Nazwa jednostki organizacyjnej	**Centrum Kultury Promocji i Turystyki w Poniatowej**		
Dokument	**Polityka Bezpieczeństwa Danych Osobowych**		
Wersja dokumentu	**1.0**	Dokument wdrażający	**Zarządzenie Nr .../2024 Dyrektora CKPiT w Poniatowej**
Data opracowania	**19.07.2024 r.**	Data wdrożenia	**.....2024 r.**

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

CENTRUM KULTURY PROMOCJI I TURYSTYKI W PONIATOWEJ

ul. Fabryczna 1, 24-320 Poniatowa

OCHRONA DANYCH OSOBOWYCH

PCA

Niniejszy dokument jest wyłącznie dokumentem wewnętrznym stanowiącym własność Administratora Danych osobowych. Dokument stanowi tajemnicę organizacji i nie należy go publikować, lecz rozpowszechniać jedynie wśród pracowników organizacji.

Wszelkie prawa zastrzeżone. Żadna część niniejszego dokumentu, w celach innych niż na użytek własny, nie może być powielana ani rozpowszechniana za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i innych - bez pisemnej zgody autora. Naruszenie praw autorskich będzie skutkowało odpowiedzialnością karną, określoną w przepisach prawa, w szczególności w przepisach ustawy o prawie autorskim i prawach pokrewnych, ustawy o zwalczaniu nieuczciwej konkurencji, przepisach prawa prasowego oraz przepisach kodeksu cywilnego.

SPIS TREŚCI

1. 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. **dane szczególnej kategorii:** oznaczają dane osobowe ujawniające 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;
3. **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 przesyłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
4. **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);
5. **Administrator Danych Osobowych (ADO):** osoba fizyczna, firma lub instytucja, która ma prawo i obowiązek zarządzania danymi osobowymi zgodnie z obowiązującymi przepisami o ochronie danych osobowych. ADO jest odpowiedzialny za podejmowanie decyzji dotyczących celów i środków przetwarzania danych osobowych, zapewnienie zgodności z prawem oraz ochronę praw i prywatności osób, których dane są przetwarzane. Administrator Danych Osobowych ma obowiązek zaimplementować odpowiednie środki bezpieczeństwa i procedury, aby chronić dane osobowe przed nieuprawnionym dostępem, utratą, uszkodzeniem lub nieautoryzowanym ujawnieniem;
6. **podmiot przetwarzający (procesor):** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora Danych Osobowych i jest odpowiedzialny za zachowanie bezpieczeństwa danych;
7. **ocena podmiotów przetwarzających:** proces oceny i monitorowania zgodności działań podmiotów przetwarzających, takich jak dostawcy usług, którzy przetwarzają dane osobowe w imieniu administratora danych, w celu zapewnienia odpowiedniego poziomu ochrony danych
8. **Inspektor Ochrony Danych (IOD):** jest niezależną, powołaną przez ADO osobą odpowiedzialną za monitorowanie i nadzór nad przetwarzaniem danych osobowych w organizacji. Inspektor Ochrony Danych ma za zadanie zapewnić, że organizacja przestrzega przepisów dotyczących ochrony danych osobowych. Obowiązki IOD obejmują udzielanie porad i konsultacji w kwestiach ochrony danych osobowych, monitorowanie zgodności z przepisami o ochronie danych, prowadzenie szkoleń dla personelu oraz pełnienie roli punktu kontaktowego dla osób, których dane są przetwarzane. Inspektor

Ochrony Danych pełni istotną rolę w zapewnieniu zgodności organizacji z przepisami o ochronie danych osobowych i ochronie praw i prywatności osób, których dane są przetwarzane.

9. **Administrator Systemu Informatycznego (ASI):** oznacza osobę powołaną przez Administratora Danych Osobowych do zarządzania, konfiguracji, utrzymywania i nadzorowania systemem informatycznym;
10. **pracownik:** oznacza każdą osobę świadczącą pracę na rzecz Administratora Danych Osobowych na podstawie umowy o pracę oraz innych form zatrudnienia;
11. **Polityka Bezpieczeństwa Danych osobowych (PBDO):** jest to dokument zawierający zestaw praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych, wewnątrz organizacji. PBDO odnosi się całościowo do problemu zabezpieczenia danych przetwarzanych tradycyjnie – w formie papierowej, jak i danych przetwarzanych w systemie informatycznym. Celem dokumentu jest wskazanie działań jakie należy wykonać oraz ustanowienie zasad i reguł postępowania, które należy stosować aby właściwie wykonywać obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia danych osobowych;
12. **zgoda:** oznacza dobrowolne, konkretne, świadome i jednoznaczne wyrażenie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;
13. **profilowanie:** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników konkretnej osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów jej pracy, sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;
14. **pseudonimizacja:** proces zamiany danych osobowych w taki sposób, że nie można ich już przyporządkować do konkretnej osoby bez użycia dodatkowych informacji;
15. **ogólna ocena ryzyka:** to uporządkowany proces, będący częścią planowania projektów oraz zarządzania ryzykiem w projekcie, który umożliwia kierownikowi projektu identyfikować, planować i zarządzać ryzykami w celu wyeliminowania ich bądź obniżenia do akceptowalnego poziomu. W zakresie bezpieczeństwa przetwarzania informacji, w tym danych osobowych analizę ryzyka, należy przeprowadzić, biorąc pod uwagę potencjalne negatywne skutki (straty materialne i niematerialne) zarówno dla Administratora Danych Osobowych, jak i osób, których dane dotyczą;
16. **ocena skutków dla ochrony danych (ang. data protection impact assessment, DPIA)**: to proces polegający na szacowaniu wpływu planowanych działań przetwarzania danych na ochronę danych. Proces ten ma być realizowany przed przystąpieniem do przetwarzania danych (na etapie planowania) i dotyczy niektórych rodzajów przetwarzania, z którymi może wiązać się duże ryzyko. Ocenę skutków dla ochrony danych przeprowadza się wtedy, gdy istnieje wysokie ryzyko naruszenia praw i wolności osób, których dane dotyczą;
17. **naruszenie ochrony danych osobowych:** nieautoryzowany dostęp, utrata, ujawnienie lub uszkodzenie danych osobowych, które mogą prowadzić do przypadkowego lub nielegalnego zniszczenia, utraty, zmiany, nieuprawnionego ujawnienia lub dostępu do danych;
18. **prawa osób, których dane dotyczą:** uprawnienia przysługujące osobom fizycznym, których dane osobowe są przetwarzane, zgodnie z przepisami o ochronie dany osobowych;

19. **zabezpieczenie danych osobowych:** środki techniczne i organizacyjne stosowane w celu ochrony danych osobowych przed przypadkowym lub nieautoryzowanym dostępem, utratą, zmianą, uszkodzeniem lub ujawnieniem;
20. **audyt bezpieczeństwa danych**: niezależna ocena i weryfikacja zgodności działań organizacji z Polityką Bezpieczeństwa Danych Osobowych oraz z przepisami dotyczącymi ochrony danych;
21. **retencja danych:** okres przechowywania danych osobowych;
22. **monitorowanie zgodności**: proces regularnego sprawdzania, czy organizacja przestrzega przepisów dotyczących ochrony danych osobowych oraz wewnętrznych zasad i procedur określonych w Polityce Bezpieczeństwa Danych Osobowych.

2. STRATEGIA I CELE BIZNESOWE ORGANIZACJI

Centrum Kultury Promocji i Turystyki w Poniatowej jest Samorządową Instytucją Kultury dla której organizatorem jest Gmina Poniatowa. Celem CKPiT w Poniatowej jest wielokierunkowa działalność kulturowa, aktywizowanie społeczności lokalnej, kształtowanie kultury wypoczynku i życia codziennego, promowanie lokalnego dziedzictwa kulturowego, a także rozbudowa potencjału turystycznego i rekreacyjnego Gminy Poniatowa. Stwarzanie warunków do prowadzenia różnych form edukacji, budowanie nawyków do korzystania i promowania dóbr kultury lokalnej oraz zasobów przyrodniczych Gminy wraz ze współdziałaniem z instytucjami upowszechniania min. kultury, turystyki, ochrony środowiska lokalnego.

Działalność jednostki w sposób nierozerwalny związana jest z przetwarzaniem na dużą skalę danych osobowych kategorii zwykłej w szczególności mieszkańców Gminy Poniatowa, a także uczestników organizowanych np. konkursów, targów, imprez masowych. ADO jako podmiot realizujący zadania publiczne opracowuje i ustanawia, wdraża i eksploatuje, monitoruje i przegląda oraz utrzymuje i doskonali system ochrony osobowych, zapewniający poufność, dostępność i integralność informacji z uwzględnieniem atrybutów dodatkowych jak: autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

ADO, jako podmiot publiczny, wyznaczył Inspektora Ochrony Danych, który wspiera go we wszystkich kwestiach związanych z ochroną danych osobowych.

3. PODSTAWA PRAWNA

Akty prawne:

1. 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 Osobowych – RODO).
2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych, Dz.U. 2018 poz. 1000.
3. Ustawa z dnia 17 lutego 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne, Dz. U. 2014 poz. 1114.
4. Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych Dz.U. z 2017 r., poz. 2247.

Podstawowe przepisy szczegółowe, w oparciu, o które działa organizacja:

1. Ustawa z dnia 26 czerwca 1974 r. - Kodeks pracy
2. Ustawa z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej

Inne dokumenty:

1. Norma PN-EN ISO 19011:2012.
2. Norma PN-EN ISO/IEC 27001:2022
3. Norma PN-EN ISO/IEC 27002.
4. Komunikat Prezesa Urzędu Ochrony Danych Osobowych z dnia 17 sierpnia 2018 r. w sprawie wykazu rodzajów operacji przetwarzania danych osobowych wymagających oceny skutków przetwarzania dla ich ochrony M.P. 2018 poz. 827.
5. Wytyczne EROD oraz Grupy Roboczej Art. 29.
6. Bieżące wskazówki UODO oraz Ministerstwa Cyfryzacji.
7. Kodeks branżowy „dobre praktyki".

4. DEKLARACJA STOSOWANIA KIEROWNICTWA

Zmieniająca się rzeczywistość prawna związana z obowiązywaniem RODO wymusiła na Administratorze Danych Osobowych inwentaryzację zasobów danych osobowych i procesów ich przetwarzania. Z uwagi na pojawienie się nowych regulacji ADO deklaruje, że wdroży niezbędne procedury oparte na zasadach i podstawach przetwarzania zawartych w obowiązujących przepisach dotyczących ochrony danych osobowych.

Administrator Danych Osobowych świadomy wagi problemów i zagrożeń związanych z ochroną danych osobowych, wprowadza Politykę Bezpieczeństwa Danych Osobowych zwaną dalej PBDO. Opracowanie niniejszego dokumentu wynika ze zrozumienia znaczenia bezpieczeństwa danych we współczesnym świecie.

Deklaracja Stosowania Kierownictwa dla Polityki Bezpieczeństwa Danych Osobowych:

Jako kierownictwo Centrum Kultury Promocji i Turystyki w Poniatowej zobowiązujemy się do pełnego przestrzegania i wdrażania Polityki Bezpieczeństwa Danych Osobowych w celu ochrony poufności, integralności i dostępności danych osobowych, które przetwarzamy w naszej organizacji. Nasze zobowiązanie obejmuje:

1. **Przestrzeganie przepisów i standardów**: Zapewniamy, że będziemy przestrzegać wszelkich obowiązujących przepisów dotyczących ochrony danych osobowych, takich jak Ogólne Rozporządzenie o Ochronie Danych (RODO) oraz przepisów Ustawy o ochronie danych osobowych. Będziemy również dążyć do spełniania międzynarodowych standardów i najlepszych praktyk dotyczących bezpieczeństwa danych.
2. **Odpowiedzialność i nadzór**: Wyznaczamy odpowiedzialne osoby do nadzoru i zarządzania bezpieczeństwem danych osobowych w naszej organizacji. Będziemy zapewniać odpowiednie zasoby, szkolenia i wsparcie, aby umożliwić tym osobom efektywne wykonywanie swoich obowiązków.

3. **Bezpieczeństwo danych:** Będziemy stosować odpowiednie techniczne i organizacyjne środki bezpieczeństwa, aby chronić dane osobowe przed nieuprawnionym dostępem, utratą, zmianą lub zniszczeniem.
4. **Świadomość i szkolenia**: Zapewnimy regularne szkolenia i podnoszenie poziomu świadomości dla naszych pracowników w zakresie ochrony danych osobowych. Będziemy promować kulturę dbałości o poufność i bezpieczeństwo danych osobowych we wszystkich obszarach naszej organizacji.
5. **Zarządzanie ryzykiem**: Będziemy systematycznie identyfikować, oceniać i zarządzać ryzykiem związanym z przetwarzaniem danych osobowych, tak aby stale aktualizować stosowane przez nas środki techniczne i organizacyjne ochrony danych adekwatnie do zidentyfikowanych zagrożeń oraz zmieniającej się rzeczywistości.
6. **Monitorowanie i audyty**: Będziemy regularnie monitorować i oceniać skuteczność naszych środków bezpieczeństwa danych osobowych. Przeprowadzamy audyty wewnętrzne i zewnętrzne, aby zapewnić zgodność z naszą Polityką Bezpieczeństwa Danych Osobowych i identyfikować obszary wymagające ulepszeń.
7. **Ciągłe doskonalenie**: Dążymy do ciągłego doskonalenia naszych działań w zakresie ochrony danych osobowych i przestrzegania obowiązujących przepisów o ochronie danych.

4.1. Cel wprowadzenia Polityki Bezpieczeństwa Danych Osobowych

Celem wdrożenia niniejszej Polityki Bezpieczeństwa Danych Osobowych jest ochrona interesów osób, których dane dotyczą poprzez zapewnienie należytej, adekwatnej do przewidywanych zagrożeń oraz kategorii przetwarzanych danych, ochrony posiadanych zasobów informacyjnych. Bezpieczeństwo danych oznacza zapewnienie ich **poufności, integralności, dostępności** i **rozliczalności**.

Cele realizowane są poprzez:

1. określenie zasad i reguł postępowania, które należy stosować, aby właściwie wykonywać obowiązki Administratora Danych Osobowych w zakresie zabezpieczenia danych osobowych;
2. budowanie świadomości o konieczności ochrony i zabezpieczania wszystkich danych osobowych wśród osób przetwarzających dane;
3. określenie zestawu praw, procedur i praktycznych doświadczeń regulujących sposób zarządzania, zabezpieczania i dystrybucji danych osobowych przetwarzanych tradycyjnie w formie papierowej, jak i danych przetwarzanych w systemach informatycznych, wewnątrz jak i na zewnątrz organizacji.

4.2. Zakres przedmiotowy

Zakres przedmiotowy obejmuje wszystkie dane przetwarzane przez Administratora Danych Osobowych w związku z prowadzoną działalnością, zarówno w formie elektronicznej, jak i papierowej.

1. **Dane osobowe:** PBDO dotyczy wszelkich danych osobowych przetwarzanych przez Centrum Kultury Promocji i Turystyki w Poniatowej, w szczególności są to informacje identyfikujące osoby fizyczne, takie jak imię, nazwisko, adres, numer telefonu, adres e-mail, PESEL, numer identyfikacyjny itp.
2. **Procesy przetwarzania danych osobowych:** PBDO dotyczy wszelkich procesów przetwarzania danych osobowych, takich jak gromadzenie, przechowywanie, przekazywanie, udostępnianie, analizowanie, archiwizowanie, niszczenie itp., zarówno w formie elektronicznej, jak i papierowej.

3. **Systemy informatyczne:** PBDO dotyczy wszelkich systemów informatycznych, infrastruktury sieciowej, oprogramowania, serwerów, urządzeń przechowujących dane, systemów zarządzania bazami danych i innych technologii wykorzystywanych do przetwarzania danych osobowych.
4. **Bezpieczeństwo fizyczne:** PBDO dotyczy również środków bezpieczeństwa fizycznego, takich jak kontrole dostępu, monitorowanie systemów, zabezpieczenia pomieszczeń, oznaczenia obszarów ograniczonego dostępu, aby zapewnić ochronę danych osobowych przed nieuprawnionym dostępem, kradzieżą, uszkodzeniem lub zniszczeniem.
5. **Współpraca z podmiotami zewnętrznymi:** PBDO obejmuje zasady bezpiecznego przekazywania danych osobowych do podmiotów zewnętrznych, takich jak partnerzy biznesowi, dostawcy usług, kontrahenci itp. Wymaga się, aby takie podmioty przestrzegały odpowiednich zabezpieczeń danych.

