POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH ZWIĄZKU STOWARZYSZEŃ CENTRUM AKTYWNOŚCI

Spis treści

I. Cel PBDO

Działalność każdego podmiotu, którego siedziba lub też działalność zlokalizowane są na terenie Unii Europejskiej wiąże się z przetwarzaniem danych osobowych. Przyjęcie wewnętrznej regulacji, która związana jest przede wszystkim z zasadą rozliczalności wskazanej w Rozporządzeniu 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 z dnia 10 maja 2018 r. o ochronie danych osobowych.

PBDO ukierunkowana jest na przestrzeganie zasad ochrony danych osobowych w tym danych samych pracowników Związku, ale przede wszystkim danych osobowych podmiotów biorących udział w poszczególnych projektach.

Związek Stowarzyszeń Centrum Aktywności, zwany dalej "CAS" lub "Związkiem", zobowiązuje się do ochrony danych osobowych zgodnie z obowiązującymi przepisami prawa oraz najlepszymi praktykami ochrony prywatności. Niniejsza polityka bezpieczeństwa danych osobowych stanowi integralną część działań CAS w zakresie ochrony informacji, w tym danych osobowych, które są przetwarzane w ramach jego działalności.

CAS przetwarza dane osobowe w celu realizacji swojego statutowego zadania wspierania rozwoju społecznego i gospodarczego miasta Mikołowa oraz całego powiatu mikołowskiego. Dane te mogą być również przetwarzane w celu wykonania umów, prowadzenia działań społecznych oraz wypełniania obowiązków prawnych.

CAS zapewnia odpowiednie środki bezpieczeństwa w celu ochrony przetwarzanych danych osobowych przed nieuprawnionym dostępem, utratą, uszkodzeniem lub nieuprawnionym ujawnieniem. Wdrożono procedury zarządzania bezpieczeństwem informacji oraz regularnie przeprowadza się audyty bezpieczeństwa.

Dostęp do danych osobowych mają jedynie upoważnione osoby zatrudnione w CAS, które są zobowiązane do zachowania poufności. Dane osobowe mogą być udostępniane tylko w zakresie niezbędnym do realizacji określonych celów przetwarzania, zgodnie z obowiązującym prawem.

CAS może współpracować z innymi organizacjami pozarządowymi, biznesem, organami administracji państwowej i samorządowej oraz grupami nieformalnymi. Współpraca ta obejmuje również wymianę danych osobowych, która odbywa się zgodnie z obowiązującymi przepisami prawa i w ramach zawartych umów.

Jako przedsiębiorstwo społeczne, CAS priorytetowo traktuje cele społeczne nad osiąganiem zysków. Zyski uzyskane z działalności gospodarczej są przeznaczane na realizację działań statutowych oraz wspieranie reintegracji społecznej i zawodowej pracowników zagrożonych ubóstwem lub wykluczeniem społecznym.

CAS aktywnie angażuje się w zatrudnianie osób zagrożonych ubóstwem, umożliwiając im rzeczywiste uczestnictwo w zarządzaniu przedsiębiorstwem społecznym oraz wspierając ich reintegrację społeczną i zawodową.

Niniejsza polityka bezpieczeństwa danych osobowych jest stale monitorowana i aktualizowana, aby dostosować się do zmieniających się wymagań prawnych oraz zapewnić skuteczną ochronę danych osobowych przetwarzanych przez CAS.

II. Słownik pojęć i skrótów

1. Pojęcia

a) 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 Europejskiej lub w prawie państwa członkowskiego, to również w prawie Unii Europejskiej lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania;

b) Anonimizacja - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, w ten sposób, iż proces ma charakter nieodwracalny, wskutek czego określone dane tracą przymiot danych osobowych;

c) CAS - Związek Stowarzyszeń Centrum Aktywności, Rynek 2, 43-190 Mikołów, NIP: 6351862747, KRS: 0000985840, REGON: 522750665;

d) **Dane osobowe** - oznaczają wszelkie 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;

e) Inspektor ochrony danych –osoba wyznaczona przez Administratora zgodnie z art. 37 RODO- w ramach niniejszej polityki zadania IOD realizowane są przez koordynatora ODO;

f) Koordynator ODO – koordynator ochrony danych osobowych;

g) 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;

