Fundacja OPEN MIND
ul. Średzka 39a/4 54-001 Wrocław
tel. +48 71 733 44 31
e-mail: biuro@fundacjaopenmind.pl

REGON 02 199 2442
NIP 899 27 38 982
KRS 0000 435843
www.fundacjaopenmind.pl

POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Aktualizacja na dzień 25.05.2018 r.

§ 1 POSTANOWIENIA OGÓLNE

1. Niniejsza Polityka bezpieczeństwa została opracowana w celu zapewnienia zgodności procesu przetwarzania danych osobowych z obowiązującymi przepisami prawa, w szczególności z Rozporządzeniem 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 ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. poz. 1000).
2. Celem Polityki bezpieczeństwa przetwarzania danych osobowych przez Fundację OPEN MIND zwanej dalej „POLITYKĄ" jest wskazanie podstaw dla właściwego wykonania obowiązków Administratora danych w zakresie bezpieczeństwa i prawidłowej ochrony przetwarzanych danych osobowych.
3. Polityka określa zasady przetwarzania danych osobowych oraz ich zabezpieczenia, jako zbiór reguł i zaleceń, regulujących sposób ich zarządzania, ochrony i przetwarzania.
4. Polityka zawiera zestaw informacji dotyczących szacowania procesów przetwarzania danych osobowych oraz obowiązujących zabezpieczeń technicznych i organizacyjnych, zapewniających właściwą ochronę przetwarzania danych osobowych.
5. Opracowaną Politykę stosuje się do danych osobowych:
   a) przetwarzanych w systemach informatycznych,
   b) przetwarzanych na nośnikach elektronicznych,
   c) przetwarzanych w sposób tradycyjny

§ 2 DEFINICJE I POJĘCIA ZAWARTE W POLITYCE

1. Wszystkie pojęcia i definicje zawarte w Polityce są powiązane z innymi dokumentami w zakresie ochrony danych osobowych.
2. Określenia użyte w Polityce oznaczają:
   a) **Administrator** – Fundacja OPEN MIND z siedzibą we Wrocławiu (54-001) przy ul. Średzkiej 39a/4, wpisana do Rejestru Stowarzyszeń, innych Organizacji Społecznych i Zawodowych, Fundacji oraz Samodzielnych Publicznych Zakładów Opieki Zdrowotnej pod numerem KRS: 0000435843, NIP: 899 27 38 982, REGON: 02 199 2442. Jednostka, która samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych i odpowiada za ich bezpieczeństwo. W sprawie danych osobowych należy kontaktować się z Wioletą Król, w następujący sposób:
      a. *e-mail: rodo@krzywykomin.pl,*
      b. *korespondencyjnie: Centrum Rozwoju Zawodowego Krzywy Komin, ul. Dubois 33-35a, 50-207 Wrocław, należy wpisać na kopercie dopisek „Rodo"*
   b) **Autentyczność** – właściwość oznaczająca, że zawartość zasobu informacyjnego oraz tożsamość osoby mającej dostęp do tego zasobu, jest taka jak deklarowana;
   c) **Bezpieczeństwo danych** – stan, w którym informacja jest chroniona przed wieloma różnymi zagrożeniami w taki sposób, aby zapewnić ciągłość prowadzenia działalności, zminimalizować straty i zagwarantować zachowanie jej poufności, integralności i dostępności, a dodatkowo również autentyczności, rozliczalności, niezaprzeczalności i niezawodności;
   d) **Dane osobowe** (dane) – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, w rozumieniu przepisów RODO tj. osoby, 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;