4.3. Zakres podmiotowy

Zakres podmiotowy PBDO odnosi się do:

1. **Administratora Danych Osobowych i pracowników:** PBDO obejmuje dyrekcję Centrum Kultury Promocji i Turystyki w Poniatowej, pracowników, współpracowników, stażystów i praktykantów jednostki.
2. **Uczestników zajęć lub wydarzeń kulturalnych, rodziców lub opiekunów prawnych:** PBDO obejmuje dane osobowe uczestników zajęć lub wydarzeń kulturalnych, ich rodziców lub opiekunów prawnych. Zobowiązuje do zapewnienia poufności, integralności i dostępności tych danych oraz odpowiedniego przetwarzania w zgodzie z obowiązującymi przepisami o ochronie danych osobowych.
3. **Kontrahentów i podwykonawców:** PBDO rozszerza się na wszelkie osoby trzecie, takie jak kontrahenci, podwykonawcy, najemcy, dostawcy usług IT, którzy przetwarzają dane osobowe w imieniu Centrum Kultury Promocji i Turystyki w Poniatowej. Wymaga się od tych podmiotów przestrzegania odpowiednich zabezpieczeń i zasad ochrony danych.
4. **Innych stron trzecich:** PBDO obejmuje również inne strony trzecie, takie jak audytorzy, organy ścigania, regulacyjne oraz kontrolne itp., które mogą mieć dostęp do danych osobowych w określonych przypadkach, zgodnie z obowiązującymi przepisami.

5. Role i odpowiedzialność

1. Odpowiedzialny za **wdrożenie i utrzymanie** niniejszej Polityki Bezpieczeństwa Danych Osobowych jest Administrator Danych Osobowych.
2. Za **nadzór i monitorowanie** przestrzegania PBDO odpowiadają:
   a. Administrator Danych Osobowych,
   b. Inspektor Ochrony Danych,
   c. Administrator Systemów Informatycznych,
3. Za **stosowanie** niniejszej Polityki Bezpieczeństwa Danych Osobowych odpowiedzialni są:
   a. Administrator Danych Osobowych,
   b. wszyscy pracownicy,
   c. jednostki i podmioty współpracujące z Administratorem Danych Osobowych na podstawie zawartych umów, porozumień, które zobowiązały się do przestrzegania regulacji wewnętrznych Administratora Danych Osobowych w zakresie ochrony danych.

5.1. Administrator Danych Osobowych

Administrator Danych Osobowych jest podstawowym adresatem RODO. Odpowiada za całość przetwarzania danych, także w części powierzonej podmiotowi przetwarzającemu. Uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, zapewnia:

1. sprawowanie nadzoru nad bezpieczeństwem oraz przetwarzaniem danych osobowych;
2. właściwe środki techniczne i organizacyjne mające na celu zagwarantowanie bezpieczeństwa danych przetwarzanych w organizacji;
3. należytą i terminową obsługę i realizację praw osób, których dane dotyczą;
4. uwzględnienie ochrony danych w fazie projektowania oraz domyślną ochronę danych (minimalizacja przetwarzania);
5. dopuszczenie do przetwarzania danych wyłącznie osób, którym zostało udzielone upoważnienie do przetwarzania danych;
6. w przypadku powierzenia przetwarzania danych zawarcie umowy powierzenia przetwarzania danych i korzystanie tylko z wiarygodnych przetwarzających;
7. zarządzanie, obsługę i zgłaszanie naruszeń ochrony danych Prezesowi Urzędu Ochrony Danych Osobowych oraz informowanie o naruszeniu osób, których dane dotyczą;
8. przeprowadzenie oceny skutków dla ochrony danych;
9. prowadzenie rejestru czynności przetwarzania danych i rejestru kategorii przetwarzania danych;
10. wyznaczenie Inspektora Ochrony Danych oraz powiadomienie o tym fakcie Prezesa Urzędu Ochrony Danych Osobowych.

5.2. Inspektor Ochrony Danych

Wyznaczony w organizacji Inspektor Ochrony Danych wspiera Administratora Danych Osobowych w realizacji obowiązków dotyczących ochrony danych osobowych. Pełni w organizacji rolę konsultanta i doradcy.

Do zadań Inspektora Ochrony Danych należy:

1. informowanie Administratora Danych Osobowych, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;
2. monitorowanie przestrzegania przepisów prawa o ochronie danych oraz PBDO i procedur przyjętych przez Administratora Danych Osobowych w dziedzinie ochrony danych osobowych;
3. podejmowanie działań zwiększających świadomość oraz szkolenie personelu uczestniczącego w operacjach przetwarzania;
4. prowadzenie audytów mających na celu ocenę skuteczności wdrożonych środków technicznych i organizacyjnych, w tym przegląd obowiązującej dokumentacji z zakresu ochrony danych osobowych;
5. udzielanie na żądanie ADO zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

6. współpraca z Prezesem Urzędu Ochrony Danych Osobowych;
7. pełnienie funkcji punktu kontaktowego dla Prezesa Urzędu Ochrony Danych Osobowych w kwestiach związanych z przetwarzaniem, w tym w zakresie naruszeń oraz uprzednich konsultacji;
8. pełnienie roli punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem przysługujących im praw.

5.3. Administrator Systemów Informatycznych

Administrator Systemów Informatycznych odpowiada za zapewnienie przestrzegania zasad ochrony danych osobowych przetwarzanych w systemach informatycznych.

Do zadań Administratora Systemów Informatycznych należy:

1. współpraca przy przygotowaniu, wdrażaniu oraz respektowaniu przez pracowników dokumentacji z zakresu ochrony danych osobowych, w szczególności dokumentacji związanej z zarządzaniem systemami teleinformatycznymi;
2. zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe oraz przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego;
3. prowadzenie szkoleń z zakresu bezpieczeństwa informacji przetwarzanych w systemach informatycznych, cyberbezpieczeństwa;
4. współpraca przy przeprowadzaniu okresowych sprawdzeń przestrzegania RODO;
5. współpraca podczas przeprowadzania procesu analizy ryzyka;
6. zapewnienie ciągłości działania systemu, w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych;
7. wykonywanie, przechowywanie i testowanie kopii zapasowych zgodnie z przyjętymi procedurami;
8. zapewnienie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej systemów informatycznych służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich integralności;
9. nadzór nad naprawą, konserwacją oraz niszczeniem elektronicznych nośników danych;
10. kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych;
11. zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego;
12. zapewnienie poufności, integralności, dostępności i rozliczalności danych przetwarzanych w systemach informatycznych;
13. dostosowanie systemów informatycznych służących do przetwarzania danych osobowych do wymogów RODO oraz innych obowiązujących przepisów;
14. zabezpieczenie pomieszczeń, w których przetwarzane są dane osobowe, w szczególności szachtów sieciowych lub pomieszczenia, w którym znajduje się serwer przed dostępem osób nieuprawnionych lub innymi zdarzeniami losowymi;
15. ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie organizacyjnych, fizycznych i technicznych zabezpieczeń chroniących przed nieuprawnionym dostępem;

16. nadawanie uprawnień do przetwarzania danych zgodnie z udzielonymi upoważnieniami;
17. nadzór i prowadzenie ewidencji sprzętu teleinformatycznego oraz oprogramowania (inwentaryzacja);
18. nadzór i przeprowadzanie wewnętrznych audytów teleinformatycznych i audytów cyberbezpieczeństwa zgodnie z przyjętymi regulacjami wewnętrznymi;
19. zgłaszanie do Administratora Danych Osobowych potrzeb dotyczących zwiększenia bezpieczeństwa przetwarzania informacji w systemach informatycznych.

5.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH

Każdy pracownik odpowiedzialny jest za bezpieczeństwo informacji w zakresie przetwarzania danych osobowych, stosownie do zajmowanego stanowiska i udzielonego upoważnienia.

Do obowiązków każdej osoby upoważnionej do przetwarzania danych należy:

1. zapoznanie się z przepisami prawa w zakresie ochrony danych oraz postanowieniami wdrożonej w organizacji dokumentacji z tego zakresu, w tym w szczególności z Polityką Bezpieczeństwa Danych Osobowych;
2. stosowanie się do wszelkich ustanowionych w organizacji procedur z zakresu ochrony danych osobowych;
3. stosowanie się do zaleceń w zakresie ochrony danych osobowych wydawanych przez Administratora Danych Osobowych, Inspektora Ochrony Danych, Administratora Systemów Informatycznych.
4. informowanie bez zbędnej zwłoki Administratora Danych Osobowych, Inspektora Ochrony Danych, Administratora Systemów Informatycznych o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w organizacji;
5. zgłaszanie bez zbędnej zwłoki Administratorowi Danych Osobowych, Inspektorowi Ochrony Danych, Administratorowi Systemów Informatycznych sytuacji (incydentów) naruszenia ochrony danych osobowych;
6. przetwarzanie danych osobowych wyłącznie w zakresie określonym w udzielonym upoważnieniu do przetwarzania danych osobowych oraz w celu wykonywania obowiązków służbowych;
7. zachowanie w poufności danych osobowych w sytuacji dostępu do nich podczas wykonywania zadań;
8. zabezpieczania danych przed dostępem osób nieupoważnionych, zabraniem, uszkodzeniem oraz nieuzasadnioną modyfikacją lub zniszczeniem.

6. ZASADY PRZETWARZANIA DANYCH

Nadzór:	ADO, ASI, IOD
Stosowanie:	wszyscy pracownicy

Przetwarzanie danych osobowych obejmuje wszystkie działania związane z posługiwaniem się danymi osobowymi od rozpoczęcia cyklu przetwarzania, a więc pierwszego kontaktu z danymi, aż do momentu ich usunięcia.

Zasady przetwarzania danych osobowych:

1. **„zgodność z prawem i przejrzystość"**
   a. Dane osobowe należy przetwarzać zgodnie z prawem, w sposób zrozumiały i nie budzący wątpliwości osoby, której dane dotyczą,
   b. Przed zebraniem danych osobowych należy umożliwić osobie zapoznanie się z informacją dotyczącą operacji przetwarzania, celami, a także przysługującymi w związku z tym przetwarzaniem prawami.

Administrator Danych Osobowych realizuje zasadę zgodności z prawem i przejrzystości między innymi poprzez:

- warstwową realizację obowiązku informacyjnego wobec osób, których dane dotyczą (warstwowość ma na celu uproszczenie komunikacji i umożliwienie osobie fizycznej zapoznanie się z czytelnym komunikatem);
- niezwłoczne udzielanie odpowiedzi na wniosek o realizację prawa osoby fizycznej (np. w kwestii dostępu do danych i uzyskania ich kopii);
- prowadzenie aktualnego Rejestru czynności przetwarzania danych (RCPD), w którym zinwentaryzowane zostały wszystkie procesy przetwarzania danych osobowych wraz ze wskazaniem celu i podstawy prawnej przetwarzania danych wynikającej z RODO (wskazanie przesłanki z art. 6 ust. 1 lub art. 9 ust.2 RODO) oraz szczegółowego przepisu prawa.

2. **„rzetelność i prawidłowość"**
   c. Należy zawsze informować osoby, których dane dotyczą, o sytuacji faktycznej i nie stosować rozwiązań asekuracyjnych.
   d. Należy pilnować, aby dane osobowe były prawidłowe i w razie konieczności uaktualniane.
   e. Należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane.

Administrator Danych Osobowych realizuje zasadę rzetelności i prawidłowości między innymi poprzez:

- przeprowadzanie okresowych przeglądów przyjętych wniosków i formularzy, pod kątem poprawności przetwarzanych danych;
- ocenianie wiarygodności źródła pozyskiwanych danych (dotyczy sytuacji zbierania danych w sposób inny niż od podmiotu danych);
- przetwarzanie danych na podstawie wyłącznie wyraźnej i jednoznacznej, a nie domniemanej, czy wymuszonej zgody;
- prowadzenie ewidencji uzyskanych zgód od osób fizycznych, których dane dotyczą w przypadku gromadzenia danych na podstawie zgody;
- przeprowadzanie okresowych przeglądów przyjętych wniosków i formularzy, pod kątem poprawności przetwarzanych danych.

3. **„ograniczenie celu"**
   f. Należy czuwać aby dane osobowe były zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarzane dalej w sposób niezgodny z tymi celami.

g. Jeżeli pozyskane dane osobowe mają być wykorzystane w innym celu niż cel, w którym zostały zebrane, przed takim dalszym przetwarzaniem należy poinformować o tym zamiarze osoby, których dane dotyczą oraz udzielić im wszelkich innych stosownych informacji tj. o przysługujących prawach, nowym celu przetwarzania, podstawie przetwarzania.

Administrator Danych Osobowych realizuje zasadę ograniczenia celu między innymi poprzez:

- stosowanie nowatorskiej, czytelnej i przejrzystej formy informowania o celach, dla których pozyskiwane są dane osobowe od osób fizycznych, adekwatnej do formy pozyskania danych (skrócona informacja na stosowanych wnioskach i formularzach),
- systematyczne aktualizowanie Rejestru czynności przetwarzania danych (RCPD).

4. **„minimalizacja danych"**

h. Dane osobowe gromadzone w organizacji muszą być adekwatne, stosowne oraz ograniczone do tego, co niezbędne do realizacji celów, w których są przetwarzane (minimalizacja danych).

i. Zakazuje się gromadzenia danych zbędnych dla osiągnięcia określonego celu przetwarzania danych tj. nadmiarowych, oraz danych zbieranych „na wszelki wypadek".

Administrator Danych Osobowych realizuje zasadę minimalizacji danych między innymi poprzez:

- przeprowadzanie okresowych przeglądów stosowanych wniosków i formularzy, a także systemów pod kątem zakresu zbieranych danych w odniesieniu do celu i podstawy ich przetwarzania (stosowanie zasady privacy by default);
- dokonywanie analizy, jakie dane są niezbędne do osiągnięcia założonych celów, na etapie projektowania każdego nowego systemu lub planowania nowego procesu (stosowanie zasady privacy by design).

5. **„ograniczenie przechowywania"**

j. Administrator Danych Osobowych odpowiada za wprowadzenie procedur wyznaczających terminy przechowania danych (okresy retencji) lub procedur określających terminy okresowych przeglądów danych.

Administrator Danych Osobowych realizuje zasadę ograniczenia przechowywania danych między innymi poprzez:

- wdrożenie wewnętrznych procedur ustalających okres retencji danych przetwarzanych w formie tradycyjnej (papierowo, elektronicznie) oraz w systemach informatycznych (np. wdrożenie procedury retencji danych publikowanych na BIP);
- zautomatyzowanie procesu usuwania danych wraz z upływem okresu ich retencji;
- przeprowadzanie cyklicznych przeglądów pod kątem okresu retencji przetwarzanych danych.

6. **„integralność i poufność"**

k. Należy przetwarzać dane w sposób zapewniający odpowiednie bezpieczeństwo w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem.

Administrator Danych Osobowych realizuje zasadę zapewnienia integralności i poufności danych między innymi poprzez:

- opracowanie ustanowienie i wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji oraz stałe zarządzanie bezpieczeństwem informacji (w tym danych osobowych) zgodnie z Polityka Bezpieczeństwa Informacji i załącznikami do niej;
- stosowanie zabezpieczeń fizycznych takich jak zamykanie na klucz pomieszczeń z dokumentami zawierającymi dane osobowe;
- wprowadzenie procedur nadawania upoważnień oraz dostępu do systemów informatycznych w organizacji;
- wprowadzenie polityki haseł zgodnej z najnowszymi zaleceniami i trendami.

7. **„rozliczalność"**

I. Administrator Danych Osobowych odpowiedzialny jest za wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie danych osobowych odbywało się z zgodzie z przepisami prawa z zastrzeżeniem, że musi mieć on możliwość wykazania tego.

Administrator Danych Osobowych realizuje zasadę rozliczalności między innymi poprzez:

- wdrożenie polityk, procedur i instrukcji w sposób jasny i jednoznaczny określających strategię oraz zasady ochrony informacji (w tym danych osobowych);
- stosowanie upoważnień do przetwarzania danych osobowych oraz uprawnień do systemu;
- zapewnienie rozliczalności działania każdej osoby upoważnionej do przetwarzania danych, w szczególności w systemach informatycznych (m.in. dany login do systemu IT może być przypisany tylko jednej osobie);
- prowadzenie i aktualizację Rejestru czynności przetwarzania danych (RCPD);
- weryfikowanie potencjalnych podmiotów przetwarzających przed nawiązaniem z nimi współpracy oraz zawarciem umów powierzenia, a także prowadzenie i aktualizację rejestru umów powierzenia;
- analizowanie na bieżąco ryzyka naruszenia danych osobowych;
- przeprowadzanie systematycznych przeglądów oraz udokumentowanych audytów skuteczności funkcjonowania systemu ochrony danych osobowych w organizacji.