h) Ocena skutków dla ochrony danych - proces przeprowadzany przez Administratora, dokonywany przed podjęciem przetwarzania, w przypadku, gdy istnieje prawdopodobieństwo wysokiego ryzyka naruszenia praw i wolności osób fizycznych i zachodzi wraz z wykorzystaniem nowych technologii, biorąc pod uwagę charakter, zakres, kontekst i cele przetwarzania. Proces ten musi ocenić wpływ planowanych operacji przetwarzania na ochronę danych osobowych;

i) Pracownik - osoba świadcząca pracę w CAS na podstawie stosunku pracy lub na podstawie innego formalnego i udokumentowanego instrumentu prawnego (np. umowa cywilnoprawna, odbywanie stażu, praktyki, wolontariatu);

j) Podmiot danych - osoba fizyczna, której dane są przetwarzane;

k) Podmiot przetwarzający (procesor) - osoba fizyczna lub prawna, organ publiczny, jednostką lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora, jako podmiot przetwarzający rozumiane są również dalsze podmioty przetwarzające;

1) Przetwarzanie - 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 innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

l) Pseudonimizacja - 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;

m) Szczególne kategorie danych osobowych - dane, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, członkostwo w związkach zawodowych i obejmują przetwarzanie danych genetycznych, dane biometryczne w celu jednoznacznej identyfikacji osoby fizycznej, dane dotyczące zdrowia, dane dotyczące życia seksualnego osoby lub orientację seksualną;

n) Zarząd CAS – Zarząd Związku Stowarzyszeń Centrum Aktywności działający zgodnie z zasadami reprezentacji CAS lub osoba upoważniona przez Zarząd CAS.

2. Skróty

a) ADO – Administrator Danych Osobowych;
b) PBDO - Polityka Bezpieczeństwa Danych Osobowych;
c) PUODO - Prezes Urzędu Ochrony Danych Osobowych;
d) 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) (Dz. Urz. UE L z 04.05.2016 r.);
e) UODO - Ustawa z dnia 10 maja 2018 r o ochronie danych osobowych.

III. Postanowienia ogólne

A. ADO wyznacza koordynatora ODO oraz jest upoważniony do wyznaczania wszelkich innych funkcji wskazanych w PBDO.
B. Wszyscy Pracownicy CAS są zobowiązani do stałej współpracy z koordynatorem ODO w zakresie ochrony danych osobowych.
C. Zobowiązuje się wszystkich Pracowników do stosowania i przestrzegania niniejszej PBDO.
D. Przetwarzanie danych osobowych z pominięciem uregulowań wynikających z przepisów prawa powszechnie obowiązującego oraz niniejszej PBDO, jest zabronione.

IV. Zasady przetwarzania danych

Dane osobowe muszą być przetwarzane w zgodzie z następującymi zasadami:

A. **zgodności z prawem** - co oznacza obowiązek przetwarzania danych osobowych na podstawie przesłanek legalności wskazanych w art. 6 i art. 9 RODO;
B. **rzetelności i przejrzystości** - co oznacza, że dane osobowe muszą być przetwarzane rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą, w szczególności poprzez prawidłową realizację obowiązków informacyjnych;
C. **ograniczenia celu przetwarzania danych** - co oznacza, że dane osobowe muszą być zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami, przy czym dalsze przetwarzanie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych nie jest uznawane za niezgodne z pierwotnymi celami;

D. **minimalizacji danych -** co oznacza, że dane osobowe muszą być przetwarzane w sposób adekwatny, stosowny oraz ograniczony do tego, co niezbędne do celów, w których są przetwarzane;
E. **prawidłowości -** co oznacza, że dane osobowe muszą być 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;
F. **ograniczenia przechowywania -** co oznacza, że dane osobowe muszą być 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, z zastrzeżeniem, że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą. 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[1], w określonych przypadkach dane będą zanonimizowane lub pseudonimowane w przypadku braku wymagań identyfikowalności;
G. **integralności i poufności -** co oznacza, że dane osobowe muszą być 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,
H. **dostępności -** co oznacza, że dane osobowe muszą być zabezpieczone przed ich zniszczeniem, a działanie systemów informatycznych ma zapewnić, aby dane osobowe były dostępne dla osób upoważnionych wtedy, gdy ich potrzebują lub będą potrzebować.