e) **Dostępność danych** – właściwość zapewniająca, że osoby upoważnione mają dostęp do informacji i związanych z nimi zasobów na żądanie i w określonym czasie;
f) **Hasło** – ciąg znaków literowych, cyfrowych lub innych znany jedynie użytkownikowi;
g) **Identyfikator** – ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujących osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym;
h) **Incydent bezpieczeństwa** - każde wykryte naruszenie (albo wykryta próba) naruszenia bezpieczeństwa informacji, będące naruszeniem obowiązujących przepisów wewnętrznych lub przepisów prawa, źródłem incydentu bezpieczeństwa może być zarówno przypadkowe, jak i celowe działanie albo zaniechanie;
i) **Integralność danych** – właściwość zapewniająca dokładność i kompletność informacji oraz metod jej przetwarzania;
j) **Integralność systemu** – właściwość zapewniająca nienaruszalność systemu i niemożności jakiejkolwiek modyfikacji w sposób nieuprawniony;
k) **Instrukcja zarządzania systemem informatycznym** – instrukcja określająca sposób zarządzania systemem informatycznym służącym do przetwarzania danych osobowych, która została przyjęta i wdrożona w Biurze, stanowiąca obok Polityki, podstawowy dokument z zakresu ochrony danych osobowych;
l) **Naruszenie ochrony danych osobowych** – 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;
m) **Niezaprzeczalność danych** – właściwości pozwalająca na ustalenie, że uczestnictwo danej osoby w całości lub części wymiany danych jest niepodważalne, w szczególności poprzez zapewnienie niezaprzeczalności otrzymania danych rozumianej jako zdolność systemu do udowodnienia, że adresat informacji otrzymał ją w określonym miejscu i czasie oraz niezaprzeczalności odbioru danych rozumianej jako zdolność systemu do udowodnienia, że nadawca informacji faktycznie ją nadał lub wprowadził do systemu w określonym miejscu i czasie;
n) **Niezawodność danych** – właściwość pozwalająca na ustalenie, że zamierzone zachowania i skutki są spójne;
o) **Nośnik danych** – nośnik taki jak papier, płyta, dysk twardy, karta pamięci lub inny, służący do przechowywania i zapisu danych;
p) **Personel** - osoby - zatrudnione w Biurze na podstawie stosunku pracy, umów cywilnoprawnych, przedsiębiorcy wykonujący osobiście i jednoosobowo działalność, osoby odbywające staże, praktyki - wykonujące prace związane z przetwarzaniem danych osobowych;
q) **Podmiot przetwarzający** – osoba upoważniona do przetwarzania danych osobowych w imieniu Biura;
r) **Poufność danych** - właściwość zapewniająca, że informacja nie jest ujawniana podmiotom do tego nieuprawnionym;
s) **Przetwarzanie danych osobowych** – operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub każde innego rodzaju udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie lub niszczenie;
t) **Pseudonimizacja** – przetworzenie danych osobowych w taki sposób, by nie można ich już było przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, przechowywanych osobno i objętych środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;
u) **RODO** – Rozporządzenie Parlamentu Europejskiego i Rady UE 2016/679 z dnia 27 kwietnia 2016r., 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);

v) **Ustawa** – ustawa o ochronie danych osobowych z 10 maja 2018 r. o ochronie danych osobowych Dz.U. z 2018 r., poz. 1000;
w) **Rozliczalność** - możliwość jednoznacznego przypisania działań danej osoby tylko tej osobie;
x) Biuro – Centrum Rozwoju Zawodowego Krzywy Komin, mieszczące się we Wrocławiu (50-207_ przy ul. Dubois 33/35a, którego Administrator jest zarządcą i operatorem programowym;
y) **System informatyczny** – system współpracujących z sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;
z) **Udostępnianie danych** – przekazywanie, ujawnianie, rozpowszechnianie danych osobowych odbiorcy danych;
aa) **Usuwanie danych** – zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą;
bb) **Uwierzytelnianie** – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu;
cc) **Użytkownik** – członek personelu Biura, upoważniony na piśmie do przetwarzania danych osobowych albo inna osoba, która w imieniu lub za zgodą Biura upoważniona jest do przetwarzania danych osobowych, której nadano identyfikator lub przyznano hasło dostępu do systemu informatycznego;
dd) **Zbiór danych** – uporządkowany i posiadający określoną strukturę zestaw danych osobowych, dostępnych według określonych kryteriów, niezależnie od tego, czy jest on zcentralizowany czy zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie;
ee) **Zgoda** (osoby której dane dotyczą) – dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, wyrażone poprzez oświadczenie bądź wyraźne działanie potwierdzające, którym osoba fizyczna, której dane dotyczą, przyzwala na przetwarzanie dotyczących jej danych osobowych.