7. PRZETWARZANIE DANYCH OSOBOWYCH WEWNĄTRZ ORGANIZACJI

Organizacja realizując niniejszą Politykę Bezpieczeństwa Danych Osobowych w zakresie udostępniania danych osobowych w ramach własnej (wewnętrznej) struktury, zezwala na ich przetwarzanie w systemie informatycznym lub w wersji papierowej wyłącznie pracownikom (w niektórych przypadkach praktykantom, stażystom). Zezwolenie na przetwarzanie danych osobowych realizowane jest poprzez nadanie stosownego upoważnienia.

Celem niniejszej procedury jest określenie zasad nadawania i odbierania upoważnień do przetwarzania danych wewnątrz organizacji.

7.1. PROCEDURA NADAWANIA UPOWAŻNIENIA DO PRZETWARZANIA DANYCH

1. Upoważnienia do przetwarzania danych osobowych nadaje Administrator Danych Osobowych. Upoważnienie wydawane jest każdemu pracownikowi osobno, w zakresie adekwatnym do pełnionych obowiązków służbowych.
2. Dokument zawiera informacje doprecyzowujące, czego dotyczy upoważnienie:
   a. kategorie danych osobowych, do których upoważniona osoba może mieć dostęp,
   b. kategorie osób, których dane może przetwarzać upoważniona osoba,
   c. procesy związane z przetwarzaniem danych, które może realizować upoważniona osoba,
   d. formę przetwarzania danych – wersja papierowa dokumentów, wersja elektroniczna dokumentów,
   e. system informatyczny, do którego upoważniona osoba może mieć dostęp,
   f. wykaz pomieszczeń szczególnej ochrony, do których osoba upoważniona może mieć dostęp.
3. Upoważnienia wydawane są na czas określony lub nieokreślony.
   a. Upoważnienia wydane na czas określony ustają po terminie, na jaki zostały wydane lub z chwilą ustania stosunku prawnego z tytułu zatrudnienia, wykonywania pracy, stażu lub z chwilą odebrania upoważnienia.
   b. Upoważnienia na czas nieokreślony ustają z chwilą ustania stosunku prawnego z tytułu zatrudnienia, wykonywania pracy, stażu lub z chwilą odebrania upoważnienia.
4. Fakt nadawania upoważnienia jest odnotowywany w Rejestrze upoważnień, którego wzór stanowi załącznik do niniejszej PBDO.
5. Administrator Danych Osobowych informuje o nadaniu upoważnia do przetwarzania danych pracownikowi osobę nadzorującą system informatyczny, która nadaje dostęp do systemu informatycznego. Procedura nadawania dostępu do systemów informatycznych znajduje się w „Instrukcji Zarządzania Systemami Informatycznymi".
6. Nadane przez Administratora Danych Osobowych upoważnienia mogą być modyfikowane w trakcie ich obowiązywania. Modyfikacja może nastąpić wskutek zmiany zakresu wykonywanych prac przez osobę upoważnioną.
7. Ewidencja osób upoważnionych do przetwarzania danych podlega przeglądowi każdorazowo z przeglądem organizacyjnych i technicznych środków bezpieczeństwa, czyli nie rzadziej niż raz w roku.
8. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik do PBDO.

7.2. PROCEDURA ODBIERANIA UPOWAŻNIEŃ DO PRZETWARZANIA DANYCH

Administrator Danych Osobowych w określonych sytuacjach, może odebrać pracownikowi udzielone upoważnienie do przetwarzania danych. Sytuacja taka ma miejsce, gdy:

1. pracownik posługuje się danymi w sposób niewłaściwy, przetwarza je w zakresie wykraczającym poza nadane upoważnienie;
2. pracownik w sposób rażący naruszy zasady obowiązujących w organizacji polityk bezpieczeństwa;
3. dojdzie do rozwiązania stosunku pracy bądź innego stosunku prawnego łączącego osobę upoważnioną z Administratorem Danych Osobowych;
4. nastąpi zmiana stanowiska pracy, na stanowisko uzasadniające konieczność posiadania upoważnienia w innym zakresie.

W sytuacji odebrania upoważnienia do przetwarzania danych stosuje się niniejsze zasady:

1. Administrator Danych Osobowych lub osoba przez niego wyznaczona informuje pracownika o przebiegu przekazywania obowiązków i rozliczeniu się tej osoby z pobranego sprzętu, materiałów i dokumentów należących do pracodawcy według przyjętych procedur.
2. Administrator Danych Osobowych lub osoba wyznaczona informuje osobę nadzorującą system informatyczny o konieczności zablokowania dostępu pracownika do poczty elektronicznej oraz systemów informatycznych.
3. Blokowanie dostępu do poczty elektronicznej oraz systemów informatycznych odbywa się na zasadach określonych w „Instrukcji Zarządzania Systemami Informatycznymi"
4. Pracownikowi odbiera się możliwość dostępu do budynków i pomieszczeń należących do organizacji (klucze, karty dostępu).
5. W przypadku zmiany stanowiska pracy powyższe reguły stosuje się odpowiednio.
6. Fakt odebrania upoważnienia odnotowuje się w rejestrze upoważnień wraz ze wskazaniem daty.

7.3. POUFNOŚĆ DANYCH OSOBOWYCH

1. Od każdego pracownika, zarówno posiadającego upoważnienie do przetwarzania danych osobowych, jak i tego, który co do zasady nie posiada dostępu do danych, odbiera się oświadczenia o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych Administratora Danych Osobowych.
2. Każdego pracownika zobowiązuje się do zachowania w poufności wszelkich danych osobowych uzyskanych w ramach wykonywanych obowiązków lub też w sytuacji przypadkowego uzyskania do nich dostępu.
3. Pracowników informuje się, że postępowanie sprzeczne zasadami ochrony danych wdrożonymi w organizacji może być uznane za ciężkie naruszenie obowiązków pracowniczych w rozumieniu art. 52 § 1 pkt 1 kodeksu pracy, a także za naruszenie przepisów karnych, RODO oraz ustawy o ochronie danych osobowych.
4. Wzór oświadczenia o zachowaniu poufności stanowi załączniki do PBDO.

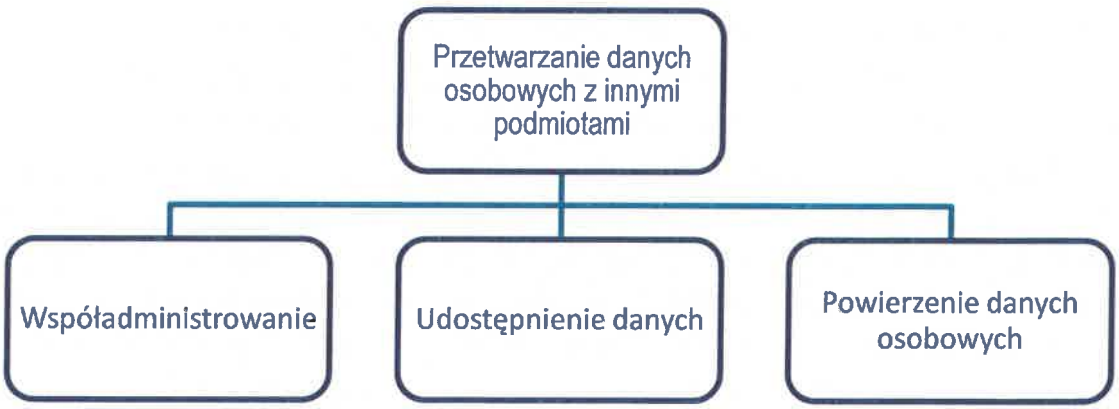
8. PRZETWARZANIE DANYCH OSOBOWYCH NA ZEWNĄTRZ ORGANIZACJI

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

1. W procesie przetwarzania danych może brać udział więcej niż jeden podmiot.
2. W sytuacji, gdy w procesie przetwarzania danych ma brać udział więcej niż jeden podmiot, Administrator Danych Osobowych dokonuje skrupulatnej analizy mającej na celu prawidłowe zidentyfikowanie relacji pomiędzy podmiotami zaangażowanymi w dany proces.
3. W ramach analizy Administrator Danych Osobowych:
   a. identyfikuje i opisuje proces, który ma zostać poddany analizie;
   b. wymienia podmioty zaangażowane w dany proces przetwarzania;

c. opisuje wpływ poszczególnych podmiotów na proces przetwarzania:
   - jakie podstawy przetwarzania danych mają poszczególne podmioty (wskazanie przepisu prawa lub rzeczywistych kompetencji);
   - kto ustala cele przetwarzania;
   - kto ustala zasady przetwarzania.

4. W oparciu o wynik analizy, ADO identyfikuje relację pomiędzy podmiotami w danym procesie przetwarzania danych na zewnątrz organizacji:
   a. **współadministrowania danymi** - co najmniej dwóch administratorów wpływa na proces przetwarzania danych; każdy z podmiotów w jakimś fragmencie podejmuje decyzje dotyczące celów i sposobów przetwarzania danych, a suma tych cząstkowych decyzji składa się na całość decyzji podejmowanych w ramach danej czynności, czy procesu, przy czym wpływ podmiotów na przetwarzanie nie musi być taki sam (równy), jak również, nie ma wymogu dostępu do danych osobowych przez wszystkich współadministratorów.
   b. **udostępnienia danych** - adresat danych ma własny cel i podstawę przetwarzania danych osobowych, a więc staje się odrębnym Administratorem Danych Osobowych.
   c. **powierzenia przetwarzania danych** - umocowanie przez Administratora Danych Osobowych innego podmiotu do przetwarzania danych w jego imieniu. W relacji powierzenia mamy zatem do czynienia z ADO, który zleca procesorowi przetwarzanie danych osobowych w jego imieniu, na jego rzecz, we wskazanych przez niego celach i na określonych zasadach.



5. Po zidentyfikowaniu relacji pomiędzy podmiotami, ADO podejmuje działania zgodne z właściwą procedurą uwzględnioną w niniejszej PBDO.

9. WSPÓŁADMINISTROWANIE DANYMI OSOBOWYMI

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

Czynnikiem decydującym o współadministrowaniu w podmiocie publicznym jest czynnik prawa.

W sytuacji, gdy przepis prawa nie wskazuje bezpośrednio relacji pomiędzy podmiotami zaangażowanymi w proces, ale przewiduje wspólne realizowanie zadań lub celów, identyfikacji tej relacji dokonuje się poprzez analizę kompetencji podmiotów.

9.1. PROCEDURA NAWIĄZYWANIA RELACJI WSPÓŁADMINISTROWANIA DANYMI

1. W przypadku gdy w wyniku wstępnej analizy dotyczącej relacji pomiędzy podmiotami ADO ustala, że zajdzie relacja współadministrowania danymi, dokonuje on oceny, czy zakres obowiązków współadministratorów jest regulowany przepisami szczególnymi (krajowymi lub unijnymi).
2. Jeśli przepisy szczególne regulują zagadnienia dotyczące współadministrowania, to współadministratorzy podejmują działania mające na celu spełnienie obowiązku realizacji wymogów określonych tymi przepisami.
3. Administratorzy Danych Osobowych **w drodze konkretnych i precyzyjnych ustaleń** gwarantujących spełnienie zasady przejrzystości i rozliczalności, ustalają **zakresy swoich obowiązków i odpowiedzialności**, w tym obligatoryjnie określają minimum:
   a. który z współadministratorów będzie realizował obowiązki informacyjne;
   b. który ze współadministratorów będzie realizował prawa osób, których dane dotyczą;
   c. kto będzie pełnił rolę punktu kontaktowego dla osób, których dane dotyczą.
4. W związku z faktem, że obowiązujące przepisy prawa nie precyzują w jakiej formie powyższe uzgodnienia powinny zostać zawarte, ADO w porozumieniu z drugim współadministratorem w każdym przypadku podejmuje decyzję, co do formy tych ustaleń, przy czym formą preferowaną jest forma pisemna - uzgodnienia w postaci umowy o współadministrowaniu lub w innej pisemnej formie np. forma wiadomości elektronicznej. Wzór umowy o współadministrowaniu stanowi załącznik do niniejszej PBDO.
5. Współadministratorzy dokonują udostępnienia zasadniczej treści uzgodnień osobom, których dane dotyczą. Udostępnienie następuje w formie elektronicznej za pośrednictwem stron internetowych podmiotów oraz w formie papierowej w siedzibie podmiotów.

10. UDOSTĘPNIANIE DANYCH OSOBOWYCH

Nadzór:	ADO, IOD
Stosowanie:	ASI, wszyscy pracownicy

Administrator Danych Osobowych w uzasadnionym przypadku może podjąć decyzję o przekazaniu danych osobowych innym podmiotom. Udostępnienie danych osobowych następuje, gdy adresat ma własny cel i podstawę przetwarzania danych osobowych, a więc staje się odrębnym Administratorem Danych Osobowych.

10.1. ZASADY OGÓLNE UDOSTĘPNIANIA DANYCH

1. Podstawą udostępnienia danych może być::
   a. **udokumentowana zgoda osoby, której dane dotyczą na udostępnienie jej danych** - zgoda osoby, której dane dotyczą może służyć np. udostępnieniu przez pracodawcę firmie szkoleniowej, danych pracownika, w celu umożliwienia zawarcia z nim umowy;
   b. **wniosek od podmiotu uprawnionego do otrzymywania danych osobowych na podstawie przepisów prawa** - udostępnienie w związku z obowiązkiem wynikającym z przepisów prawa, wymaga wskazania przez wnioskodawcę zarówno szczegółowego przepisu w randze ustawy (tzn. ustawa oraz jej konkretne artykuły), a także celu i zakresu danych, które mają podlegać udostępnieniu;
   c. **konieczność zrealizowania umowy z innym podmiotem**, w ramach której istnieje konieczność udostępnienia danych,
   d. **prawnie uzasadniony interes wnioskodawcy** - prawnie uzasadniony interes wnioskodawcy, wskazany we wniosku o udostępnienie, wymaga wykazania, że ten interes jest faktyczny. Wnioskodawca musi także wykazać, że udostępnienie danych w tym celu jest niezbędne do jego zrealizowania, a także że jego interes przewyższa interesy osoby lub osób, których danych chce uzyskać.
2. Administrator Danych Osobowych nie wymaga korzystania z konkretnego wzoru wniosku o udostępnienie danych osobowych z zastrzeżeniem jednak, że wniosek musi zawierać niezbędne elementy umożliwiające dokonanie oceny zasadności wniosku takie, jak:
   a. dane podmiotu, który wnioskuje o uzyskanie danych;
   b. wskazanie podstawy udostępnienia;
   c. wskazanie osoby, której dane dotyczą;
   d. zakres danych, których ma dotyczyć udostępnienie;
   e. cel udostępnienia;
   f. podpis i dane osoby działającej w imieniu składającego wniosek.
3. Administrator Danych Osobowych dopuszcza składanie wniosku drogą elektroniczną opatrzonego podpisem elektronicznym (kwalifikowanym lub profilem zaufanym).