V. Role w systemie ochrony danych

A. Zarząd CAS

Zarząd CAS jako podmiot kierujący działalnością CAS sprawuje bezpośredni nadzór nad realizacją obowiązków wynikających z przepisów o ochronie danych osobowych oraz obowiązków wynikających z niniejszej PBDO oraz innych dokumentów określających zasady i odpowiedzialność w obszarze ochrony danych osobowych.

Zarząd (przy wsparciu koordynatora ODO) odpowiedzialny jest za:

[1] W przypadku danych pseudonimizowanych, do których CAS nie posiada klucza identyfikacyjnego, nie występuje obowiązek takiego przetwarzania, które umożliwiałoby identyfikację osoby, której dane dotyczą

1. stosowanie zasad opisanych w PBDO, a także w innych dokumentach określających środki techniczne i organizacyjne oraz zasady wpływające na bezpieczeństwo przetwarzania danych osobowych;
2. nadzorowanie Pracowników w zakresie opisanym w pkt 1;
3. prowadzenie bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony danych osobowych a w przypadku stwierdzenia konieczności aktualizacji przyjętych rozwiązań, niezwłoczne informowanie koordynatora ODO o tym fakcie;
4. monitorowanie aktualności przepisów merytorycznych wpływających na realizację zadań odnoszących się albo mających wpływ na procesy przetwarzania danych osobowych;

B. **Koordynator ODO**

Odpowiedzialny jest w szczególności za:

1. prowadzenie oraz aktualizowanie rejestru czynności przetwarzania danych osobowych oraz rejestru kategorii czynności przetwarzania
2. informowanie ADO, podmiotów przetwarzających oraz osób wykonujących pracę o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów prawa powszechnie obowiązującego w zakresie ochrony danych osobowych oraz doradzanie im w tej sprawie;
3. monitorowanie przestrzegania RODO, innych przepisów prawa powszechnie obowiązującego w zakresie ochrony danych osobowych oraz polityk ADO w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość,
4. szkolenie personelu uczestniczącego w operacjach przetwarzania lub organizowanie takich szkoleń;
5. przeprowadzanie audytów i kontroli ochrony danych osobowych lub zlecanie takich audytów lub kontroli;
6. udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 ust. 2 RODO;
7. monitorowanie przesyłania cząstkowych rejestrów czynności przetwarzania danych osobowych oraz rejestrów kategorii czynności przetwarzania przez Pracowników;
8. współpracę z PUODO oraz 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
9. współuczestniczenie w przeprowadzaniu analiz ryzyka w obszarze przetwarzania danych osobowych,
10. uczestniczenie w przygotowaniu umów powierzenia przetwarzania danych osobowych, umów dalszego powierzenia przetwarzania danych osobowych, umów

udostępnienia danych osobowych, umów o współadministrowaniu danymi osobowymi oraz innych instrumentów prawnych regulujących przekazywanie danych do podmiotów trzecich.

11. .

C. Pracownicy

Osoby wykonujące pracę odpowiedzialne są w szczególności:

1. za stosowanie zasad opisanych w PBDO, a także innych dokumentach określających środki techniczne i organizacyjne wpływające na bezpieczeństwo przetwarzania danych osobowych;
2. Współpracę z Kierownikami KO i Koordynatorami ODO;
3. Ochronę danych osobowych:
   a) przed dostępem do nich osób nieuprawnionych,
   b) przed przypadkowym lub umyślnym zniszczeniem, utratą lub modyfikacją.

VI. Zasady rozliczalności i ustalania uprawnień

A. Ogólne zasady

1. Uprawnionymi do przetwarzania danych osobowych są jedynie Pracownicy CAS.
2. Wszystkie osoby mające dostęp do danych osobowych zobowiązane są przetwarzać te dane zgodnie z przepisami o ochronie danych osobowych oraz według zasad zawartych w PBDO i powiązanych z nią dokumentach.
3. Zakres uprawnień poszczególnych osób do przetwarzania danych osobowych (polecenie i upoważnienie) obejmuje działania tych osób niezbędne do realizacji przydzielonych im zadań. Zadania te ustalone są w szczególności w:

   a) Stosownych procedurach lub zasadach wewnętrznych CAS;
   b) Umowie stanowiącej podstawę nawiązania stosunku pracy lub innej umowie, na podstawie której realizowane są usługi na rzecz CAS.

