celami („ograniczenie celu”);
 - c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
 - d) 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”);
 - e) 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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą („ograniczenie przechowywania”);
 - f) 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”).
2. Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).

VII. Przetwarzanie szczególnych kategorii danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, 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, seksualności lub orientacji seksualnej tej osoby.
2. Ust. 1 nie ma zastosowania, jeżeli spełniony jest jeden z poniższych warunków:
 - a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
 - b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
 - c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
 - d) przetwarzanie dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
 - e) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
 - f) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
 - g) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
 - h) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki

zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia i z zastrzeżeniem warunków i zabezpieczeń, o których mowa w ust. 3;

i) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;

j) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

3. Dane osobowe, o których mowa w ust. 1, mogą być przetwarzane do celów, o których mowa w ust. 2 lit. h), jeżeli są przetwarzane przez – lub na odpowiedzialność – pracownika podlegającego obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe lub przez inną osobę również podlegającą obowiązkowi zachowania tajemnicy zawodowej na mocy prawa Unii lub prawa państwa członkowskiego, lub przepisów ustanowionych przez właściwe organy krajowe.

4. Państwa członkowskie mogą zachować lub wprowadzić dalsze warunki, w tym ograniczenia w odniesieniu do przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

VIII. Przetwarzanie danych osobowych dotyczących wyroków skazujących i naruszeń prawa

1. Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa lub powiązanych środków bezpieczeństwa na podstawie art. 6 ust. 1 wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem Unii lub prawem państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw i wolności osób, których dane dotyczą. Wszelkie kompletne rejestry wyroków skazujących są prowadzone wyłącznie pod nadzorem władz publicznych.

IX. Zgodność przetwarzania z prawem

1. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
 - a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
 - b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
 - e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
 - f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Akapit pierwszy lit. f) nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

X. Zasady przetwarzania danych

1. Obszar przetwarzania danych:
 - 1.1. Przetwarzanie danych osobowych z użyciem sprzętu komputerowego oraz kartotek odbywa się wyłącznie na obszarze wyznaczonym przez Administratora Danych.
 - 1.2. Obszar pomieszczeń Centrum Integracji Społecznej w Świętochłowicach w którym przetwarzane są dane osobowe, obejmuje zarówno miejsca, w których wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające komputerowe nośniki informacji z kopiami zapasowymi danych, stacje komputerowe i inne urządzenia komputerowe).
 - 1.3. Obszar przetwarzania danych osobowych zabezpiecza się przed dostępem osób nieuprawnionych na czas nieobecności w nim osób upoważnionych.
 - 1.4. Pomieszczenia stanowiące obszar przetwarzania danych powinny być zamykane na klucz. Przed opuszczeniem pomieszczeń należy zamknąć okna, a także usunąć z biurka wszystkie dokumenty i nośniki informacji oraz umieścić je w odpowiednich zamykanych szafach.

- 1.5. Szczegółowy wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe, określa Załącznik nr 9 do Polityki.
2. Zbiory i zakres danych osobowych przetwarzanych Centrum Integracji Społecznej w Świętochłowicach.
 - 2.1. Szczegółowe zestawienie przetwarzanych zbiorów wraz z ich charakterystyką i opisem struktury, stanowi załącznik nr 17 do niniejszej dokumentacji.
 - 2.2. Centrum Integracji Społecznej w Świętochłowicach korzysta z oprogramowania Firmy Vulcan Pakiet Finanse Optivum, Płace Optivum, Kadry Optivum, Kasa Optivum, Inwentarz Optivum, Płatnik, FillUp.
 - 2.3. Oprogramowanie wspiera w procesach: kadrowych, księgowych, płacowych.
 - 2.4. W Centrum Integracji Społecznej w Świętochłowicach utworzono i wydzielono następujące zbiory danych osobowych:
 - a) kadry – zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;
 - b) księgowość – zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów;
 - c) dane uczestników CIS – zbiór uczestników CIS; zbiór płac uczestników CIS;
 - d) dokumentacja CIS (obieg dokumentów) - zbiór pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów;
 - e) składnica akt kadry - zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;
 - f) składnica akt księgowość - zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne, zbiór kontrahentów, zbiór płac pracowników, zbiór pracowników;
 - g) składnica akt uczestnicy CIS - zbiór pracowników, zbiór płac pracowników, zbiór uczestników CIS, zbiór płac uczestników CIS, zbiór osób współpracujących z Centrum Integracji Społecznej w oparciu o umowy cywilnoprawne;
 - h) Składnica akt - dokumenty dot. projektów dofinansowanych z źródeł zewnętrznych – zbiór uczestników CIS, zbiór płac uczestników CIS
3. Sposób przepływu danych.
 - 3.1. Przepływ informacji pomiędzy zbiorami danych a systemem informatycznym jest dwukierunkowy (do odczytu i do zapisu).