10.2. PROCEDURA OBSŁUGI WNIOSKU O UDOSTĘPNIENIE DANYCH

1. O otrzymanym wniosku należy niezwłocznie poinformować IOD, który udzieli wsparcia w ocenie jego zasadności oraz realizacji.
2. W przypadku otrzymania żądania w formie ustnej, w treści wiadomości e-mail, poprzez komunikator internetowy, itp. należy poinformować wnioskodawcę o konieczności sformalizowania wniosku o udostępnienie danych tak, aby zawierał wymagane informacje wskazane powyżej.
3. W przypadku otrzymania wniosku we właściwej formie, należy zweryfikować, czy zawiera on wszystkie niezbędne dane.
4. W przypadku stwierdzenia braków we wniosku, należy niezwłocznie skontaktować się z wnioskodawcą i poinformować go o konieczności uzupełnienia wniosku. Dopuszczalny jest kontakt telefoniczny lub z wykorzystaniem poczty e-mail, w celu przyśpieszenia procedury udostępnienia danych.
5. Jeżeli wnioskodawca nie udzieli odpowiedzi lub dodatkowych wyjaśnień, należy pozostawić wniosek bez rozpatrzenia, a po upływie 30 dniu przekazać decyzję o odmowie udostępnienia danych ze względu na błędy formalne we wniosku.
6. W przypadku stwierdzenia, że wskazany we wniosku prawnie uzasadniony interes wnioskodawcy nie jest rzeczywisty lub udostępnienie danych nie jest niezbędne do zrealizowania wskazanych celów, należy odmówić udostępnienia danych, wskazując na niewystarczające uzasadnienie prawnego interesu wnioskodawcy.
7. W przypadku powołania się na przepis prawa, należy dokonać weryfikacji podanego we wniosku przepisu prawa, tzn.
    a. Czy wskazany przepis prawa istnieje i jest obowiązujący?
    b. Czy przepis jest w randze ustawy?
    c. Czy treść przywołanego przepisu faktycznie uprawnia wnioskodawcę do żądania udostępnienia danych?
    d. Czy wskazany we wniosku cel przetwarzania jest spójny z celem wskazanym w przepisie?
8. Jeżeli wnioskodawca powołał się na przepis prawa, jednakże nie wskazał jego konkretnych artykułów, należy wezwać go do uszczegółowienia podstawy prawnej. Nie można udostępnić danych na podstawie przypuszczenia, że wskazany przepis faktycznie uprawnia wnioskodawcę do otrzymania danych.
9. Jeżeli wnioskodawca wskazał nieobowiązujący już przepis prawa lub przepis w randze rozporządzenia, należy wezwać go do wskazania właściwej podstawy prawnej.
10. Jeżeli wnioskodawca wskazał we wniosku cel udostępnienia niezgodny z celami, dla których dopuszcza możliwość udostępnienia danych wskazany przez niego przepis, należy poinformować wnioskodawcę o braku możliwości zrealizowania żądania udostępnienia ze względu na rozbieżność wskazanych celów i podstawy udostępnienia.
11. Jeżeli wskazany we wniosku przepis prawa nie uprawnia do udostępnienia danych, należy poinformować wnioskodawcę o braku możliwości zrealizowania żądania udostępnienia.
12. Jeżeli wskazany we wniosku zakres danych jest zbyt szeroki w odniesieniu do wskazanej przez wnioskodawcę podstawy prawnej, należy zwrócić się do wnioskodawcy o uzupełnienie podstawy prawnej lub zmianę zakresu żądanych danych. Do czasu udzielenia wyjaśnień, wniosek pozostaje bez rozpatrzenia. Po 30 dniach od wysłania dodatkowych pytań i braku uzyskania odpowiedzi, należy rozpatrzyć wniosek negatywnie.

13. W przypadku pozytywnej oceny wniosku, należy przekazać wniosek wraz z decyzją o udostępnieniu danych do Inspektora Ochrony Danych w celu zatwierdzenia udostępnienia.
14. Udostępnienie danych następuje w formie jakiej zażądał wnioskodawca, a w przypadku braku wskazania formy udostępnienia, jest realizowane w formie w jakiej został złożony wniosek.
15. Udostępnienie danych następuje z zastrzeżeniem konieczności zapewnienia ich poufności w czasie przekazania, tzn.
    a. w przypadku przekazywania drogą elektroniczną, należy dane zapisać w pliku zabezpieczonym hasłem, które zostanie przekazane wnioskodawcy ustaloną drogą komunikacji (nigdy w treści wiadomości zawierającej załącznik);
    b. w przypadku przekazywania drogą pocztową, należy zastosować dwie koperty, gdzie na wewnętrznej zostanie dodany dopisek "Do rąk własnych .....". Przesyłka pocztowa musi być rejestrowana i wysłana za potwierdzeniem odbioru;
    c. w przypadku osobistego odbioru, należy dokonać weryfikacji tożsamości wnioskodawcy poprzez okazanie dowodu osobistego lub innego dokumentu potwierdzającego tożsamość osoby fizycznej. Przekazanie danych odbywa się za pokwitowaniem, gdzie wnioskodawca wskazuje swoje imię, nazwisko, datę odbioru i potwierdza podpisem odebranie danych.
16. Każdy przypadek udostępnienia danych należy odnotować w wewnętrznym rejestrze stanowiącym załącznik do niniejszej PBDO.
17. Wniosek o udostępnienie wraz z decyzją o sposobie realizacji wniosku, w formie adnotacji dokonanej po zrealizowaniu wniosku przez osobę odpowiedzialną za rozpatrzenie wniosku, należy przechowywać przez okres 3 lat.

11. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

Powierzenie przetwarzania danych osobowych to umocowanie przez Administratora Danych Osobowych innego podmiotu do przetwarzania danych w jego imieniu. W relacji powierzenia mamy zatem do czynienia z ADO, który zleca procesorowi przetwarzanie danych osobowych w jego imieniu, na jego rzecz, we wskazanych przez niego celach i na określonych zasadach.

W przypadku powierzenia danych podmiot zewnętrzny otrzymuje dane osobowe na podstawie umowy powierzenia zawartej z Administratorem Danych Osobowych lub innego instrumentu prawnego. Dokument określa między innymi konkretny przedmiot, charakter, cel i czas, w jakim podmiot przetwarzający (procesor) może przetwarzać dane w imieniu ADO, a także obowiązki i zakres odpowiedzialności podmiotu, któremu powierzono przetwarzanie danych.

Podmiot przetwarzający zawsze jest odbiorą danych, co znajduje odzwierciedlenie w zapisach zawartych w RCPD.

Na etapie podejmowania decyzji o powierzeniu przetwarzania danych, ADO dokonuje analizy ryzyka.

11.1. Wybór podmiotu przetwarzającego

Wybór podmiotu przetwarzającego ma kluczowe znaczenie dla bezpieczeństwa danych osobowych. Administrator Danych Osobowych.

1. Podstawowe kryteria, które Administrator Danych Osobowych bierze pod uwagę przy wyborze podmiotu przetwarzającego to:
   a. wiedza fachowa – np. doświadczenie organizacji, kompetencje personelu potwierdzone np. certyfikatami, wdrożenie norm, udokumentowane wcześniejsze realizacje;
   b. wiarygodność – okres prowadzenia działalności, legalność działalności, referencje od innych klientów;
   c. zasoby – posiadanie odpowiednich zasobów gwarantujących skuteczne wdrożenie zabezpieczeń technicznych i organizacyjnych zgodnych z RODO
2. Czynnikiem decydującym o wyborze danego podmiotu przetwarzającego jest wynik pisemnej Ankiety dla podmiotu przetwarzającego, która ma na celu określenie, czy podmiot przetwarzający może dać ADO gwarancję bezpiecznego przetwarzania danych osobowych w sposób zgodny z wymaganiami RODO.

11.2. Weryfikacja podmiotu przetwarzającego przed zawarciem umowy powierzenia

Zasady postępowania w sytuacji wystąpienia potrzeby powierzenia przetwarzania danych osobowych:

1. Pracownik informuje Administratora Danych Osobowych i Inspektora Ochrony Danych o potrzebie powierzenia danych osobowych do przetwarzania.
2. Informowanie powinno odbyć się co najmniej z 7 dniowym wyprzedzeniem przed terminem zawarcia umowy powierzenia danych osobowych.
3. Administrator Danych Osobowych (lub wyznaczony przez niego pracownik) kieruje do podmiotu, któremu zostaną powierzone dane, prośbę o wypełnienie Ankiety dla podmiotu przetwarzającego. Ankieta przekazywana jest w formie elektronicznej za pośrednictwem wiadomości e-mail. Wzór Ankiety stanowi załącznik do niniejszej PBDO.
4. Administrator Danych Osobowych wyznacza procesorowi termin na wypełnienie i dostarczenie do niego wypełnionej Ankiety.
5. Wypełniona Ankieta poddawana jest weryfikacji i ocenie przez Administratora Danych Osobowych wg poniższych zasad:
   a. za każdą udzieloną odpowiedź „TAK", podmiot ankietowany otrzymuje 1 punkt;
   b. za każdą udzieloną odpowiedź „NIE" lub „NIE WIEM", podmiot ankietowany otrzymuje 0 punktów;
   c. w przypadku, gdy na ankietowanym podmiocie nie ciąży prawny obowiązek wyznaczenia Inspektora Ochrony Danych, pytanie nie podlega ocenie;
   d. Administrator Danych Osobowych dokonuje oceny poprzez obliczenie, na jaki procent pytań podmiot ankietowany udzielił odpowiedzi „TAK", wg wzoru:

$$\frac{\textit{liczba udzielonych odpowiedzi „TAK"}}{\textit{liczba pytań podlegających ocenie}}$$

6. Uzyskanie wyniku Ankiety na poziomie 60% lub więcej, oznacza ocenę pozytywną, co Administrator Danych Osobowych odnotowuje w Ankiecie. W takiej sytuacji przystępuje się do przygotowania umowy powierzenia przetwarzania danych, zgodnie z procedurą opisaną w rozdziale 11.3.
7. Uzyskanie wyniku Ankiety na poziomie niższym niż 60%, oznacza ocenę negatywną, co Administrator Danych Osobowych odnotowuje w Ankiecie i informuje podmiot o braku możliwości podjęcia współpracy.
8. W przypadku uzyskania oceny negatywnej, Administrator Danych Osobowych może przeprowadzić indywidualną analizę, czy korzyści wynikające z nawiązania współpracy z podmiotem przetwarzającym, a w efekcie powierzenia mu przetwarzania danych, przewyższają negatywne skutki braku nawiązania współpracy i ryzyko powierzenia danych. Na podstawie analizy ADO może podjąć decyzję o warunkowym powierzeniu przetwarzania danych.
9. Warunkiem zawarcia umowy powierzenia będzie wdrożenie w określonym czasie przez podmiot przetwarzający uzgodnionych przez strony środków technicznych i organizacyjnych gwarantujących bezpieczeństwo przetwarzania danych osobowych.
10. W przypadku warunkowego powierzenia przetwarzania danych, Administrator Danych Osobowych informuje podmiot przetwarzający o negatywnym wyniku Ankiety, zobowiązuje w treści umowy powierzenia, podmiot do wdrożenie niezbędnych działań mających na celu podniesienie poziomu wdrożenia RODO. ADO informuje podmiot o planowanym powtórzeniu ankiety po upływie 6 miesięcy.
11. Umowa powierzenia zostanie zawarta pod warunkiem rozwiązującym, co oznacza, że w przypadku nie wywiązania się przez podmiot przetwarzający z ciążących na nim obowiązków wdrożenia niezbędnych zabezpieczeń, umowa zostanie rozwiązana.
12. Administrator Danych Osobowych rozpoczyna procedurę zawarcia umowy powierzenia przetwarzania danych.
13. Ankieta przechowywana jest wraz z zawartą umową powierzenia.
14. Informacja o dacie i wyniku weryfikacji podmiotu przetwarzającego odnotowywana jest w rejestrze umów powierzenia.

11.3. PROCEDURA ZAWARCIA UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Celem niniejszej procedury jest zapewnienie zgodności przetwarzania danych z RODO, czyli ze wskazanymi w tym akcie prawnym zasadami i warunkami przetwarzania danych osobowych.

Zasady postępowania w przypadku zawierania umowy powierzenia przetwarzania danych:

1. Inspektor Ochrony Danych w porozumieniu z pracownikiem przygotowuje projekt umowy powierzenia danych osobowych innemu podmiotowi według wzoru załączonego do niniejszej Polityki Bezpieczeństwa Danych Osobowych.
2. Projekt umowy powinien określać:
   a. kategorie powierzanych danych (np. dane kategorii zwykłej, dane kategorii szczególnej, dane o wyrokach skazujących);
   b. zakres powierzonych danych (np. imię i nazwisko, nr PESEL, adres zamieszkania, informacje o stanie zdrowia itp.),
   c. kategorie osób (np. pacjenci, pracownicy, współpracownicy itp.),
   d. cel przetwarzania tj. w jakim celu dane zostaną powierzone zewnętrznemu podmiotowi.

e. zobowiązanie o zachowaniu poufności przez podmiot przetwarzający oraz osoby biorące udział w przetwarzaniu;
f. zasady dotyczące obsługi praw jednostki, w szczególności obowiązek informowania Administratora Danych Osobowych o otrzymaniu zgłoszenia i sposobie jego realizacji;
g. zobowiązanie do niezwłocznego zgłaszania ADO wszelkich podejrzeń o naruszeniu ochrony powierzonych danych;
h. opis sposobu przekazania danych po zakończeniu trwania przetwarzania;
i. opis realizacji uprawnień kontrolnych;
j. zasady dalszego powierzania danych przez podmiot przetwarzający.

3. Sporządzony projekt umowy przedkładany jest Administratorowi Danych Osobowych do podpisu.
4. W przypadku konieczności naniesienia poprawek lub uzupełnień, projekt umowy przesyłany jest ponownie do Inspektora Ochrony Danych w celu weryfikacji.
5. Informacja o zawarciu umowy powierzenia odnotowywana jest w rejestrze umów powierzenia, który stanowi załącznik do niniejszej PBDO.
6. Rejestr umów powierzenia zawiera:
   a. nazwę i adres podmiotu, któremu dane zostały powierzone;
   b. datę zawarcia umowy;
   c. kategorie powierzonych danych
   d. zakres powierzonych danych;
   e. kategorie osób, których dane dotyczą;
   f. okres powierzenia;
   g. cel powierzenia;
   h. informację, czy i kiedy dokonano weryfikacji podmiotu przetwarzającego;
   i. informację o wyniku weryfikacji podmiotu przetwarzającego;
   j. uwagi.
7. Inspektor Ochrony Danych ma prawo do występowania do poszczególnych pracowników o przekazanie informacji na temat zawartych umów powierzenia przetwarzania danych w imieniu Administratora Danych Osobowych.

11.4. Procedura kontroli podmiotu przetwarzającego w trakcie trwania współpracy

1. Administrator Danych Osobowych wiedząc, jak duże znaczenie dla ochrony danych osobowych ma weryfikacja spełniania przez procesora obowiązków wynikających z RODO, zgodnie z art. 28 ust. 3 pkt h RODO ma możliwość przeprowadzenia okresowej lub doraźnej kontroli zmierzającej do ustalenia, czy środki zastosowane przez podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych mu danych osobowych nadal spełniają postanowienia umowy powierzenia i są zgodnie z wymogami nałożonymi przez RODO.
2. Decyzję, czy kontrola w odniesieniu do danego procesora będzie przeprowadzona, czy będzie miała ona charakter okresowy, czy doraźny, każdorazowo podejmuje Administrator Danych Osobowych w porozumieniu z Inspektorem Ochrony Danych, analizując charakter powierzonych danych, ich liczbę,

jednorazowość lub ciągłość przetwarzania, a także zakres i szczegółowość, a także biorąc pod uwagę wynik wstępnej weryfikacji procesora (zgodnie z procedurą opisaną w punkcie 14.3 niniejszej PBDO).

3. Kontrola podmiotu przetwarzającego może mieć postać zdalną lub osobistą w siedzibie podmiotu przetwarzającego.
4. W przypadku kontroli zdalnej, Administrator Danych Osobowych może posłużyć się powtórnie ankietą dla podmiotu przetwarzającego dodatkowo żądając dowodów zapewnienia przez podmiot przetwarzający wystarczających gwarancji ochrony tych danych, a także przetwarzania ich zgodnie z przepisami o ochronie danych osobowych i zawartą umową powierzenia, np. w postaci dowodów na zweryfikowanie dalszych podmiotów przetwarzających w zakresie dawania odpowiednich gwarancji ochrony danych lub listy osób upoważnionych do przetwarzania powierzonych danych, w tym dowodów ich upoważnienia, zobowiązana do poufności oraz przeszkolenia w zakresie ochrony danych i obowiązujących procedur.
5. W przypadku kontroli osobistej w siedzibie podmiotu przetwarzającego, Administrator Danych Osobowych stosuje się do zapisów zawartych w umowie powierzenia w paragrafie „Prawo kontroli", w którym podany zostaje termin z jakim Administrator Danych Osobowych zobowiązany jest uprzedzić procesora o kontroli.
6. W ramach kontroli Administrator Danych Osobowych ma między innymi prawo do:
   a. kontroli pomieszczeń i sprzętu używanego przy przetwarzaniu danych osobowych, w zakresie niezbędnym do stwierdzenia prawidłowości stosowanych zabezpieczeń danych osobowych;
   b. wglądu w dokumentację ochrony danych, zwłaszcza w zakresie zarządzania uprawnieniami, postępowania przy naruszeniu danych, realizacji praw osób, obowiązków osób upoważnionych;
   c. wglądu do kopii umów dalszego powierzenia danych;
   d. uzyskania listy osób upoważnionych do przetwarzania powierzonych danych, w tym dowodów ich upoważnienia, zobowiązana do poufności oraz przeszkolenia w zakresie ochrony danych i obowiązujących procedur;
   e. uzyskania dowodów na wdrożenie adekwatnych do ryzyk i zagrożeń środków ochrony;
   f. dowodów na zapewnienie skutecznego nadzoru nad ochroną danych.
7. Po przeprowadzonej kontroli, Administrator Danych Osobowych uprawniony jest do przekazania podmiotowi przetwarzającemu pisemnych zaleceń pokontrolnych wraz z terminem ich realizacji.
8. Administrator Danych Osobowych weryfikuje, czy uchybienia stwierdzone podczas kontroli zostały usunięte.
9. Kontrola podmiotu przetwarzającego przeprowadzana jest przez Administratora Danych Osobowych, przez wyznaczoną przez niego osobę lub Inspektora Ochrony Danych.