4. Wszelkie inne działania dotyczące przetwarzania danych osobowych mogą być wykonywane tylko na podstawie poleceń bezpośrednich przełożonych, wydanych zgodnie z obowiązującym procedurami lub zasadami wewnętrznymi CAS lub umową stanowiącej podstawę nawiązania stosunku pracy lub innej umowie, na podstawie której realizowane są usługi na rzecz CAS.
5. W przypadku gdy zbiory danych powierzonych CAS na określonej podstawie prawnej (jak np. zgoda na wykorzystanie danych z placówek szkolnych), które to dokumenty wprost wskazują osoby, do których powinien zostać ograniczony krąg Pracowników którym ten zbiór danych zostanie udostępniony.

6. Wskazanie uprawnień, o których mowa w ust. 3, następuje poprzez wniosek składany przez odpowiedzialnego merytorycznie za dany proces Pracownika, który jest przekazywany do koordynatora ODO w celu weryfikacji konieczności wydania w imieniu ADO polecenia i upoważnienia do przetwarzania danych osobowych w sposób określony we wniosku.
7. Wniosek nie ma określonej formy, ale powinien być zrealizowany w formie emailowej lub pisemnej, określać cel i przyczynę wydania dodatkowego upoważnienia.
8. Bieżący nadzór nad Pracownikami i osobami przetwarzającymi dane osobowe w zakresie wykonywania przez nie tylko tych czynności przetwarzania, które są niezbędne do realizacji przydzielonych im zadań, należy do bezpośrednich przełożonych tych osób.

VII. Czynności przetwarzania danych osobowych

A. Pracownicy zobowiązani są do identyfikowania następujących zdarzeń dotyczących przetwarzania danych osobowych oraz zawiadamiania o nich koordynatora ODO, to jest:

1. potrzeby podjęcia, bądź podjęcia nowych czynności przetwarzania;
2. potrzeby dokonania, bądź dokonania zmiany w dotychczasowych czynnościach przetwarzania, w szczególności dotyczących: celu i zakresu przetwarzania, współadministratorów, odbiorców danych, podmiotów przetwarzających dane;
3. potrzeby zawarcia umów powierzenia przetwarzania danych osobowych, także w przypadkach, gdy CAS jest podmiotem przetwarzającym na rzecz innego podmiotu oraz potrzeby zawarcia umów o udostępnieniu danych osobowych lub współadministrowaniu danymi osobowymi lub innych instrumentów prawnych regulujących przekazywanie danych do podmiotów trzecich,
4. potrzeby spełnienia, bądź spełnienia obowiązku informacyjnego wobec Podmiotów danych.

B. W CAS prowadzony jest rejestr czynności przetwarzania danych osobowych oraz rejestr kategorii czynności przetwarzania. Rejestry prowadzone są w formie elektronicznej.
C. ADO może zdecydować o konieczności wprowadzenia dodatkowych rejestrów jako odpowiednich środków organizacyjnych mających zapewnić, aby przetwarzanie odbywało się zgodnie z RODO. Inicjatywa wprowadzenia dodatkowego rejestru może pochodzić od koordynatora ODO.
D. Pracownicy zobowiązani są niezwłocznie do przekazywania koordynatorowi ODO informacji o zmianach w rejestrach, o których mowa w literze B.
E. Szczegółowy, minimalny zakres informacyjny rejestrów określają:
   1. załącznik nr 1 – Rejestr czynności przetwarzania;
   2. załącznik nr 2 – Rejestr kategorii czynności przetwarzania.
F. ADO może poszerzyć zakres informacji gromadzonych w rejestrach. Poszerzenie zakresu informacji gromadzonych w rejestrach nie wymaga zmiany PBDO.

VIII. Zasady rozliczalności dla systemów informatycznych

A. W przypadku zmiany przez osobę posiadającą konto w systemie informatycznym, w którym przetwarzane są dane osobowe, jej dotychczasowe uprawnienia w tym systemie powinny być zmienione na podstawie udokumentowanego (formalnych dokumentów wydanych przez np. Zarząd, które potwierdzać będą określone uprawnienia) wskazania nowych uprawnień przez przełożonego lub Zarząd. Nie dotyczy to poczty elektronicznej. Przyjmuje się, iż okres dotyczący uzyskania formalnych uprawnień nie powinien trwać dłużej niż 7 dni roboczych.
B. Uprawnienia w systemach informatycznych powinny być adekwatne do zakresu obowiązków wynikających z dokumentów dotyczących Pracownika.
C. W zakres uprawnień osoby posiadającej konto w systemie informatycznym zaangażowane mogą być inne organy CAS w zależności od przedmiotu przetwarzanych danych osobowych (np. sprawy kadrowe).