§ 3 PRZESŁANKI LEGALIZUJĄCE PRZETWARZANIE DANYCH OSOBOWYCH

1. Dane osobowe w Biurze są:
   a) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty;
   b) zbierane w celach konkretnych, wyraźnie określonych i prawnie uzasadnionych i nie mogą być przetwarzane w sposób niezgodny z tymi celami;
   c) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
   d) prawidłowe, uaktualniane w razie potrzeby, a także usuwane lub prostowane w razie ustalenia, że są nieprawidłowe w świetle celu ich przetwarzania;
   e) przechowywane w formie ułatwiającej identyfikację osoby, której dane dotyczą przez okres nie dłuższy niż jest to niezbędne dla celów, w jakich następuje ich przetwarzanie, z zastrzeżeniem wyjątków przewidzianych w RODO;
   f) przetwarzane w sposób zapewniający ich integralność i poufność, a także rozliczalność.
2. Przetwarzanie danych osobowych jest zgodne z prawem, jeśli:
   a) osoba, której dane dotyczą wyraziła na to zgodę;
   b) przetwarzanie jest niezbędne do wykonania umowy łączącej Biuro z osobą, której dane dotyczą, w szczególności do wykonania umów z usługodawcami, członkami personelu lub innymi osobami związanymi ze Biurem stosunkiem prawnym;
   c) przetwarzanie jest niezbędne do podjęcia działań na żądanie osoby, której dane dotyczą;
   d) przetwarzanie jest niezbędne do wypełnienia ciążącego na Biurze obowiązku prawnego;
   e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym;
   f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Biuro lub przez osobę trzecią, z wyłączeniem sytuacji określonych w RODO;
   g) przetwarzanie jest niezbędne dla ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;

h) przetwarzanie jest niezbędne do wykonania zadań realizowanych na podstawie umów zawartych z ZUS, NFZ, a także innych umów, jakie w przyszłości mogą zostać zawarte między Administratorem a podmiotami publicznymi w rozumieniu przepisów powszechnie obowiązującego prawa.

3. Przesłanki, legalizujące przetwarzanie danych osobowych mogą wystąpić samodzielnie i niezależnie od siebie, albo jednocześnie i łącznie.
4. Administrator informuje osobę, której dane dotyczą o podstawie przetwarzania jej danych osobowych, a w przypadkach określonych w ust. 2 pkt g również o podstawie przetwarzania danych osobowych innej osoby fizycznej. Realizacja obowiązku informacyjnego może polegać na umieszczeniu informacji w miejscu ogólnie dostępnym, w siedzibie Biura albo na jego stronie internetowej.

§ 4 OBOWIĄZKI ADMINISTRATORA DANYCH OSOBOWYCH

1. Administrator zobowiązany jest do podjęcia wszelkich działań, których celem jest zapewnienie prawidłowej ochrony danych osobowych, w szczególności zapewnienie przetwarzania danych ze szczególną starannością realizując następujące zasady:
   a) przetwarzanie zgodnie z przepisami prawa;
   b) zbieranie danych dla określonych celów i nie poddawanie dalszemu przetwarzaniu niezgodnie z tymi celami;
   c) dane będą merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
   d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, jednak nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
   e) zabezpieczenie środkami technicznymi i organizacyjnymi, które zapewnią rozliczalność, poufność i integralność.
2. W Biurze stosuje się zabezpieczenie, którego celem jest zmniejszenie ryzyka poprzez obniżenie prawdopodobieństwa zrealizowania zagrożenia lub też minimalizacja strat związanych ze zrealizowanym zagrożeniem: program antywirusowy, anonimizacja, pseudonominizacja, procedury bezpieczeństwa.