11.5. Zakończenie relacji z podmiotem przetwarzającym

Po zakończeniu współpracy związanej z przetwarzaniem danych, zależnie od ustaleń pomiędzy ADO a podmiotem przetwarzającym uwzględnionych w umowie powierzenia lub innym instrumencie prawnym, procesor usuwa lub zwraca ADO wszelkie dane osobowe oraz usuwa wszelkie ich istniejące kopie, chyba że przepisy prawa stanowią inaczej i nakazują procesorowi dalsze przechowywanie danych osobowych. W takiej sytuacji procesor staje się samodzielnym ADO.

1. Po zakończeniu współpracy ADO odbiera od podmiotu przetwarzającego wszystkie powierzone mu dane osobowe lub odbiera potwierdzenie ich usunięcia.
2. W przypadku, gdy przepisy prawa nakładają na podmiot przetwarzający obowiązek dalszego przetwarzania danych, ADO odnotowuje w rejestrze umów powierzenia przez, jaki okres od zakończenia współpracy dane będą w posiadaniu procesora.

12. CENTRUM KULTURY PROMOCJI I TURYSTYKI W PONIATOWEJ JAKO PODMIOT PRZETWARZAJĄCY

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

Organizacja realizując zadania (związane z przetwarzaniem danych osobowych) na rzecz innego Administratora Danych Osobowych w celach i zakresie ściśle określonych przez tego ADO, pełni rolę podmiotu przetwarzającego.

Wprowadza się następujące zasady obowiązujące przy pełnieniu przez organizację roli procesora:

3. Przed przystąpieniem do współpracy związanej z przetwarzaniem powierzonych danych, na życzenie podmiotu powierzającego, podmiot przetwarzający czynnie uczestniczy w procesie weryfikacji jej jako procesora.
4. Przed przystąpieniem do współpracy podmiot przetwarzający zawiera z Administratorem Danych Osobowych umowę powierzenia danych. Treść umowy powierzenia danych każdorazowo konsultowana jest z Inspektorem Ochrony Danych.
5. Powierzone przez Administratora Danych Osobowych dane podmiot przetwarzający przetwarza wyłącznie w celu wywiązania się z zadań określonych w umowie głównej oraz umowie powierzenia oraz na zasadach i warunkach ściśle określonych przez ADO.
6. Podmiot przetwarzający prowadzi rejestr kategorii przetwarzania danych.
7. Podmiot przetwarzający zobowiązuje się przy przetwarzaniu powierzonych danych osobowych do ich zabezpieczenia poprzez stosowanie odpowiednich środków technicznych i organizacyjnych określonych w niniejszej PBDO, zapewniających adekwatny stopień bezpieczeństwa, odpowiadający ryzyku związanemu z przetwarzaniem tych danych osobowych, w szczególności poprzez zabezpieczenie danych osobowych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną oraz zmianą, utratą, uszkodzeniem lub zniszczeniem danych.
8. Procesor dokłada wszelkiej staranności przy przetwarzaniu powierzonych mu danych.
9. Podmiot przetwarzający nadaje upoważnienia do przetwarzania danych osobowych wszystkim osobom, które będą przetwarzały powierzone przez Administratora Danych Osobowych dane.
10. Podmiot przetwarzający udziela ADO, na każde jego żądanie, informacji na temat przetwarzania powierzonych mu danych osobowych oraz umożliwia ADO realizację prawa do przeprowadzenia kontroli zmierzającej do ustalenia, czy środki zastosowane przez podmiot przetwarzający przy przetwarzaniu i zabezpieczeniu powierzonych mu danych osobowych spełniają postanowienia łączącej strony umowy i są zgodnie z wymogami nałożonymi przez RODO.

11. Po zakończeniu współpracy związanej z przetwarzaniem danych procesor zwraca ADO wszelkie dane osobowe oraz usuwa wszelkie istniejące kopie tych danych. Termin zwrotu i usunięcia danych procesor ustala z ADO w treści umowy powierzenia danych.
12. Podmiot przetwarzający, w miarę możliwości pomaga ADO w niezbędnym zakresie wywiązywać się z obowiązku odpowiadania na żądania osoby, której dane dotyczą oraz wywiązywania się z obowiązków określonych w art. 32-36 RODO.
13. W przypadku stwierdzenia naruszenia ochrony danych osobowych, procesor bez zbędnej zwłoki zgłasza je Administratorowi Danych Osobowych.
14. Podmiot przetwarzający zachowuje w tajemnicy wszelkie informacje, materiały, dokumenty i dane osobowe otrzymane od Administratora Danych Osobowych i od współpracujących z nim osób oraz dane uzyskane w jakikolwiek inny sposób, zamierzony czy przypadkowy w formie ustnej, pisemnej lub elektronicznej.

12.1. Dalsze powierzenie przetwarzania danych

W sytuacji, gdy organizacja jako podmiot przetwarzający (procesor) do realizacji zadania korzysta z wsparcia innych podmiotów, do których mogą trafić dane osobowe powierzone przez Administratora Danych Osobowych, dochodzi do sytuacji dalszego powierzenia danych, a podmiot trzeci ma status innego podmiotu przetwarzającego (dalszego podmiotu przetwarzającego).

1. W sytuacji, gdy do realizacji danego zadania związanego z przetwarzaniem danych osobowych podmiot przetwarzający chce skorzystać z wsparcia innych podmiotów, weryfikuje on zapisy w umowie powierzania w celu sprawdzenia, czy Administrator Danych Osobowych dopuszcza do dalszego powierzania danych, a następnie postępuje zgodnie z zasadami opisanymi w umowie powierzenia.
2. W przypadku zgody ogólnej na dalsze powierzenie danych zawartej w umowie powierzenia, dalsze kroki realizowane są zgodnie z wcześniej opisaną procedurą weryfikacji podmiotu przetwarzającego oraz procedurą zawierania umów powierzenia z zastrzeżeniem, że umowa w sposób jednoznaczny określa, że dotyczy relacji pomiędzy podmiotem przetwarzającym (procesorem) a dalszym podmiotem przetwarzającym (subprocesorem).
3. W przypadku zgody szczególnej zawartej w umowie powierzenia, podmiot przetwarzający ma możliwość skorzystania z wsparcia wyłącznie konkretnego subprocesora wskazanego przez ADO i/lub na ściśle określonych przez ADO zasadach.
4. Jeżeli umowa powierzenia danych nie reguluje kwestii dalszego powierzenia danych, podmiot przetwarzający zwraca się do Administratora Danych Osobowych z prośbą o zgodę na skorzystanie ze wsparcia konkretnego subprocesora.
5. Wybrany subprocesor musi spełniać te same gwarancje i obowiązki, jakie zostały nałożone na podmiot przetwarzający w umowie zawartej z ADO.
6. W przypadku braku zgody na dalsze powierzenia danych, podmiot przetwarzający odstępuje od dalszego powierzenia danych.
7. Podmiot przetwarzający ma świadomość, że ponosi pełną odpowiedzialność za przetwarzanie danych przez subprocesora.

13. PROCEDURA REALIZACJI OBOWIĄZKU INFORMACYJNEGO

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

Jednym z podstawowych obowiązków ADO oraz osób upoważnionych przez ADO do przetwarzania danych w jego imieniu, jest informowanie osoby, której dane dotyczą o przetwarzaniu jej danych, niezależnie czy dane pozyskiwane są bezpośrednio od tej osoby, czy też w inny sposób.

Celem niniejszej procedury jest zapewnienie realizacji podstawowego obowiązku ADO, którym jest informowanie osób, których dane dotyczą, **zgodnie z zasadami i warunkami przetwarzania danych osobowych wskazanymi w RODO.**

W celu wypełnienia obowiązku informacyjnego wprowadza się następujące reguły:

1. Przed podjęciem działań związanych z pozyskaniem danych osobowych należy umożliwić osobie zapoznanie się z klauzulą informacyjną, a informowanie to powinno się dokonać bez prośby zainteresowanego.
2. Organizacja wdrożyła warstwowość obowiązku informacyjnego poprzez stosowanie klauzul w wersji skróconej i pełnej oraz informacji o przetwarzaniu danych osobowych na stosowanych formularzach, drukach, na których zbierane są dane osób - w formie papierowej lub elektronicznej.
3. Pierwsza warstwa obowiązku informacyjnego (klauzula skrócona) zawiera najistotniejsze informacje o Administratorze Danych Osobowych, Inspektorze Ochrony Danych, przysługujących prawach związanych z ochroną danych oraz informację, gdzie można zapoznać się z pełną treścią klauzuli informacyjnej.
4. Druga warstwa obowiązku informacyjnego, pełna klauzula informacyjna – Przewodnik ochrony danych, zawiera wszystkie informacje z art. 13 i 14 RODO.
5. Rolą informacji o przetwarzaniu danych osobowych jest wskazanie miejsca, w którym osoba fizyczna może zapoznać się z pełną treścią klauzuli informacyjnej.
6. Obowiązek informacyjny spełnia się poprzez:
   a. pozostawienie skróconej treści klauzuli informacyjnej w miejscu dostępnym dla osób fizycznych, od których pozyskiwane są dane osobowe;
   b. zamieszczenie informacji o przetwarzaniu danych osobowych na stosowanych formularzach, drukach, umowach, itp., na których zbierane są dane osobowe (zarówno w formie papierowej jak i elektronicznej);
   c. udostępnienie pełnej treści klauzuli informacyjnej (Przewodnik ochrony danych) w wersji papierowej w siedzibie Administratora Danych Osobowych;
7. Publikację pełnej treści klauzuli informacyjnej (Przewodnik ochrony danych) na stronie internetowej oraz Biuletynie Informacji Publicznej jednostki.
8. Treść informacji powinna być czytelna, przejrzysta i zrozumiała, wyrażona w łatwo dostępnej formie, jasnym i prostym językiem dla osób, których dane są lub mogą być przetwarzane.

9. Treść każdej nowej, tworzonej przez pracownika klauzuli należy skonsultować każdorazowo z Inspektorem Ochrony Danych, w celu potwierdzenia zgodności z obowiązującymi przepisami prawa.

13.1. INDYWIDUALNA REALIZACJA OBOWIĄZKU INFORMACYJNEGO

1. Pełny obowiązek informacyjny wobec wszystkich osób, których dane przetwarza jednostka (m.in. uczestników zajęć lub wydarzeń kulturalnych, ich rodziców lub opiekunów prawnych, pracowników, rodzin pracowników, współpracowników, stażystów, praktykantów, kontrahentów dostawców, uczestników zamówień publicznych) spełnia się poprzez:
   a. publikację pełnej treści klauzuli informacyjnej (Przewodnik ochrony danych) w formie elektronicznej na stronie internetowej jednostki w zakładce poświęconej ochronie danych osobowych oraz na stronach Biuletynu Informacji Publicznej, oraz w wersji papierowej w siedzibie Administratora Danych Osobowych, w miejscu dostępnym dla osób zainteresowanych, np. sekretariat.
   b. zamieszczenie informacji o przetwarzaniu danych w stopkach wiadomości e-mail wysyłanych z kont służbowych.

Dodatkowo:

1. obowiązek informacyjny **wobec kandydatów na uczestników zajęć lub wydarzeń kulturalnych, ich rodziców lub opiekunów prawnych** spełnia się poprzez:
   a. umieszczenie skróconej treści klauzuli informacyjnej w siedzibie organizacji, np. sekretariat, gdzie pobierane są dane osobowe;
   b. zamieszczenie krótkich informacji o przetwarzaniu danych osobowych na stosowanych do zbierania danych formularzach i drukach (formularz stosowany w procesie rekrutacji uczniów);
2. obowiązek informacyjny **wobec kandydatów do pracy** spełnia się poprzez:
   a. zamieszczenie krótkich informacji o przetwarzaniu danych osobowych w treści ogłoszenia o pracę w formie papierowej lub elektronicznej (w tym na stronie Biuletynu Informacji Publicznej);
3. obowiązek informacyjny **wobec osób monitorowanych** spełnia się poprzez:
   a. umieszczenie skróconych klauzul informacyjnych zawierających piktogram kamery w widocznym miejscu przed wejściem w obszar monitorowany;
4. obowiązek informacyjny **wobec osób odwiedzających media społecznościowe jednostki** spełnia się poprzez:
   a. zamieszczenie krótkich informacji o przetwarzaniu danych osobowych na profilach mediów społecznościowych;
5. obowiązek informacyjny **wobec osób kontaktowych w zawartych umowach** spełnia się poprzez:
   a. zamieszczenie krótkich informacji o przetwarzaniu danych osobowych na stosowanych wzorach umów, zarówno w formie papierowej, jak i elektronicznej;

14. PROCEDURA OBSŁUGI PRAW WYNIKAJĄCYCH Z RODO

Nadzór:	ADO, IOD
Stosowanie:	wszyscy pracownicy

1. **Celem niniejszej procedury** jest zapewnienie rzetelności i przejrzystości przetwarzania danych osobowych oraz usystematyzowanie działań podejmowanych w ramach realizacji praw osób, których dane są przetwarzane.
2. Procedurę stosuje się każdorazowo, gdy osoba, której dane dotyczą, domaga się skorzystania z przysługujących jej praw, takich jak:
   - prawo dostępu do danych,
   - prawo do sprostowania danych,
   - prawo do usunięcia danych (prawo do „bycia zapomnianym"),
   - prawo do ograniczenia przetwarzania,
   - prawo do wniesienia sprzeciwu wobec przetwarzania,
   - prawo do przenoszenia danych.

Obsługa uprawnień, które zostały zawarte w przepisach rozdziału III RODO stanowi gwarancję poszanowania praw i wolności osób fizycznych i jako podstawowe prawo realizowane jest poprzez wypełnienie poniższych reguł.

1. Administrator Danych Osobowych gwarantuje by wszelkie przekazywane informacje były sformułowane w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
2. Administrator Danych Osobowych zapoznaje pracowników z procedurą dotyczącą sposobu realizacji praw osób, których dane dotyczą.
3. Administrator Danych Osobowych udostępnia w swojej siedzibie w wersji papierowej oraz na stronie internetowej i Biuletynie Informacji Publicznej w wersji elektronicznej procedurę, do kogo i w jakiej formie osoby mogą skierować żądanie realizacji praw. Procedura stanowi integralną część Przewodnika ochrony danych.
4. Realizacja żądania osób fizycznych w zakresie realizacji praw wynikających z RODO należy do obowiązków Inspektora Ochrony Danych.
5. Zgłoszenie żądania osoby fizycznej powinno zawierać:
   a. imię, nazwisko osoby, której zgłoszenie dotyczy,
   b. opis zgłoszonego żądania wraz ze wskazaniem ewentualnych zastrzeżeń,
   c. podpis osoby zgłaszającej żądanie w przypadku zgłoszeń pisemnych,
   d. pełnomocnictwo, jeśli w imieniu zgłaszającego żądanie kieruje pełnomocnik,
   e. informacje o preferowanej formie odpowiedzi, jeżeli kanał odpowiedzi ma być inny niż zgłoszone żądanie.
6. Pracownik może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby składającej żądanie w przypadku, gdy ma co do niej uzasadnione wątpliwości.
7. Jeżeli zgłoszenie nastąpiło w formie ustnej, pracownik zobowiązany jest do sporządzenia notatki, zawierającej dane, o których mowa w punkcie 5.