IX. Zasady ochrony technicznej i organizacyjnej

A. W celu zapewnienia bezpieczeństwa danych osobowych stosuje się ogólne środki ochrony takie jak:
   1. możliwość przebywania osób nieuprawnionych do dostępu do danych osobowych, w pomieszczeniach, w których odbywa się przetwarzanie danych, wyłącznie w obecności osoby wykonującej pracę na rzecz CAS lub innej osoby uprawnionej działającej na rzecz CAS;
   2. przechowywanie dokumentów i informatycznych nośników danych zawierających dane osobowe w sposób uniemożliwiający ujawnienie tych danych osobom nieupoważnionym;
   3. przetworzenie zbędnych dokumentów sporządzonych w formie papierowej lub danych na nośnikach informatycznych zawierających dane osobowe w sposób uniemożliwiający odczytanie tych danych, w szczególności przed zbyciem lub oddaniem do dyspozycji podmiotowi innemu niż osobie odpowedzialnej za wsparcie IT, lub ich skuteczna likwidacja;
   4. przechowywanie danych osobowych z zastosowaniem ochrony kryptograficznej (szyfrowanie) w przypadkach przenośnych informatycznych nośników danych (np. karty pamięci, pendrive, płyty, dyski twarde, komputery przenośne, itp.) lub innych adekwatnych zabezpieczeń w przypadku braku możliwości lub utrudnień w zastosowaniu technik szyfrowania, z wyłączeniem kopii zapasowych wykonywanych przez administratorów systemów informatycznych i przechowywanych w warunkach zapewniających inne skuteczne zabezpieczenia lub innych adekwatnych zabezpieczeń w przypadku braku możliwości lub utrudnień w zastosowaniu technik szyfrowania;
   5. zestawienia, wykazy lub rejestry zawierające dane osobowe, zwłaszcza zawierające szczególne kategorie danych osobowych (tzw. dane osobowe wrażliwe) mogą być

przekazywane do podmiotów zewnętrznych pocztą elektroniczną lub na nośniku informatycznym jedynie z zastosowaniem ochrony kryptograficznej (szyfrowanie), o ile taka komunikacja przez podmiot zewnętrzny jest obsługiwana;

6. zastosowanie dodatkowych zabezpieczeń (np. kod dostępu) dla urządzeń drukujących, które nie mają zapewnionego nadzoru osoby wykonującej pracę na rzecz CAS,
7. pseudonimizacja lub anominizacja w zależności od potrzeby zastosowania określonego procesu.

B. Przetwarzanie danych osobowych w systemach informatycznych odbywa się przy zapewnieniu najwyższego stopnia rozliczalności w zakresie dostępu, wprowadzania i edycji danych, lub innych czynności pozwalających zidentyfikować osobę, która dokonywała przetwarzania danych osobowych.
C. Każda osoba posiadająca dostęp do systemu informatycznego ma prawo do wykonywania w tym systemie tylko tych czynności, które są konieczne do realizacji zadania lub polecenia służbowego wydanego zgodnie z procedurami wewnętrznymi CAS i innymi dokumentami wewnętrznymi oraz do których jest uprawniona. Wszelkie przekroczenia lub próby przekroczenia przyznanych uprawnień traktowane będą, jako naruszenie niniejszej PBDO oraz podstawowych obowiązków służbowych.
D. Systemy informatyczne służące do przetwarzania danych osobowych muszą być zabezpieczane przed nieuprawnionym dostępem poprzez zapewnienie w nich mechanizmu wymuszającego tworzenie indywidualnych kont i przyznawanie niepowtarzalnych identyfikatorów oraz stosowanie haseł lub innych metod uwierzytelniania.
E. Systemy muszą umożliwiać różnicowanie zakresu praw dostępu ich użytkowników do danych i funkcji systemu.
F. W uzupełnieniu obowiązujących w tym zakresie dokumentów wewnętrznych CAS, Administrator dokłada staranności w celu ustalenia się ogólnych warunków funkcjonowania infrastruktury teleinformatycznej, a w szczególności zwraca uwagę na:
    1. obowiązkowe stosowanie ochrony wewnętrznych sieci komputerowych na stykach z siecią publiczną poprzez dedykowane do tej ochrony rozwiązania teleinformatyczne;
    2. zapewnienie dla krytycznej infrastruktury informatycznej (np. serwery, macierze dyskowe) pomieszczeń spełniających powszechnie przyjęte normy w tym zakresie oraz zapewnienie odpowiedniego poziomu jej niezawodności oraz redundantność;
    3. wykonywanie kopii zapasowych, zapewniających integralność i odpowiednią aktualność danych w nich zawartych, w szczególności kopie zapasowe powinny:
        a) zabezpieczać dane przed ich utratą, nieuprawnioną zmianą, zniszczeniem;
        b) gwarantować możliwość szybkiego i integralnego odtworzenia danych;
        c) być przechowywane w sposób bezpieczny i w różnych lokalizacjach fizycznych;