§ 5 AKTUALIZACJA DOKUMENTACJI ZWIĄZANEJ Z OCHONĄ DANYCH OSOBOWYCH

1. Niniejsza Polityka oraz wszystkie dokumenty z nią powiązane będą aktualizowane wraz ze zmianami w przepisach prawa dotyczącymi ochrony danych osobowych oraz zmianami wynikającymi z organizacji i funkcjonowania Biura.
2. W przypadku potrzeby wynikającej ze zdarzeń związanych z naruszeniem ochrony danych osobowych należy dostosować dokumentację do właściwych procedur, które w sposób skuteczny będą chroniły dane osobowe.
3. W każdym przypadku zmiany zapisów niniejszej Polityki wymagają aktualizacji innych dokumentów powiązanych z Polityką.
4. O wszelkich zmianach w dokumentacji powinien być informowani Użytkownicy.

§ 6 ZARZĄDZANIE OCHRONĄ DANYCH OSOBOWYCH

1. Celem właściwej realizacji zamierzeń a także skutecznej ochrony danych osobowych należy stosować następujące obowiązki:
   a) przeszkolić personel uprawniony do przetwarzania danych osobowych w zakresie zasad bezpieczeństwa;
   b) przypisać użytkownikom określonych cech pozwalających na ich identyfikację w systemach informatycznych, dających możliwość dostępu do przetwarzania danych osobowych odpowiednio do zakresu upoważnienia;
   c) okresowo kontrolować użytkowników sposób postępowania przy przetwarzaniu danych osobowych;
   d) w przypadku stwierdzonych nieprawidłowości podejmować stosowne działania celem ich wyeliminowania;

e) na bieżąco wdrażać nowe rozwiązania organizacyjne i techniczne, które wzmocnią bezpieczeństwo przetwarzania danych osobowych.

2. W procesie nadzoru należy szczególnie uwzględniać zabezpieczenie w zakresie integralności, poufności oraz rozliczalności przetwarzania danych osobowych.
3. W procesie zarządzania należy stosować działania, które spowodują, że personel, użytkownicy zewnętrzni będą:
   a) odpowiednio przygotowani i wprowadzeni do przetwarzania danych osobowych;
   b) zapoznają się z obowiązującymi procedurami i zasadami przetwarzania danych osobowych w Biurze;
   c) na bieżąco informowani o wszelkich zmianach w procedurach.

§ 7 ODPOWIEDZIALNOŚĆ ADMINISTRATORA DANYCH OSOBOWYCH

1. Administrator jest odpowiedzialny za prawidłowe przetwarzanie danych osobowych i ich ochronę zgodnie z obowiązującymi przepisami prawa. Ponadto jest obowiązany do stosowania odpowiednich procedur zapewniających prawidłowe przetwarzanie danych osobowych, a także za zapewnienie ochrony przed zmianą, uszkodzeniem zniszczeniem danych osobowych przez nieuprawnioną osobę.
2. Do kompetencji Administratora należy:
   a) określenie celów oraz strategii działań w zakresie ochrony danych osobowych,
   b) podział zadań i obowiązków związanych z organizacją ochrony danych osobowych.
3. Do obowiązków Administratora należy:
   a) zapewnienie szkoleń dla personelu w zakresie przepisów o ochronie danych osobowych oraz zagrożeń związanych z ich przetwarzaniem;
   b) opracowanie i wdrożenie dokumentacji związanej z ochroną danych osobowych w biurze;
   c) nadawanie upoważnień personelowi oraz użytkownikom zewnętrznym do przetwarzania danych osobowych;
   d) zapewnienie ochrony fizycznej pomieszczeń, w których są przetwarzane dane osobowe;
   e) zapewnienie ochrony danych osobowych przetwarzanych w systemach informatycznych oraz nieinformatycznych;
   f) prowadzenie i aktualizacja rejestru czynności i rejestru kategorii przetwarzania.