8. W przypadku skierowania żądania realizacji praw bezpośrednio pracownikowi, zobowiązany jest on najpóźniej w terminie 7 dni przesłać treść żądania Inspektorowi Ochrony Danych.
9. Pracownik jest zobowiązany do udzielania informacji IOD niezbędnych do realizacji żądania osoby fizycznej.
10. Wprowadza się obowiązek rejestracji każdego wniosku o realizację praw osób wpływający bezpośrednio do siedziby organizacji lub na skrzynki mailowe pracowników, poprzez wpisanie do rejestru obsługi praw osób fizycznych wraz ze wskazaniem daty otrzymania wniosku. Wzór rejestru obsługi praw osób fizycznych stanowi załącznik do niniejszej PBDO.
11. Odpowiedź na wniosek zostaje udzielona bez zbędnej zwłoki, jednak nie później niż w terminie jednego miesiąca od dnia otrzymania zgłoszenia.
12. W uzasadnionych przypadkach tj. z uwagi na skomplikowany charakter żądania lub liczbę zgłoszeń, okres udzielenie odpowiedzi może zostać wydłużony maksymalnie o kolejne dwa miesiące. W takim przypadku, informuje się osobę fizyczną o niemożności rozpoznania jej wniosku w terminie, przyczynie opóźnienia oraz planowanym terminie udzielenie odpowiedzi.
13. W przypadku, gdy realizacja wniosku nie jest możliwa, Administrator Danych Osobowych informuje osobę o powodach braku podjęcia działań oraz możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

15. ŚRODKI OCHRONY DANYCH OSOBOWYCH

Nadzór:	ADO, IOD, ASI,
Stosowanie:	wszyscy pracownicy

Administrator Danych Osobowych uwzględniając charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia, ma obowiązek zapewnić bezpieczeństwo przetwarzania danych osobowych poprzez wdrożenie odpowiednich środków technicznych i organizacyjnych.

Środki organizacyjne mają charakter wewnętrznych norm prawnych, przyjętych zasad postępowania oraz polityk bezpieczeństwa. Środki techniczne mają zwykle charakter materialny i odnoszą się do pomieszczeń, gdzie przetwarzane są dane (zabezpieczenia fizyczne), lub charakter informatyczny.

15.1. ŚRODKI ORGANIZACYJNE

1. Opracowano i wdrożono Politykę Bezpieczeństwa Danych Osobowych.
2. Opracowano i wdrożono Instrukcję Zarzadzania Systemami Informatycznymi .
3. Opracowano i wdrożono procedurę postępowania w sytuacji naruszenia bezpieczeństwa danych osobowych.
4. Opracowano i wdrożono procedurę realizacji praw osób, których dane dotyczą.
5. Wyznaczono Inspektora Ochrony Danych oraz Administratora Systemów Informatycznych.
6. Do przetwarzania danych dopuszczone są wyłącznie osoby posiadające upoważnienie:

a. wobec pracowników stosuje się upoważnienia adekwatne do zakresu przetwarzania zgodnego z zajmowanym stanowiskiem służbowym i zakresem realizowanych zadań;
b. upoważnienia do przetwarzania danych pracowników mających dostęp do danych szczególnej kategorii i pomieszczeń szczególnej ochrony, zawierają szczegółowe umocowania;
c. prowadzony jest rejestr osób upoważnionych do przetwarzania danych.

7. Wprowadzono obowiązek odbierania oświadczenia pracowników o zapoznaniu się z przepisami dotyczącymi ochrony danych osobowych oraz wewnętrznymi regulacjami bezpieczeństwa danych osobowych Administratora Danych Osobowych wraz z obowiązkiem zachowania poufności wszelkich informacji uzyskanych w ramach wykonywanych obowiązków, również po ustaniu zatrudnienia. Wzór oświadczenia dla pracownika (przetwarzającego dane) oraz oświadczenia o zachowaniu poufności dla osoby nie przetwarzającej danych osobowych, stanowią załączniki do PBDO.
8. Opracowano i wdrożono Rejestr czynności przetwarzania danych (RCPD). Wzór rejestru stanowi załącznik do niniejszej PBDO.
9. W przypadku przetwarzania danych osobowych powierzonych przez inny podmiot, Administrator Danych Osobowych prowadzi Rejestr kategorii czynności przetwarzania. Wzór rejestru stanowi załącznik do niniejszej PBDO.
10. Wprowadzono obowiązek bezpiecznego powierzania danych osobowych podmiotom zewnętrznym poprzez zawieranie umów powierzenia (lub innych instrumentów prawnych) oraz zobowiązania do zachowania danych osobowych w poufności.
11. Wprowadzono procedurę weryfikacji podmiotu przetwarzającego przed zawarciem umowy powierzenia oraz określono zasady przeprowadzania okresowej kontroli procesora.
12. Wprowadzono obowiązek cyklicznego szkolenia pracowników z obowiązujących przepisów dotyczących ochrony danych osobowych, jak i wewnętrznych regulacji bezpieczeństwa danych stosowanych przez Administratora Danych Osobowych.
13. Wprowadzono obowiązek cyklicznego prowadzenia dla pracowników szkoleń podnoszących świadomość zagrożeń związanych z nieautoryzowanym dostępem fizycznym do systemów IT służących do przetwarzania danych osobowych, a także szkoleń z zakresu cyberbezpieczeństwa.
14. Wprowadzono obowiązek stosowania zasady **„czystego biurka i ekranu"** w szczególności poprzez:
    a. schowanie wszystkich dokumentów, nośników zawierających dane osobowe w miejsce niedostępne dla innych osób w trakcie pracy, w trakcie sprzątania pomieszczeń oraz po zakończeniu pracy;
    b. dbanie o porządek, poprzez pozostawienie na stanowisku pracy wyłącznie dokumentów, które są niezbędne do wykonywania czynności służbowych;
    c. blokowanie dostępu lub wylogowanie się z systemu przy czasowym opuszczeniu stanowiska pracy;
    d. zamknięcie wszystkich aplikacji, wylogowanie się z systemu i wyłączenie komputera po zakończeniu pracy;
    e. zachowanie porządku na pulpicie komputera poprzez cotygodniowy przegląd połączony z porządkowaniem oraz usuwaniem zbędnych folderów i plików znajdujących się na pulpicie systemu oraz w folderach plików pobranych.
15. Wprowadzono obowiązek dbania o prawidłową wentylację komputerów (zabrania się zasłaniania kratek wentylatorów meblami, zasłonami lub stawiania komputerów tuż przy ścianie).

16. Zabrania się podłączania do listew podtrzymujących napięcie przeznaczonych dla sprzętu komputerowego innych urządzeń, szczególnie tych łatwo powodujących spięcia (np. grzejniki, czajniki, wentylatory).
17. Wprowadzono obowiązek ustawiania monitora w sposób uniemożliwiający przeglądanie wyświetlanych treści osobom nieupoważnionym.
18. Wydano zalecenie zamykania okien w razie opadów czy innych zjawisk atmosferycznych, które mogą zagrozić bezpieczeństwu danych osobowych.

15.2. Zabezpieczenia fizyczne

Częściowy opis zabezpieczeń fizycznych znajduje się w Polityce kluczy.

1. W budynku CKPiT zastosowano ochronę fizyczną w postaci osób monitorujących dostęp do obiektu w godzinach pracy.
2. Zainstalowano system monitoringu wizyjnego.
3. Do przechowywania danych osobowych w szczególności wrażliwych stosowane są szafy zamykane na klucze lub zamki szyfrowane, wprowadzono obowiązek zamykania szaf, biurek, szuflad na klucze, zamki.
4. W części budynku zamontowano rolety antywłamaniowe,
5. Zastosowano oświetlenie wewnętrzne ewakuacyjne, zewnętrzne zmierzchowe wraz z detekcją ruchu w miejscach szczególnie wrażliwych.
6. Umieszczono oznaczenia zawierające informację o monitoringu i zabezpieczeniach celem odstraszenia potencjalnych włamywaczy.
7. Wyszczególniono specjalne pomieszczenie z kontrolowaną wilgotnością i temperaturą celem prawidłowego przechowywania i zapobieżenia ich uszkodzeniu.

15.3. Zabezpieczenia techniczne (informatyczne)

Szczegółowy opis zastosowanych środków technicznych (informatycznych), znajduje się w Instrukcji Zarządzania Systemami Informatycznymi.

16. Procedura dostępu do pomieszczeń szczególnie chronionych

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Szczegółowy opis dostępu do pomieszczeń szczególnie chronionych zawarty jest w Polityce Kluczy CKPiT w Poniatowej.

17. STRATEGIE OCHRONY DANYCH W FAZIE PROJEKTOWANIA I FAZIE DOMYŚLNEJ

Nadzór:	ADO, IOD, ASI
Stosowanie:	wszyscy pracownicy

Privacy by design oraz privacy by default, czyli uwzględnienie ochrony danych w fazie projektowania oraz domyślna ochrona danych, to zasady kluczowe z punktu widzenia ochrony danych. Oznaczają one konieczność przeprowadzenia oceny ryzyka, jakim obarczone jest przetwarzanie danych w każdym planowanym procesie (przy uwzględnieniu określonych narzędzi i technologii), zaplanowanie adekwatnych do ryzyka oraz kategorii danych, ich zakresu, celu oraz kontekstu przetwarzania, organizacyjnych i technicznych środków bezpieczeństwa, a następnie określenie sposobów, i zgodne z nimi, monitorowanie przydatności i skuteczności stosowanych zabezpieczeń. Celem nadrzędnym jest doprowadzenie do sytuacji, w której domyślnie przetwarzane będą wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu przetwarzania określonego przez Administratora Danych Osobowych.

17.1. STRATEGIA OCHRONY DANYCH W FAZIE PROJEKTOWANIA

Uwzględniając koncepcję ochrony danych w fazie projektowania Administrator Danych Osobowych już podczas planowania systemu ochrony danych osobowych wdraża takie środki, by od samego początku chronić przetwarzane dane oraz prywatność osób, których dane dotyczą. W tym celu Administrator Danych Osobowych wprowadza następujące reguły:

1. Każde planowane przedsięwzięcie w organizacji musi zostać poprzedzone analizą wpływu planowanych zmian na bezpieczeństwo danych osobowych.
2. Jako planowane procesy, w których Administrator Danych Osobowych zobowiązany jest wziąć pod uwagę bezpieczeństwo danych osobowych wyróżnia się w szczególności:
   a. przystąpienie do przetargu w ramach zamówień publicznych,
   b. przystąpienie do projektów realizowanych ze środków europejskich,
   c. zakup nowego systemu bądź aktualizacja obecnego systemu informatycznego,
   d. zakup nowych lub modernizacja istniejących systemów ochrony fizycznej (systemy alarmowe, monitoring) jak i systemów bezpieczeństwa IT,
   e. zatrudnienie nowych pracowników,
   f. zmiana lub identyfikacja nowych celów przetwarzania.
3. Już na etapie planowania procesu, Administrator Danych Osobowych bądź wyznaczony przez niego pracownik, zobowiązany jest wdrożyć odpowiednie środki techniczne i organizacyjne zapewniające bezpieczeństwo danych osobowych, a w szczególności zobowiązany jest do stosowania:
   a. pseudonimizacji,
   b. szyfrowania,
   c. minimalizacji danych,
   d. prawidłowości i przejrzystości zbieranych danych,
   e. ograniczenia do niezbędnej ilości zbieranych danych osobowych,
   f. ograniczenia do niezbędnego zakresu przetwarzania danych,

g. ograniczenia do niezbędnego okresu przechowywania danych,
h. technik zapewniających odpowiedni poziom dostępności,

4. Na etapie planowania procesów Administrator Danych Osobowych bądź wyznaczony przez niego pracownik zobowiązany jest również:
   a. rozważyć na jakiej przesłance legalności zostanie oparty proces przetwarzania danych, przy czym, jeśli będzie to zgoda, należy przygotować odpowiednio wcześniej jej treść oraz ustalić sposób jej zbierania i odwołania,
   b. opracować treść oraz sposób realizacji obowiązku informacyjnego,
   c. poinformować Inspektora Ochrony Danych o wszystkich planowanych przedsięwzięciach oraz umożliwić mu podjęcie wszelkich koniecznych działań niezbędnych do zapewnienia bezpieczeństwa przetwarzania danych osobowych,
   d. przy wyborze kontrahenta, partnera biznesowego, kooperanta rozważyć, który z nich w najpełniejszy sposób realizuje zasadę bezpiecznego przetwarzania danych osobowych,
   e. przy wyborze nowego systemu informatycznego, systemu ochrony bądź wprowadzaniu zmian technologicznych kierować się również zapewnieniami producenta dotyczącymi bezpieczeństwa przetwarzania danych osobowych oraz dostosowaniu do wymogów RODO.

Administrator Danych Osobowych świadomy jest, że zasada ochrony danych w fazie projektowania nie ogranicza się jedynie do procesu planowania, gdyż z przepisów RODO jasno wynika, że ocena zgodności z przepisami dotyczy również etapu realizacji procesu. Wobec powyższego ADO wprowadza zasadę regularnego przeglądu funkcjonowania procesów przetwarzania danych oraz jego elementów składowych poprzez:

1. Audyty systemu informatycznego (uwzględniającego zasady cyberbezpieczeństwa, jak i adekwatności przetwarzanych w systemach danych osobowych).
2. Sprawdzenie poprawności metod zbierania i przechowywania zgód na przetwarzanie danych osobowych (w tym zasadność ich zbierania, możliwość ich wycofania oraz treści samej zgody).
3. Sprawdzenie realizacji wypełniania obowiązków informacyjnych.
4. Audyty procesów przetwarzania danych osobowych pod względem adekwatności ich przetwarzania oraz ograniczenia do niezbędnej ilości zbieranych danych. W tym celu Administrator Danych Osobowych zobowiązuje:
   a. pracowników odpowiedzialnych za realizację postępowań o udzielenie zamówienia publicznego do przeglądu wszystkich aktualnie prowadzonych postępowań i dostosowanie treści ich ogłoszeń zgodnie z nowymi regulacjami dotyczącymi ochrony danych osobowych, poprzez umieszczenie stosownych klauzul informacyjnych dla zmawiającego oraz oświadczeń wymaganych od wykonawcy,
   b. pracowników odpowiedzialnych za umieszczenie informacji publicznych na stronie Biuletynu Informacji Publicznej (BIP) zobowiązuje do przeglądu umieszczanych na stronie treści pod kątem prawidłowej anonimizacji umieszczanych danych
   c. administrator zobowiązuje pracownika odpowiedzialnego za umieszczanie informacji publicznych na stronie BIP-u do czuwania nad aktualizacją umieszczanych tam treści.
   d. pracowników odpowiedzialnych za prowadzenie rekrutacji zobowiązuje do przestrzegania procedury rekrutacyjnej określonej w niniejszej Polityce Bezpieczeństwa Danych Osobowych,

e. pracowników do wykonywania cyklicznej inwentaryzacji zasobów poczty służbowej i usuwania wiadomości, które utraciły znaczenia dla wypełniania obowiązków służbowych.

17.2. STRATEGIA OCHRONY DANYCH W FAZIE DOMYŚLNEJ

Realizując zasadę ochrony prywatności i bezpieczeństwa jako właściwości domyślnych *(privacy by default),* Administrator Danych Osobowych bądź pracownik nadzorujący pracę systemu informatycznego zobowiązany jest do:

1. konfiguracji systemu informatycznego w taki sposób, aby od momentu jego uruchomienia system zapewniał odpowiedni poziom ochrony według ustawień domyślnych;
2. konfiguracja systemu informatycznego powinna zapewniać:
   a. aby system nie pozwalał na zbieranie nadmiernej ilości danych osobowych,
   b. aby system wskazywał bądź umożliwiał wprowadzenie informacji dotyczących okresu przechowywania danych,
   c. aby system umożliwiał dostęp do danych jedynie upoważnionym w danym zakresie pracownikom;
3. wprowadzenia zakazu dokonywania jakichkolwiek samodzielnych zmian przez pracowników w ustawieniach fabrycznych komputerów oraz w ustawieniach systemu informatycznego.