4. stosowanie ochrony wszystkich komputerowych stanowisk pracy, serwerów oraz urządzeń sieci komputerowej przed działaniem szkodliwego oprogramowania i zakłóceniami pracy wynikającymi z czynników środowiskowych.

X. Udostępnianie danych

A. Dane osobowe mogą być udostępniane tylko osobom lub podmiotom uprawnionym, na udokumentowany wniosek (może być to pismo, wiadomość email itp.).
B. Potrzebę udostępnienia Pracownik powinien skonsultować z koordynatorem ODO a w przypadku udostępnienia- zawiadomić o tym fakcie koordynatora ODO.
C. Dane osobowe są przekazywane wnioskodawcy w sposób minimalizujący ryzyko ujawnienia tych danych osobom nieuprawnionym np. w przypadku formy elektronicznej - poprzez ich szyfrowanie.
D. W przypadku przesłania zaszyfrowanej wiadomości poza CAS, hasło powinno zostać udostępnione innym kanałem komunikacji (np. SMS, komunikator internetowy).
E. Hasło wskazane w pkt D nie powinno być przesyłane w następnej wiadomości w sposób jaki został przesłany zaszyfrowany plik.
F. Koordynator ODO zapewniają prowadzenie rejestru udostępnień, w którym wskazywany jest podmiot, któremu udostępniono dane, zakres udostępnienia, sposób udostępnienia i data udostępnienia danych.
G. W rejestrze udostępnień nie odnotowuje się udostępnień:
    1. dokonanych w związku z konkretnym postępowaniem prowadzonym przez podmioty publiczne składające takie żądanie, w szczególności sądy i organy egzekucyjne,
    2. gdy system informatyczny automatycznie odnotowuje informacje, o których mowa w lit. C.
    3. gdy na podstawie udostępnienia określony pracownik innego podmiotu trzeciego czasowo lub stale zostanie dopuszczony do infrastruktury CAS.

XI. Zasady dotyczące przypadków naruszenia ochrony danych osobowych

A. Wszystkie osoby wykonujące pracę na rzecz CAS są zobowiązane do reagowania na nieprawidłowości w przetwarzaniu danych osobowych.
B. Tryb postępowania w przypadku stwierdzenia naruszenia lub podejrzenia naruszenia bezpieczeństwa danych osobowych opisują Zasady zgłaszania naruszeń ochrony danych osobowych w CAS w Instrukcji nr 3 do niniejszej PBDO.

XII. Ocena skutków dla ochrony danych

A. Jeżeli dany rodzaj przetwarzania - w szczególności z użyciem nowych technologii - ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Pracownicy odpowiedzialni merytorycznie za proces przetwarzania, przed rozpoczęciem

przetwarzania, przygotowują dla ADO ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych przy współpracy z Koordynatorem ODO.

B. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
C. Koordynator ODO udziela zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 RODO.
D. Ocena zawiera co najmniej:
   1. systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie - prawnie uzasadnionych interesów realizowanych przez Administratora;
   2. ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą;
   4. środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie RODO, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.
E. Ocena skutków dla ochrony danych podlega uzgodnieniu z Zarządem CAS lub osobą przez niego upoważnioną.