XI. Warunki wyrażenia zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych.
2. Jeżeli osoba, której dane dotyczą, wyrażą zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem. Część takiego oświadczenia osoby, której dane dotyczą, stanowiąca naruszenie niniejszego rozporządzenia nie jest wiążąca.
3. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wycofać zgodę. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Osoba, której dane dotyczą, jest o tym informowana, zanim wyrazi zgodę. Wycofanie zgody musi być równie łatwe jak jej wyrażenie.
4. 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.

XII. Odpowiedzialność za bezpieczeństwo danych osobowych, obowiązki Administratora Danych oraz Inspektora Danych Osobowych

1. Bezpieczeństwo przetwarzania

1.1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator i podmiot przetwarzający wdrażają odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:

- a) pseudonimizację i szyfrowanie danych osobowych;
- b) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- c) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- d) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

1.2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub

niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

1.3. Wywiązywanie się z obowiązków, o których mowa w ust. 1 niniejszego artykułu, można wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania, o którym mowa w art. 40 lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42.

1.4. Administrator oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo Unii lub prawo państwa członkowskiego.

2. Obowiązki Administratora Danych:

- a) uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, administrator wdraża odpowiednie środki techniczne i organizacyjne, aby przetwarzanie odbywało się zgodnie z niniejszym rozporządzeniem i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
- b) jeżeli jest to proporcjonalne w stosunku do czynności przetwarzania, środki, o których mowa w ust. 1, obejmują wdrożenie przez administratora odpowiednich polityk ochrony danych.
- c) stosowanie zatwierdzonych kodeksów postępowania, o których mowa w art. 40 RODO, lub zatwierdzonego mechanizmu certyfikacji, o którym mowa w art. 42 RODO, może być wykorzystane jako element dla stwierdzenia przestrzegania przez administratora ciężących na nim obowiązków.

3. Zadania Inspektora Ochrony Danych:

- a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
- b) monitorowanie przestrzegania rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;
- c) udzielanie na żądanie zaleceń, co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

- d) współpraca z organem nadzorczym;
- e) 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;
- f) Inspektor Ochrony Danych wypełnia swoje zadania z należyтым uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

XIII. Wymogi i informacje dotyczące ochrony i przetwarzania danych osobowych

1. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są w Centrum Integracji Społecznej w Świętochłowicach dane osobowe jest treścią osobnego dokumentu stanowiącego zał. Nr 9.
2. Wykaz zbiorów danych osobowych wraz z bazami danych w których przetwarzane są dane osobowe jest treścią osobnego dokumentu stanowiącego zał. Nr 17

XIV. Postępowanie w przypadkach stwierdzenia naruszenia ochrony danych osobowych

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołączyć się wyjaśnienie przyczyn opóźnienia.
2. Podmiot przetwarzający po stwierdzeniu naruszenia ochrony danych osobowych bez zbędnej zwłoki zgłasza je administratorowi.
3. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:
 - a) opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
 - b) zawierać imię i nazwisko oraz dane kontaktowe Inspektora Ochrony Danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji,
 - c) opisywać możliwe konsekwencje naruszenia ochrony danych osobowych,
 - d) opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.
4. Jeżeli w zakresie, w jakim informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki

5. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorcemu na zweryfikowanie przestrzegania niniejszego artykułu.