§ 8 ODPOWIEDZIALNOŚĆ PERSONELU I UŻYTKOWNIKÓW SYSTEMU

1. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa przetwarzania danych osobowych konieczne jest szczególne zaangażowanie ze strony każdego użytkownika w zakresie ochrony danych osobowych.
2. Użytkownicy zobowiązani do informowania o wszelkich podejrzeniach naruszenia lub zauważonych naruszeniach oraz słabościach systemu przetwarzającego dane osobowe bezpośrednio do ADO.
3. Użytkownicy są zobowiązani do:
   a) postępowania zgodnie z Polityką,
   b) zachowania w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia,
   c) ochrony danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem.
4. Wykonywania niezbędnych działań i w procesie przetwarzania danych celem zapewnienia właściwej ich ochrony, w tym celu powinni:
   a) przestrzegać procedur związanych z otwieraniem i zamykaniem pomieszczeń, a także z wejściem do obszarów przetwarzania danych osobowych osób nieupoważnionych,
   b) informować Administratora o podejrzanych osobach poruszających się w obszarze przetwarzania danych osobowych,
   c) użytkownicy powinni na podstawie dokonanej identyfikacji ewentualnych zagrożeń, przedkładać Administratorowi projekty i propozycje nowych rozwiązań, których celem jest zwiększenie poziomu bezpieczeństwa ochrony danych osobowych.

§ 9 ODPOWIEDZIALNOŚĆ ZA NARUSZENIE ZASAD OCHRONY DANYCH OSOBOWYCH

Rozporządzenie ogólne o ochronie danych osobowych a także Kodeks Karny określają odpowiedzialność personelu w przypadku naruszenia ochrony danych osobowych.

§ 10 SZKOLENIA

1. Przed rozpoczęciem przetwarzania danych osobowych każdy użytkownik, stażysta, praktykant itp. powinien zostać przeszkolony przez Administratora. Szkolenie powinno obejmować następujące zagadnienia:
   a) obowiązujące przepisy w zakresie o ochronie danych osobowych;
   b) procedury oraz zasady przetwarzania danych osobowych;
   c) procedury dotyczące bezpiecznego przetwarzania danych osobowych w systemach informatycznych;
   d) zasady użytkowania oprogramowania, urządzeń i systemów informatycznych służących do przetwarzania danych osobowych;
   e) rodzaje zagrożeń jakie mogą być związane z przetwarzaniem danych osobowych w systemach informatycznych;
   f) zasady dostępu do pomieszczeń, w których przetwarzane są dane osobowe;
   g) zasady i sposób postępowania w przypadku naruszenia ochrony danych osobowych lub systemu informatycznego;
   h) odpowiedzialność w przypadku naruszenia ochrony danych osobowych.

2. Po przeszkoleniu każda osoba podpisuje oświadczenie o odbytym szkoleniu i zapoznaniu się z przepisami prawa (oświadczenie stanowi załącznik nr 3 do Polityki).
3. Administrator prowadzi ewidencję osób przeszkolonych (załącznik nr 1 do Polityki)

§ 11 ZASADY SZCZEGÓLNEJ STARANNOŚCI

Każdy Użytkownik dla właściwego sposobu i zasad przetwarzania danych osobowych zobowiązany jest do zachowania szczególnej staranności przy przetwarzaniu danych osobowych, a w szczególności:
1. stosowanie wszelkich metod zabezpieczeń wynikających z Polityki;
2. zabezpieczenie wydruków elektronicznych, a także tych, które mogą być tworzone w trakcie kserowania, kopiowania, skanowania;
3. udzielanie informacji zawierających dane osobowe tylko osobom, podmiotom uprawnionym;
4. prowadzenie rozmów telefonicznych w sposób bezpieczny, tak aby osoba nieuprawniona nie pozyskiwała informacji, jeżeli nie jest ona dla niej przeznaczona.