XIII. Kontrole i audyty dotyczące bezpieczeństwa danych osobowych

A. Koordynator ODO wykonuje lub zleca audyty i kontrole w zakresie ochrony danych osobowych w CAS.
B. Jeżeli w wyniku audytu lub kontroli stwierdzono przypadki naruszenia przepisów o ochronie danych osobowych lub inne istotne uchybienia, koordynator ODO przedstawia ADO informacje o stanie realizacji działań naprawczych - w terminie do 21 dni od dnia otrzymania sprawozdania lub jego odpowiedniej części. Dokumenty te tworzone są w formie dokumentowej i przesyłane mailowo lub przez system funkcjonujący w CAS.

XIV. Szkolenia

A. Wszyscy Pracownicy uczestniczący w przetwarzaniu danych osobowych podlegają szkoleniu wstępnemu oraz w miarę potrzeb szkoleniom okresowym w zakresie:
   1. obowiązujących przepisów o ochronie danych osobowych i wewnętrznych polityk, procedur oraz innych dokumentów w tym zakresie - przeprowadzanych przez koordynatora ODO lub przez osobę wskazaną przez koordynatora ODO;
   2. zasad i wewnętrznych procedur przetwarzania w systemach informatycznych oraz podstawowych zagrożeń związanych z takim przetwarzaniem.

3. zasad i wewnętrznych procedur związanych z fizycznym bezpieczeństwem przetwarzanych danych w systemach informatycznych oraz podstawowych zagrożeń związanych z takim przetwarzaniem.

B. Pracownicy oraz Koordynator ODO są zobowiązani do śledzenia zmian w zakresie obowiązujących przepisów prawnych i procedur w zakresie ochrony danych osobowych.

XV. Wydawanie upoważnień do przetwarzania danych osobowych

A. Każdy nowy przyjmowany Pracownik powinien być przeszkolony z zakresu ochrony danych osobowych, najpóźniej w ciągu 21 dni od rozpoczęcia pracy przez koordynatora ODO lub osobę przez niego wskazaną.
B. Pracownik wskazany zgodnie z lit. A, po przeprowadzeniu szkolenia, odbiera od osoby przeszkolonej oświadczenie, które stanowi załącznik nr 5 do PBDO. Oryginał tego oświadczenia osoba szkoląca przekazuje do odpowiedniego pracownika odpowiedzialnego za dokumentację pracowniczą w CAS w celu włączenia do teczek akt osobowych.
C. Z mocy przedmiotowej PBDO osobie przeszkolonej nadawane jest upoważnienie do przetwarzania danych osobowych, zgodnie ze wzorem stanowiącym załącznik nr 4 do PBDO. Oryginał upoważnienia Koordynator ODO przekazuje do odpowiedniego pracownika odpowiedzialnego za dokumentację pracowniczą w CAS w celu włączenia do teczki akt osobowych.
D. Upoważnienie do przetwarzania danych osobowych jest tożsame i adekwatne do zakresu obowiązków Pracownika.
E. Upoważnienie jest ważne do czasu realizowania czynności związanych z przetwarzaniem danych osobowych w CAS.
F. Zarząd lub pracownik wskazany przez Zarząd wydają upoważnienia do przetwarzania danych osobowych Pracownikom.

XVI. Powierzenie przetwarzania danych osobowych

A. Zlecanie czynności związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu CAS jest formą powierzenia przetwarzania danych osobowych.
B. Powierzenie przetwarzania danych osobowych odbywa się zgodnie z art. 28 RODO, na podstawie umowy zawartej na piśmie, lub w formie elektronicznej z podpisami kwalifikowanymi pomiędzy CAS a danym podmiotem, któremu zleca się czynności związane z przetwarzaniem danych osobowych.
C. Przykładowe postanowienia umowne (wzór umowy) dotyczące powierzenia przetwarzania danych osobowych zostały zamieszczone w załączniku nr 10 do niniejszej PBDO.