XV. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Administrator Danych wdraża odpowiednie środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.
2. Zalecenia dotyczące możliwości do zastosowania środków określa załącznik nr 20.

XVI. Zmiany i udostępnianie tekstu polityki

1. Dopuszcza się dokonywanie zmian w niniejszym dokumencie oraz dokumentach powiązanych tylko przez osoby upoważnione, na zasadach opisanych w pkt. V Polityki.
2. Tekst niniejszej Polityki wraz z załącznikami zostanie udostępniony osobom przetwarzającym dane, aby mogły się one z nim zapoznać i postępować zgodnie z jej postanowieniami.

XVII. Znajomość polityki

1. Do zapoznania się z niniejszym dokumentem Polityki oraz stosowania zawartych w niej zasad zobowiązane są wszystkie osoby przetwarzające dane osobowe w zbiorze danych osobowych administrowanym przez Administratora danych.

XVIII. Pozostałe informacje dotyczące systemów informatycznych i baz danych

1. Pozostałe informacje dotyczące systemów informatycznych i baz danych są zawarte w „Instrukcji zarządzania systemami informatycznymi, służącymi do przetwarzania danych osobowych”, która stanowi załącznik nr 1 do niniejszej Polityki.

XIX. Załączniki

1. Zał. Nr 1 - Instrukcja zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych.
2. Zał. Nr 2 - Elektroniczny rejestr czynności przetwarzania
3. Zał. Nr 3 - Ocena ryzyka.
4. Zał. Nr 4 - Wykaz kont osób i aplikacji przetwarzających dane osobowe.
5. Zał. Nr 5 - Zgłoszenie naruszenia ochrony danych osobowych do organu nadzorczego.
6. Zał. Nr 6 - Sprawozdanie ze sprawdzenia zgodności przetwarzania danych z przepisami ODO.
7. Zał. Nr 7 - Klauzula zgody.
8. Zał. Nr 8 - Rejestr incydentów naruszenia ochrony danych.
9. Zał. Nr 9 - Wykaz pomieszczeń, w których przetwarzane są dane.
10. Zał. Nr 10 - Zgoda na upublicznienie wizerunku.
11. Zał. Nr 11 - Wykaz udostępnień danych innym podmiotom.



12. Zał. Nr 12 - Wykaz udostępnień danych osobom, których dotyczą.
13. Zał. Nr 13 - Wniosek o udostępnienie danych osobowych.
14. Zał. Nr 14 - Umowa powierzenia przetwarzania danych.
15. Zał. Nr 15 - Wykaz podmiotów, z którymi zawarto umowy powierzenia.
16. Zał. Nr 16 - Upoważnienie do przetwarzania danych osobowych
17. Zał. Nr 17 - Zbiory danych osobowych i ich charakterystyka
18. Zał. Nr 18 - Wykaz przeprowadzonych kontroli
19. Zał. Nr 19 - Oświadczenie pracownika przetwarzającego dane osobowe
20. Zał. Nr 20 - Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych
21. Zał. Nr 21 - Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych
22. Zał. Nr 22 - Zgoda na upublicznienie wizerunku dziecka/podopiecznego
23. Zał. Nr 23 - Klauzula zgody na przetwarzania danych dziecka/podopiecznego
24. Zał. Nr 24 - Rejestr osób upoważnionych do przetwarzania danych osobowych
25. Zał. Nr 25 - Klauzula poufności - firma zewnętrzna

DYREKTOR
Centrum Integracji Społecznej
w Świętochłowicach
Kamil Wójcik

Mirosław Karwot
Inspektor Ochrony Danych