§ 12 MIEJSCA I POMIESZCZENIA PRZEZNACZONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Dane osobowe można przetwarzać wyłącznie w miejscach bezpiecznych i będących pod właściwym nadzorem osoby, która przetwarza i nadzoruje przetwarzanie danych osobowych.
2. Pomieszczenia bezpieczne to takie, które nie są pozostawione bez nadzoru odpowiedzialnego użytkownika.
3. Pomieszczenia, w których są przetwarzane dane osobowe są zamykane na klucz podczas nieobecności osoby upoważnionej/nadzorującej.
4. Obiekt, jak i inne pomieszczenia, są zabezpieczone fizycznie zgodnie z obowiązującymi procedurami i potrzebami.
5. W przypadku wykonywania prac naprawczych, remontowych, montażowych przez firmy zewnętrzne, pomieszczenie jest pod stałym nadzorem osoby upoważnionej.

6. Przechowywanie kopii zapasowych powinno być realizowane w innym pomieszczeniu niż znajdują się zasoby podstawowe.
7. Każdy użytkownik w przypadku zauważenia uchybień w zabezpieczeniu pomieszczenia zobowiązany jest niezwłocznie poinformować o tym fakcie ADO.

§ 13 UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Przetwarzanie danych osobowych jest możliwe wyłącznie po uzyskaniu przez personel upoważniony do przetwarzania danych osobowych podpisanego przez Administratora.
2. Wzór upoważnienia stanowi załącznik nr 2 do Polityki.
3. Administrator prowadzi dla personelu szkolenia z zakresu obowiązujących przepisów prawa i procedur zawartych w Polityce.
4. Personel po przeszkoleniu podpisuje oświadczenie o zapoznaniu się z przepisami i procedurami.
5. Wzór oświadczenia stanowi załącznik nr 3 do Polityki.
6. Upoważnienie oraz oświadczenie jest przechowywane w dokumentacji Administratora.

§ 14 EWIDENCJA OSÓB UPOWAŻNIONYCH

1. Administrator prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.
2. Ewidencja jest prowadzona na bieżąco.
3. Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych w Biurze stanowi załącznik nr 1 do Polityki.

§ 15 REJESTR CZYNNOŚCI PRZETWARZANIA

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, który zawiera:

   a) imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów, a także gdy ma to zastosowanie – przedstawiciela administratora;
   b) cele przetwarzania;
   c) opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych;
   d) kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych;
   e) informację o przekazaniu danych osobowych do państwa trzeciego lub organizacji międzynarodowej, z podaniem nazwy tego państwa trzeciego lub organizacji międzynarodowej i innych informacji wynikających z RODO;
   f) planowane terminy usunięcia poszczególnych kategorii danych, chyba że nie jest to możliwe „z góry";
   g) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, zgodnych z RODO.

2. Administrator w razie powierzenia mu przetwarzania danych osobowych przez inny podmiot będący administratorem danych, prowadzi rejestr kategorii przetwarzania dokonywanych w imieniu tego innego administratora, który zawiera:
   a) imię i nazwisko lub nazwę oraz dane kontaktowe podmiotu przetwarzającego lub podmiotów przetwarzających oraz każdego administratora, w imieniu którego dane są przetwarzane;
   b) kategorie przetwarzań dokonywanych w imieniu każdego z administratorów;
   c) ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, stosowanych w celu ochrony danych osobowych.
3. Rejestr prowadzony jest w formie pisemnej lub elektronicznej. Wzór rejestru czynności przetwarzania stanowi załącznik nr 6 do Polityki.

§ 16 REJESTR PRZETWARZANIA DANYCH I REJESTR KATEGORII PRZETWARZANIA

1. Personel powinien w porozumieniu z Administrator współpracować w zakresie zgłaszania lub aktualizacji rejestru przetwarzania danych osobowych.
2. Administrator prowadzi rejestr czynności przetwarzania danych i rejestr kategorii przetwarzania.