D. Odpowiedzialny za dany proces Pracownik jest odpowiedzialny za stosowanie odpowiednich postanowień dotyczących powierzania przetwarzania danych osobowych oraz przesłanie odpowiedniej informacji o zawarciu umowy do Koordynatora ODO.
E. Koordynator ODO odpowiedzialny jest za prowadzenie rejestru podmiotów, którym powierzono dane, zgodnie z załącznikiem nr 9 do PBDO.
F. Skan zawartej umowy powierzenia przetwarzania danych osobowych przekazywany jest do koordynatora ODO niezwłocznie, nie później niż w terminie 3 dni od dnia jej zawarcia.
G. W projekcie umowy/aneksu/paragrafu należy wskazać zakres czynności związanych z przetwarzaniem powierzonych danych osobowych, zakres danych oraz wymagania dotyczące ochrony danych.
H. W przypadku planowania powierzenia przetwarzania danych osobowych innemu podmiotowi, celem zapewnienia bezpieczeństwa przetwarzania danych osobowych przez ADO, należy przeprowadzić weryfikację podmiotu przetwarzającego. Zasady weryfikacji podmiotów przetwarzających dane osobowe zostały zamieszczone w Instrukcji nr 2 do niniejszej PBDO.
I. W przypadku, gdy zlecanie czynności związanych z przetwarzaniem danych osobowych podmiotom zewnętrznym w imieniu CAS dotyczy danych osobowych, które zostały powierzone CAS zgodnie z art. 28 RODO, należy zawrzeć umowę dalszego powierzenia po spełnieniu wymogów określonych przez podmiot, który powierzył CAS dane osobowe.
J. W przypadku gdy przekazanie danych osobowych innemu podmiotowi nie ma charakteru powierzenia, a na podstawie przekazania dany podmiot sam będzie ustalał cele i sposoby przetwarzania danych osobowych, przekazanie powinno odbywać się na podstawie umowy udostępnienia danych, która stanowi załącznik nr 11 do niniejszej PBDO.

XVII. Postanowienia końcowe

1. Koordynator ODO oraz każda osoba zaangażowana w realizację niniejszej PBDO zobowiązani są do zapoznania się z niniejszą PBDO, związanymi z nią instrukcjami i procedurami oraz do stosowania ich postanowień.
2. Postanowienia niniejszej PBDO stosuje się odpowiednio, w przypadku gdy CAS jest podmiotem przetwarzającym lub dalszym podmiotem przetwarzającym, współadministratorem lub przetwarza dane osobowe na innej podstawie prawnej.

XVIII. Historia przeglądu i zmian dokumentu

1. 19.01.2024 roku- przyjęcie dokumentu

Załączniki:

Załącznik nr 1 - Rejestr czynności przetwarzania;
Załącznik nr 2 - Rejestr kategorii czynności przetwarzania;
Załącznik nr 3 - Wzór pełnomocnictwa;
Załącznik nr 4 - Wzór upoważnienia do przetwarzania danych osobowych;
Załącznik nr 5 - Oświadczenie o zapoznaniu się;
Załącznik nr 6 - Przykładowa klauzula informacyjna, zbieranie danych osobowych bezpośrednio od osoby, której dane dotyczą.
Załącznik nr 7 - Przykładowa klauzula informacyjna, zbierania danych osobowych niebezpośrednio od osoby, której dane dotyczą;
Załącznik nr 8 - Przykładowy wzór zgody na przetwarzanie danych osobowych;
Załącznik nr 9 - Wzór rejestru podmiotów, którym powierzono do przetwarzania dane osobowe;
Załącznik nr 10 - Wzór umowy powierzania przetwarzania danych osobowych;
Załącznik nr 11- Wzór umowy udostępnienia danych osobowych;
Instrukcja nr 1 do PBDO - Instrukcja realizacji praw osób, których dane dotyczą;
Instrukcja nr 2 do PBDO - Zasady weryfikacji podmiotów przetwarzających;

Instrukcja nr 3 do PBDO - Instrukcja zgłaszania i oceny wagi naruszeń ochrony danych osobowych;
Instrukcja nr 4 do PBDO - Instrukcja sporządzania klauzul informacyjnych;
Instrukcja nr 5 - Instrukcja współpracy z organem nadzorczym;
Procedura nr 1 - Procedura ochrony danych osobowych w fazie projektowania i domyślnej ochrony danych;
Procedura nr 2 - Procedura oceny skutków dla ochrony danych osobowych;
Procedura nr 3 - Ocena roli podmiotu w procesie przetwarzania danych osobowych.