18. PROCEDURA SZACOWANIA RYZYKA DLA DANYCH OSOBOWYCH I OCENY SKUTKÓW

Nadzór:	ADO, IOD
Stosowanie:	ASI, pracownicy zaangażowani w proces podlegający analizie

Celem przeprowadzenia oceny ryzyka jest:

1. zapewnienie zdolności do ciągłego zapewnienia poufności, integralności i dostępności systemów i usług przetwarzania danych osobowych,
2. definiowanie i wdrożenie odpowiednich środków technicznych i organizacyjnych, zapewniających adekwatny stopień bezpieczeństwa odpowiadający ryzyku,
3. dokonanie oceny, czy stopień bezpieczeństwa jest odpowiedni, z uwzględnieniem ryzyka wiążącego się z przetwarzaniem danych osobowych, w szczególności wynikającym z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do przetwarzanych danych osobowych.

Na każdym etapie zarządzania ryzykiem ochrony danych osobowych odpowiedzialni za prawidłowy proces są:

1. Administrator Danych Osobowych;
2. Inspektor Ochrony Danych lub inna osoba wyznaczona przez ADO jako odpowiedzialna za nadzór nad ochroną danych osobowych;

3. właściciel procesu odpowiedzialny za realizację czynności przetwarzania (np. pracownik wdrażający nowe rozwiązanie);
4. inne podmioty przetwarzające dane osobowe w imieniu i na zlecenie Administratora Danych Osobowych (jeżeli zachodzi taka konieczność).

W sytuacjach budzących wątpliwości lub wymagającej wiedzy na poziomie eksperckim, ADO wspiera proces zarządzania ryzykiem poprzez pozyskiwanie opinii ekspertów, w szczególności opinii prawnych lub dotyczących kwestii środków zabezpieczających dane (sfera techniczno-organizacyjna).

18.1. IDENTYFIKACJA I KLASYFIKACJA AKTYWÓW ORGANIZACJI

Aktywa oznaczają każdy element, który ma dla organizacji wartość. Mogą to być pracownicy, sprzęt, ale także procesy biznesowe, klienci czy też mechanizmy działania w ramach organizacji.

Zarządzanie aktywami, jest realizowane w celu zapewnienia wymaganego poziomu bezpieczeństwa ochrony danych osobowych.

Należy zidentyfikować i sklasyfikować wszystkie aktywa organizacji, które wiążą się z przetwarzaniem danych osobowych. Aktywa są określane w oparciu o funkcjonujące w organizacji dokumenty, np. rejestr czynności przetwarzania danych (RCPD), schemat organizacyjny oraz wiedzę posiadaną przez administratora.

Aktywa są chronione ze względu na wymagania wynikające zarówno z przepisów prawa oraz regulacji wewnętrznych, z których wynika ochrona właściwych aktywów, a także z zasad bezpieczeństwa wymaganych przez organizację, postanowień umów pomiędzy organizacją, a podmiotami zewnętrznym czy z warunków licencji.

18.2. ZASADY ZARZĄDZANIA AKTYWAMI

Zarządzanie aktywami w organizacji odbywa się zgodnie z poniższymi zasadami:

1. Ustalenie odpowiedzialności za aktywa: należy określić właścicieli wszystkich aktywów oraz przydzieloną im odpowiedzialność za utrzymanie odpowiednich zabezpieczeń. Wdrożenie określonych zabezpieczeń może być delegowane przez właściciela aktywów, jednak pozostaje on nadal odpowiedzialny za adekwatną ochronę aktywów.
2. Identyfikacja aktywów oraz określenie ich wartości: w wyniku identyfikacji sporządza się listę aktywów istotnych z punktu widzenia zarządzania ryzykiem oraz listę procesów biznesowych, w których aktywa te są wykorzystywane. Kolejnym istotnym krokiem podczas identyfikacji aktywów jest określenie ich wartości.
3. Określenie akceptowalnego użycia aktywów: należy określić, a następnie wdrożyć zasady dopuszczalnego korzystania z aktywów i zasobów związanych z przetwarzaniem danych osobowych.
4. Klasyfikacji aktywów (szczegółowy opis stosowanych zabezpieczeń): określona jest metoda oraz sposób klasyfikacji aktywów odzwierciedlający wymagania ich ochrony na odpowiednim poziomie.
5. Oznaczania aktywów: stosowane są regulacje wewnętrzne wyznaczające zasady oznaczanie aktywów informacji i postępowania z nimi.

18.3. SZACOWANIE RYZYKA

1. Szacowanie ryzyka ma na celu określenie, co może się zdarzyć (kiedy, gdzie, jak i dlaczego) i jak dotkliwe straty mogą powstać. W ramach tego działania dla zidentyfikowanych procesów przetwarzania danych i występujących tam aktywów należy wskazać, przeanalizować i oszacować:
   a. występujące zagrożenia dla bezpieczeństwa przetwarzanych danych,
   b. zastosowane środki bezpieczeństwa,
   c. podatność przyjętych rozwiązań z uwzględnieniem zastosowanych środków bezpieczeństwa na urzeczywistnienie się zidentyfikowanych zagrożeń,
   d. potencjalne następstwa w przypadku zaistnienia określonych zagrożeń.
2. Proces zarządzania ryzykiem w bezpieczeństwie informacji realizuje się zgodnie z wytycznymi normy PN-ISO/IEC 27005:2014.
   a. Wszyscy pracownicy podczas realizacji zadań biorą pod uwagę ryzyka związane z bezpieczeństwem przetwarzania danych.
3. Zadania Inspektora Ochrony Danych oraz Administratora Systemu Informatycznego:
   a. przygotowanie procedury szacowania ryzyka,
   b. przygotowanie wykazu aktywów organizacji wraz z ich klasyfikacją,
   c. przeprowadzenie analizy szacowania ryzyka i przygotowanie raportu (wyników) szacowania ryzyka w Rejestrze ryzyka,
   d. przygotowanie planu postępowania z ryzykami,
   e. ewentualne konsultowanie oceny skutków i wsparcie ADO w jej wykonaniu.
4. Zadania Administratora Danych Osobowych:
   a. zatwierdzenie wykazu aktywów organizacji (informacyjnych),
   b. zatwierdzenie rejestru ryzyka organizacji,
   c. zatwierdzenie planów postępowania z ryzykami,
   d. przeprowadzenie i zatwierdzenie oceny skutków (jeżeli została wykonana).

18.4. METODOLOGIA PROCESU ANALIZY RYZYKA

Szczegółowa metodologia procesu analizy i szacowania ryzyka stanowi załącznik do niniejszej Polityki Bezpieczeństwa Danych Osobowych.

18.5. OCENA SKUTKÓW DLA OCHRONY DANYCH

Przepisy ogólnego rozporządzenia o ochronie danych nie wymagają przeprowadzenia oceny skutków dla ochrony danych w odniesieniu do każdej operacji przetwarzania, która może powodować ryzyko naruszenia praw i wolności osób, których dane dotyczą. Przeprowadzenie oceny skutków dla ochrony danych jest obowiązkowe wyłącznie w przypadku, gdy przetwarzanie *„może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych" (zgodnie z art. 35 ust. 1, 3 i 4 RODO).*

Przeprowadzenie oceny skutków dla ochrony danych jest wymagane zawsze wtedy, gdy:

1. dany rodzaj przetwarzania został wskazany w przepisie prawa. Przykładem takiego przepisu jest art. 35 ust. 3 RODO, zgodnie z którym przeprowadzenie oceny skutków dla ochrony danych wymagane jest w przypadku:
   a. systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   b. przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10 RODO;
   c. systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie;
2. dany rodzaj przetwarzania został wskazany w wykazie podanym do publicznej wiadomości przez krajowy organ nadzorczy, zgodnie z art. 35 ust.4 RODO;
3. poziom ryzyka określony został jako wysoki w wyniku jego szacowania przy uwzględnieniu charakteru, zakresu, kontekstu i celów przetwarzania.

Aby poprawić przestrzeganie rozporządzenia, gdy operacje przetwarzania mogą wiązać się z wysokim ryzykiem naruszenia praw lub wolności osób fizycznych, należy zobowiązać Administratora Danych Osobowych do dokonania oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi tego ryzyka. Wyniki oceny należy uwzględnić przy określaniu odpowiednich środków, które należy zastosować, by wykazać, że przetwarzanie danych osobowych odbywa się zgodnie z niniejszym rozporządzeniem. Jeżeli ocena skutków dla ochrony danych wykaże, że operacje przetwarzania powodują wysokie ryzyko, którego administrator nie może zminimalizować odpowiednimi środkami z punktu widzenia dostępnej technologii i kosztów wdrożenia, przed przetwarzaniem **należy skonsultować się z organem nadzorczym.**

Ocenę skutków dla ochrony danych należy wypełnić w fazie projektowania zmiany/projektu!

Ocenę skutków przeprowadza się w sytuacji, np.:

- powierzenia przetwarzania danych innym podmiotom,
- wprowadzenia nowego systemu informatycznego/monitoringu,
- powstanie nowej bazy danych/mikro usługi,
- przekazanie danych do hurtowni danych lub innych wewnętrznych systemów,
- zastosowanie nowej technologii,
- przetwarzanie istniejących danych w nowym celu lub gdy dochodzi do profilowania podmiotu danych,
- udostępnienia danych innym podmiotom.

Zgodnie z art. 35 ust. 7 RODO ocena skutków powinna zawierać:

a. systematyczny opis operacji przetwarzania i celów przetwarzania, który polega na określeniu charakteru, kontekstu, celów przetwarzania, aktywów pomocniczych z uwzględnieniem zatwierdzonych kodeksów postępowania dla każdego procesu,
b. ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
c. ocenę czy operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów.

Ostatnim etapem składającym się na ocenę skutków jest wskazanie przykładowych środków, które mogą pomóc w zarządzaniu ryzykiem (środki organizacyjne i techniczne).

19. PROCEDURA REKRUTACYJNA

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Proces rekrutacji w organizacji ściśle wiąże się z przetwarzaniem danych osobowych kandydatów do pracy zawartych w aplikacji oraz pozyskanych w czasie rozmowy kwalifikacyjnej.

Celem niniejszej procedury jest określenie zasad gwarantujących bezpieczeństwo przetwarzanych danych, zachowanie w poufności procesu rekrutacji oraz poszanowanie prawa do prywatności kandydatów.

Wprowadza się następujące zasady przy prowadzeniu rekrutacji:

1. Administrator Danych Osobowych (lub pracownik odpowiedzialny za rekrutację) zamieszczając ogłoszenie rekrutacyjne zobowiązany jest do zawarcia w jego treści informacji dotyczącej przetwarzania danych osobowych kandydata oraz do poinformowania o możliwości złożenia dobrowolnych oświadczeń tj.:
   a. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych zawartych w CV, liście motywacyjnym lub innych załączonych dokumentach (jeśli przekazane dane obejmują szczególne kategorie danych, bądź wykraczają poza dane, o których mowa w art. 22 k.p.),
   b. oświadczenia o wyrażeniu zgody na przetwarzanie danych osobowych w celu wykorzystania ich w kolejnych rekrutacjach prowadzonych przez organizację - o ile w danym przypadku Administrator Danych Osobowych zdecyduje o woli pozostawienia dokumentów rekrutacyjnych osób niewybranych na potrzeby przyszłych rekrutacji.
2. W przypadku braku zawarcia w dokumentach aplikacyjnych stosownej zgody z punktu 1 lit. a powyżej, pracownik skontaktuje się z kandydatem w celu odebrania stosownego oświadczenia o wyrażeniu zgody.
3. Jeżeli pracownik nie uzyska oświadczenia, zobowiązany jest do usunięcia dokumentów aplikacyjnych w sposób trwały.
4. W przypadku braku zawarcia w dokumentach aplikacyjnych stosownej zgody z punktu 1 lit. b powyżej (o ile Administrator Danych Osobowych żądał takiego oświadczenia w ogłoszeniu) i nie zatrudnienia kandydata, ADO zobowiązany jest po zakończeniu rekrutacji do usunięcia jego dokumentów aplikacyjnych w sposób trwały.
5. Pracownik odpowiedzialny za rekrutację przechowuje dokumenty aplikacyjne w miejscu zabezpieczonym przed dostępem osób nieuprawnionych.
6. W przypadku wymagań wynikających z zapisów odpowiednich przepisów prawa, po zakończeniu procesu rekrutacji dokumenty zawierające dane osobowe kandydatów do pracy są archiwizowane zgodnie z zapisami tych przepisów.
7. Dokumenty aplikacyjne są przechowywane przez okres nie dłuższy niż 9 miesięcy lub zgodnie z udzieloną zgodą kandydata.

20. PROCEDURA SZKOLENIOWA

Nadzór:	ADO, IOD, ASI,
Stosowanie:	wszyscy pracownicy

Wiedza pracowników z zakresu ochrony danych osobowych, to jeden z kluczowych elementów prawidłowego wdrożenia RODO w organizacji. Kompetencje oraz świadomość personelu mają wpływ na zgodność osiąganych wyników pracy z wymaganiami dotyczącymi zapewnienia bezpiecznego przetwarzania danych osobowych. W tym celu Administrator Danych Osobowych zapewnia aby pracownicy mieli możliwość czynnego udziału w szkoleniach z zakresu bezpiecznego przetwarzania danych osobowych.

Celem procedury jest ustalenie zasad i standardów dotyczących organizacji szkoleń z zakresu ochrony danych w organizacji.

20.1. ORGANIZACJA SZKOLEŃ

Planowanie szkoleń

1. Szkolenia związane z podnoszeniem kwalifikacji oraz poszerzania wiedzy w zakresie bezpieczeństwa przetwarzania danych osobowych są traktowane jako jedno z priorytetowych zadań organizacji i obowiązków każdego pracownika.
2. Podstawą planowania szkoleń jest analiza potrzeb szkoleniowych. Analiza potrzeb szkoleniowych to proces oceny i identyfikacji obszarów, w których pracownicy lub organizacja wymagają dodatkowego rozwoju umiejętności, wiedzy lub kompetencji.
3. Plany szkoleń sporządzane są przez Administratora Danych Osobowych na podstawie zaistniałych potrzeb (nowi pracownicy), zgłoszeń zapotrzebowania (np. po wystąpieniu incydentu, naruszenia bezpieczeństwa danych osobowych), a także wyników audytów okresowych i bieżącego monitorowania.
4. Zmiany i uzupełnienia planów szkoleń mogą być wprowadzane na podstawie zgłoszeń pracowników oraz przez Administratora Danych Osobowych.
5. Administrator Danych Osobowych konsultuje plan szkoleniowy z Inspektorem Ochrony Danych, Administratorem Systemów Informatycznych oraz osobą odpowiedzialną za cyberbezpieczeństwo w organizacji.
6. ADO na etapie opracowywania planu szkoleń podejmuje decyzję dotyczącą zasobów ludzkich niezbędnych do przeprowadzenia szkolenia:
   a. przeprowadzenie szkolenia w oparciu o zasoby ludzkie własne;
   b. przeprowadzenie szkolenia przez zewnętrznych trenerów lub specjalistów w zakresie ochrony danych osobowych (w przypadku braku własnych niezbędnych zasobów).
7. Decydując się na skorzystanie z usług zewnętrznego trenera czy firmy szkoleniowej, ADO jako kluczowe elementy oceny potencjalnego usługodawcy wskazuje:
   a. doświadczenie i specjalizacja,
   b. referencje i reputacja,
   c. kwalifikacje trenerów,

d. gotowość dostosowania programu szkoleniowego do potrzeb i specyfiki organizacji,
e. zawartość merytoryczna szkoleń,
f. metodologia szkoleń,
g. stosowane narzędzia szkoleniowe,
h. opcje dostosowania terminów i lokalizacji,
i. wsparcie po szkoleniach,
j. aktualność programów szkoleniowych,
k. koszty i zgodność z budżetem.

8. W przypadku podjęcia decyzji o skorzystaniu z zewnętrznych usług szkoleniowych niezbędne jest oszacowanie kosztów szkolenia oraz uwzględnienie tych kosztów w budżecie organizacji.

Realizacja szkoleń

1. Szkolenia przeprowadzane są zgodnie z ustalonym harmonogramem,
2. Szkolenia odbywają się w siedzibie Administratora Danych Osobowych lub innym wyznaczonym przez niego miejscu, po uprzednim uzgodnieniu terminu oraz miejsca szkolenia.
3. Szkolenia mogą być realizowane w formacie zdalnym, z wykorzystaniem narzędzi, takich jak platformy do tworzenia szkoleń online.
4. ADO bądź pracownik przez niego wyznaczony sporządza listę osób uczestniczących w szkoleniu oraz zawiadamia uczestników o terminie, formie i miejscu szkolenia z niezbędnym wyprzedzeniem.
5. Uczestnikom szkolenia dostarczane są odpowiednie materiały szkoleniowe, narzędzia, czy checklisty, które pomogą w implementacji zdobytej wiedzy w praktyce.
6. Istotnym elementem każdego szkolenia jest jego interaktywność – ADO wymaga, aby w toku każdego szkolenia został zarezerwowany czas, w którym uczestnicy mogą zadawać prowadzącemu pytania.
7. W celu monitorowania postępów uczestników oraz weryfikacji skuteczności szkoleń, w ramach każdego szkolenia przeprowadzany jest pre test wiedzy oraz post test.