§ 17 UDOSTĘPNIANIE DANYCH OSOBOWYCH – ZASADY, PROCEDURY

1. Udostępnianie danych osobowych odbywa się na zasadzie potrzeby koniecznej.
2. Udostępnianie danych osobowych zewnętrznym podmiotom uprawnionym odbywa się na pisemny wniosek.
3. Udostępnianie danych osobowych innym podmiotom odbywa się po uzyskaniu zgody osoby, od której uzyskano dane osobowe lub w oparciu o obowiązujące przepisy.
4. W przypadku udostępniania danych osobowych na zewnątrz Administrator dokonuje oceny sposobu przygotowania danych, a także analizuje sposób i prawidłowość przygotowania danych do udostępnienia.
5. Dane osobowe przekazywane na zewnątrz są przekazywane listem poleconym za zwrotnym poświadczeniem odbioru lub innym bezpiecznym sposobem określonym wymogami prawa lub umową.
6. Fakt udostępnienia danych należy udokumentować pisemnie poprzez wykonanie pisma przewodniego lub notatki urzędowej.

§ 18 DOSTĘP, SPROSTOWANIE I USUNIĘCIE DANYCH OSOBOWYCH

1. Administrator danych osobowych na wniosek osoby, której dane dotyczą umożliwia jej dostęp do danych oraz udziela informacji w zakresie określonym w ogólnym rozporządzeniu o danych osobowych.
2. Administrator danych osobowych na żądanie osoby, której dane dotyczą dokonuje sprostowania danych osobowych lub ich uzupełnienia. Osoba jest zobowiązana do złożenia żądania w formie pisemnej.
3. Administrator danych osobowych po złożeniu wniosku przez osobę , której dane dotyczą ma obowiązek usunięcia jej danych osobowych w przypadku gdy:
   a) dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
   b) osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie i nie ma innej podstawy prawnej przetwarzania;
   c) osoba, której dane dotyczą, wnosi sprzeciw wobec przetwarzania; 4) dane osobowe były przetwarzane niezgodnie z prawem;
   d) dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator.

§ 19 POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Powierzenie danych osobowych odbywa się na zasadach określonych w ustawie.
2. Powierzenie danych występuje wówczas, gdy podmiot zewnętrzny ma dostęp do danych osobowych przetwarzanych przez Biuro.
3. Administrator może powierzyć innemu podmiotowi współpracującemu z Biurem na zasadzie wynikającej z umowy powierzenia. Wzór umowy stanowi załącznik nr 9 do polityki.
4. Umowę powierzenia należy zawrzeć na piśmie, umowa powinna zawierać następujące warunki i zawierać:
   a) cel i zakres przetwarzania danych osobowych;
   b) sposoby zabezpieczenia danych i zasady ich przetwarzania;
   c) zasady organizacyjne i techniczne, jakie powinien spełnić podmiot, któremu powierzono przetwarzanie danych osobowych;

d) odpowiedzialność podmiotu, któremu powierzono dane osobowe za nieprawidłowe przetwarzanie danych osobowych;
e) prawo do kontroli podmiotu, któremu powierzono dane osobowe przez przedstawiciela Biura.

§ 20 ZASADY POSTĘPOWANIA W PRZYPADKU NARUSZENIA LUB PODEJRZENIA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Użytkownicy są zobowiązani do szczególnej staranności przy przetwarzaniu danych osobowych.
2. Użytkownicy każdorazowo przed przystąpieniem do pracy są zobowiązani do dokonania oceny i oględzin miejsca pracy pod kątem, czy nie dokonano jakichkolwiek nieuprawnionych działań związanych z ochroną danych osobowych przez osoby nieuprawnione.
3. Sytuacje, na które należy zwrócić szczególną uwagę to:

   a) próba nieuprawnionego dostępu do pomieszczenia lub dostępu do danych osobowych;
   b) naruszenie lub próba naruszenia integralności, poufności lub rozliczalności danych i systemu;
   c) niezamierzona zmiana lub utrata danych zapisanych na nośnikach jako kopie zapasowe;
   d) próba nieuprawnionego logowania lub inny sygnał wskazujący na próbę lub działanie wskazujące na nielegalny dostęp do systemu;
   e) losowe zdarzenia, takie jak brak zasilania, pożar itp.;
   f) stwierdzenie braku sprzętu informatycznego, jego części lub nośników zewnętrznych zawierających dane osobowe (wydruki, pamięć zewnętrzna, płyty CD, dysk twardy, itp.).
4. W sytuacji, gdy użytkownicy stwierdzą naruszenie lub próby naruszenia ochrony danych osobowych, wówczas są zobowiązani do niezwłocznego poinformowania o tym fakcie Administratora.
5. Przed poinformowaniem Administratora o naruszeniu lub próbie naruszenia ochrony danych osobowych, użytkownik jest zobowiązany do:

   a) wstrzymania pracy, a także wykonywania jakichkolwiek działań, które mogłyby utrudnić ocenę i analizę stwierdzonych działań związanych z naruszeniem ochrony danych osobowych;
   b) zabezpieczenia materiałów, dokumentów, aby uniemożliwić dostęp osobom nieuprawnionym i dalsza stratę;
   c) wykonywania wskazówek Administratora.

6. Administrator powinien:

   a) dokonać oceny sytuacji, szczególnie dokonać oględzin stanowiska pracy, pomieszczenia, stanu zabezpieczenia pomieszczenia, potencjalne skutki związane z naruszeniem ochrony danych osobowych;
   b) podjąć dalsze działania stosowne do potrzeb i zaistniałej sytuacji.

7. Administrator jest zobowiązany do sporządzenia raportu z naruszenia ochrony danych osobowych (wzór raportu stanowi załącznik nr 7 do Polityki).
8. Administrator jest zobowiązany w terminie 72 godzin po stwierdzeniu naruszenia, zgłosić takie naruszenie organowi nadzorczemu, chyba że jest mało prawdopodobne, by takie naruszenie skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.
9. Sytuacja związana z naruszeniem lub próbą naruszenia ochrony danych osobowych powinna być przedmiotem analizy i wniosków celem uniemożliwienia podobnych zdarzeń w przyszłości.

§ 21 ZBIORY DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane są w zbiorach z wykorzystaniem systemów informatycznych lub w formie papierowej.
2. Zbiory danych osobowych są zlokalizowane w pomieszczeniach Biura.

§ 22 OCHRONA DANYCH OSOBOWYCH W ZBIORACH NIEINFORMATYCZNYCH

1. Zbiory i dane przetwarzane w tych zbiorach to takie dane, które są przetwarzane w formie tradycyjnej bez wykorzystywania systemów informatycznych.
2. Dane osobowe w formie dokumentów i wydruków podlegają ochronie, a także odpowiedniemu ich zabezpieczeniu w meblach biurowych zamykanych na klucz.
3. Dokumenty, wydruki podlegające zniszczeniu należy zniszczyć skutecznie, tak by osoba nieuprawniona nie mogła zapoznać się z treścią tych dokumentów lub wydruków.
4. W trakcie niszczenia dokumentów należy przestrzegać przepisów prawa.

§ 23 POSTANOWIENIA KOŃCOWE

W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy rozporządzenia ogólnego o ochronie danych osobowych i innych ustaw.

ZAŁĄCZNIKI

1. Załącznik nr 1 – Wzór: Ewidencja osób upoważnionych do przetwarzania danych osobowych.
2. Załącznik nr 2 – Wzór: Upoważnienie do przetwarzania danych.
3. Załącznik nr 3 – Wzór: Oświadczenie pracownika.
4. Załącznik nr 4 – Wzór odwołania upoważnienia.
5. Załącznik nr 5 – Wzór umowy powierzenia.
6. Załącznik nr 6 – Wzór umowy poufności.
7. Załącznik nr 7 – Raport – wzór.
8. Załącznik nr 8 – Bazy danych.
9. Załącznik nr 9 – Rejestr powierzeń i udostepnień.
10. Załącznik nr 10 – Polityka czystego biurka.
11. Załącznik nr 11 – Rejestr przetwarzania danych osobowych.
12. Załącznik nr 12 – Rejestr kategorii przetwarzania