Rodzaje szkoleń

1. W organizacji prowadzone są szkolenia wstępne dla nowych pracowników, szkolenia okresowe, przeprowadzane cyklicznie dla wszystkich pracowników oraz szkolenia ad hoc.

20.2. Szkolenie wstępne

Szkolenie wstępne dla nowo przyjętych pracowników organizacji, odbywa się przed udostępnieniem stanowiska pracy i przeprowadzane jest przez Inspektora Ochrony Danych lub Administratora Ochrony Danych bądź osobę przez niego wskazaną, posiadającą niezbędną wiedzę z zakresu ochrony danych osobowych. Tematyka szkolenia wstępnego powinna obejmować m.in.:

1. terminologię z zakresu ochrony danych osobowych,
2. podstawy prawne obowiązywania ochrony danych osobowych,
3. role i odpowiedzialności osób uczestniczących w przetwarzaniu danych osobowych,
4. istniejące zagrożenia bezpieczeństwa danych osobowych,

5. stosowane przez Administratora Danych Osobowych środki zabezpieczenia danych osobowych (środki organizacyjne – wdrożone polityki i procedury; środki techniczne; środki fizyczne) i zasady ochrony stanowiska pracy,
6. procedura naruszenia ochrony danych osobowych, bezpieczeństwa informacji.

20.3. SZKOLENIE OKRESOWE

Szkolenia okresowe prowadzone są **indywidualnie** dla każdej z grup odbiorców i obejmują swoim zakresem kluczowe obszary z punktu widzenia ról, jakie odbiorcy pełnią w procesie budowania bezpieczeństwa danych osobowych w organizacji. W uzasadnionym przypadku ADO może podjąć decyzję o przeprowadzeniu szkolenia dla kilku grup odbiorców razem.

1. Szkolenia okresowe prowadzone są cyklicznie, zgodnie z planem szkoleniem, jednak nie rzadziej niż **jeden raz w ciągu roku.**
2. Poniższe zestawienie prezentuje przykładową tematykę szkoleń dla poszczególnych grup obiorców, która powinna zostać uwzględniona w harmonogramie szkoleń.

Odbiorcy	Zakres szkolenia	Tematyka
Kierownictwo,	Szkolenia skupiają się na zagadnieniach strategicznych oraz aspektach związanych z zarządzania ryzykiem	1. **Akty prawne i regulacje w zakresie bezpieczeństwa danych osobowych** informacje na temat zmian w przepisach prawnych, regulacjach i normach związanych z ochroną danych oraz skutków nieprzestrzegania tych przepisów. 2. **Rola Kierownictwa w budowaniu skutecznego systemu ochrony danych osobowych**: zrozumienie roli i odpowiedzialności najwyższego kierownictwa w kształtowaniu kultury bezpieczeństwa danych osobowych w organizacji; dobre praktyki i najnowsze trendy w obszarze ochrony danych osobowych; 3. **Fundamenty ochrony danych osobowych**: zrozumienie kluczowych zasad decydujących o skutecznym wdrożeniu ochrony danych osobowych w organizacji. 4. **Zarządzanie ryzykiem:** identyfikacja, ocena i zarządzanie ryzykiem związanym z bezpieczeństwem informacji, ze szczególnym uwzględnieniem aspektów finansowych i wizerunkowych. 5. **Reagowanie na incydenty bezpieczeństwa**: rola najwyższego kierownictwa w procesie zarządzania incydentami bezpieczeństwa, obejmujący procesy zgłaszania, analizy i poprawy procedur reagowania na incydenty bezpieczeństwa. 6. **Audyt jako narzędzie doskonalenia systemu ochrony danych osobowych:** zrozumienie istoty i metodologii przeprowadzania audytu ochrony danych oraz procesu przygotowania organizacji do audytu. 7. **Cyberzagrożenia**: świadomość najnowszych zagrożeń cybernetycznych, ataków typu phishing,

		malware'u oraz strategii obronnych na poziomie zarządczym. 8. **Etyka i świadomość bezpieczeństwa**: podkreślenie roli etyki w dziedzinie bezpieczeństwa informacji oraz promowanie świadomości pracowników na temat odpowiedzialnego korzystania z zasobów informacyjnych. 9. **Szkolenie z wybranej procedury** – szkolenie z wybranych procedur zawartych w PBDO, PBSI, PBF;
Osoby odpowiedzialne za bezpieczeństwo systemów informatycznych oraz cyberbezpieczeństwo	Szkolenia dostarczają praktycznych umiejętności, które umożliwią odpowiedzialnym za bezpieczeństwo systemów informatycznych i cyberbezpieczeństwo skuteczne rozpoznanie zagrożeń, reagowanie na incydenty i aktywne uczestnictwo w zarządzaniu ryzykiem.	1. **Podstawy prawne organizacji bezpieczeństwa danych osobowych:** zapoznanie z podstawowymi obowiązującymi przepisami prawa i regulacjami dotyczącymi bezpieczeństwa informacji oraz aspektami związanymi ze zgodnością (compliance) w kontekście systemów informatycznych. 2. **Rola specjalisty IT w budowaniu skutecznego systemu ochrony danych osobowych**: szkolenie z wybranych procedur zawartych w PBDO, PBSI, PBF; 3. **Analiza zagrożeń i reagowanie na incydenty**: skuteczne reagowanie na incydenty, w tym proces analizy zagrożeń, identyfikacji ataku i przywracania systemów do normalnej pracy. 4. **Zabezpieczanie danych**: techniki i dobre praktyki zabezpieczania danych, w tym kwestie związane z szyfrowaniem, zarządzaniem dostępem i kontrolą integralności informacji. 5. **Reagowanie na incydenty bezpieczeństwa**: efektywny udział w procesie zarządzania incydentami bezpieczeństwa, obejmujący procesy zgłaszania, analizy i poprawy procedur reagowania na incydenty bezpieczeństwa. 6. **Audyt Bezpieczeństwa:** zrozumienie istoty i metodologii przeprowadzania audytu bezpieczeństwa systemów informatycznych, w tym audytów wewnętrznych i zewnętrznych oraz proces przygotowania organizacji do audytu. 7. **Budowanie świadomości pracowników**: szkolenie budujące kompetencje dzielenia się wiedzą z zakresu bezpieczeństwa informacji, mające na celu podniesienie świadomości pracowników i zminimalizowanie ryzyka związanego z ludzkim czynnikiem.
Pozostali pracownicy	Szkolenia zwiększają świadomość pracowników i wyposażają ich w praktyczne umiejętności do skutecznego zarządzania informacjami oraz minimalizowania ryzyka związanego z bezpieczeństwem danych osobowych.	1. **Rola pracownika w budowaniu skutecznego systemu ochrony danych osobowych** – szkolenie z wybranych procedur zawartych w PBDO, PBSI, PBF; 2. **Zagrożenia cybernetyczne:** budowanie świadomości najczęstszych zagrożeń cybernetycznych, takich jak phishing, malware, ataki hakerskie i sposoby ich rozpoznawania. 3. **Bezpieczne korzystania z systemów informatycznych**: zasady bezpiecznego korzystania

		z komputerów, laptopów, smartfonów, oraz bezpiecznego korzystania z aplikacji i zasobów internetowych. 4. **Zarządzanie hasłami**: techniki tworzenia silnych haseł, zasady bezpiecznego przechowywania i udostępniania haseł oraz konieczność regularnej zmiany haseł. 5. **Szkolenia anti-phishingowe**: jak rozpoznawać i unikać prób phishingu, a także jak raportować potencjalne incydenty. 6. **Bezpieczeństwo pracy zdalnej::** zasady bezpiecznej pracy zdalnej, korzystania z VPN, zabezpieczania połączeń internetowych i chronienie informacji podczas pracy na odległość 7. **Zarządzanie dokumentacją elektroniczną**: sposoby bezpiecznego przechowywania, udostępniania i usuwania elektronicznych dokumentów, a także zasady archiwizacji. 8. **Media społeczościowe**: zagrożenia związane z korzystaniem z mediów społecznościowych w kontekście bezpieczeństwa informacji oraz zasady ochrony prywatności. 9. **Zabezpieczenia fizyczne:** wskazówki dotyczące bezpiecznego przechowywania dokumentów papierowych oraz zabezpieczeń fizycznych miejsca pracy.

20.4. DOKUMENTOWANIE SZKOLEŃ

Mając na względzie troskę o przejrzystość prowadzonych działań, ADO nakłada obwiązek dokumentowania szkoleń z zakresu bezpieczeństwa danych osobowych w organizacji.

Na dokumentację szkoleń z zakresu ochrony danych osobowych składają się:

1. **podpisana przez uczestników lista obecności na szkoleniu** - lista zawiera co najmniej nazwę organizacji, temat szkolenia, datę przeprowadzenia szkolenia, zakres godzinowy szkolenia, imię i nazwisko prowadzącego oraz podpisy uczestników; prowadzący zobligowany jest przekazać listę Administratorowi Danych Osobowych po zakończeniu szkolenia.
2. **konspekt (program, plan) przeprowadzonego szkolenia,** który prowadzący przekazuje Administratorowi Danych Osobowych po zakończeniu szkolenia.
3. **materiały szkoleniowe** przekazane uczestnikom w celu pogłębienia wiedzy, których kopię prowadzący przekazuje Administratorowi Danych Osobowych po zakończeniu szkolenia (fakultatywnie).
4. **imienne certyfikaty (zaświadczenia) potwierdzające uczestnictwo w szkoleniu** – certyfikat wystawiany jest imiennie każdemu uczestnikowi;
5. **rejestr szkoleń** – Administrator Danych Osobowych zobowiązany jest do wyznaczenia osoby odpowiedzialnej za prowadzenie rejestru szkoleń, w którym odnotowuje się, każde przeprowadzone szkolenie z zakresu ochrony danych osobowych.

21. PROCEDURA MONITORINGU

Nadzór:	ADO, IOD, ASI
Stosowanie:	wszyscy pracownicy

Celem niniejszej procedury jest określenie reguł dotyczących stosowania monitoringu wizyjnego w organizacji, ze szczególnym uwzględnieniem poszanowania prawa do prywatności osób monitorowanych.

21.1. MONITORING WIZYJNY

Zapewniając ochronę wizerunku osób fizycznych objętych monitoringiem stosowanym przez organizację wprowadza się następujące reguły.

1. Administrator Danych Osobowych zapewnia prawidłowe funkcjonowanie monitoringu mając na względzie aby nie naruszał on prawa do prywatności osób fizycznych oraz czuwa, aby przetwarzanie danych odbywało się w granicach prawa.
2. Monitoring wizyjny wykorzystywany jest w celu:
   a. zapewnienia bezpieczeństwa osób przebywających na obszarze monitorowanym (w szczególności uczniów i pracowników);
   b. zapewnienia bezpieczeństwa mienia.
3. Obowiązek informacyjny wobec osób monitorowanych realizowany jest poprzez oznaczenie obszaru objętego systemem monitoringu tabliczką zawierającą piktogram kamery wraz ze skróconym obowiązkiem informacyjnym.
4. Klauzula informacyjna zawierająca pełny obowiązek informacyjny oraz Regulamin monitoringu dostępne są w wersji papierowej w siedzibie Administratora Danych Osobowych oraz w wersji elektronicznej na stronie internetowej organizacji oraz w Biuletynie Informacji Publicznej.
5. Od pracowników odbiera się pisemne oświadczenia o zapoznaniu się zasadami funkcjonowania monitoringu. Wzór oświadczenia stanowi załącznik do PBDO.
6. Przed rozpoczęciem pracy monitoringu wizyjnego Administrator Danych Osobowych (lub wskazana przez niego osoba) dokonuje analizy obszaru, który obejmie system monitoringu wizyjnego upewniając się, iż swoim działaniem nie naruszy on godności oraz innych dóbr osób monitorowanych. Monitoring wizyjny może obejmować jedynie obszar przylegający do organizacji i to w takim zakresie jakim nie narusza on prywatności osób postronnych.
7. Monitoring nie może obejmować pomieszczeń sanitarnych, szatni sportowych, stołówek, palarni oraz pomieszczeń socjalnych.
8. System monitoringu działa całą dobę.
9. Rejestracji i zapisaniu na nośniku fizycznym podlega tylko obraz. System monitoringu nie rejestruje dźwięku.
10. Zapis z monitoringu przechowuje się przez okres 16 dni od dnia nagrania. Po upływie tego terminu dane są automatycznie nadpisywane.

11. W uzasadnionych przypadkach, gdy urządzenia monitoringu wizyjnego zarejestrowały zdarzenie związane z naruszeniem bezpieczeństwa osób i mienia, okres przechowywania danych może ulec wydłużeniu o czas niezbędny do zakończenia postępowania, którego przedmiotem jest zdarzenie zarejestrowane przez monitoring wizyjny.
12. Urządzenie, na którym przechowywane są nagrania (rejestrator) umieszcza się w pomieszczeniu, do którego dostęp mają tylko upoważnione osoby.
13. Dostęp do podglądu z kamer w czasie rzeczywistym ma pracownik upoważniony do tego procesu.
14. Stanowisko komputerowe z monitorem, na którym jest wyświetlany obraz z kamer znajduje się w sekretariacie, a widok z monitora jest niedostępny dla osób postronnych.
15. Zapis z systemu monitoringu może być udostępniony uprawnionym organom w zakresie realizowania przez nie ustawowych zadań np. policji, sądom, prokuraturom na ich pisemny wniosek.
16. Osoba zainteresowana zabezpieczeniem danych z monitoringu zwraca się pisemnie do administratora z prośbą o ich zabezpieczenie przed automatycznym usunięciem. Wniosek musi zawierać informacje takie jak:
    a. dane osoby zgłaszającej,
    b. opis zdarzenia wraz ze wskazaniem przybliżonego czasu i miejsca,
    c. cel wykorzystania nagrania.
17. Pracownik sporządza kopię nagrania z monitoringu wizyjnego za okres, którego dotyczy wniosek osoby zainteresowanej oraz oznacza ją w sposób trwały poprzez:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,
    c. okres, którego dotyczy nagranie,
    d. źródła danych.
18. Nagrania są udostępniane na nośniku elektronicznym w sposób nienaruszający wizerunku osób trzecich widocznych na nagraniu.
19. Kopia nagrania przechowywana jest przez okres 6 miesięcy na Serwerze NAS.
20. Po upływie 6 miesięcy zabezpieczona na wniosek osoby zainteresowanej kopia nagrania podlega zniszczeniu.
21. Kopia nagrania podlega zaewidencjonowaniu w rejestrze kopii z monitoringu wizyjnego.
22. Rejestr zawiera następujące informacje:
    a. numer porządkowy kopii,
    b. datę sporządzenia kopii,
    c. okres, którego dotyczy nagranie,
    d. źródło danych,
    e. informację o udostępnieniu ze wskazaniem daty,
    f. informację o zniszczeniu kopii ze wskazaniem daty.
23. Nośnik z kopią nagrania przekazuje się wnioskodawcy za pokwitowaniem odbioru.

22. PROCEDURA UTRZYMANIA CZYSTOŚCI

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Pomieszczenia, w których znajdują się dane osobowe zarówno w postaci papierowej, jak i elektronicznej, stanowią obszar przetwarzania danych osobowych. Dostęp do tych obszarów powinien być monitorowany w zakresie, w jakim jest on udostępniany osobom sprzątającym. Niezależnie od tego, czy osoby sprzątające pomieszczenia, w których przetwarza się dane osobowe są zatrudnione wewnątrz struktury organizacyjnej administratora, czy są to osoby świadczące usługi z zewnątrz, Administrator Danych Osobowych wprowadza następujące reguły:

1. Wszystkie osoby sprzątające zobowiązane są do zachowania w tajemnicy danych osobowych znajdujących się w obszarze przetwarzania danych osobowych podczas wykonywania czynności.
2. Oświadczenie o zachowaniu w tajemnicy powinno być odbierane przez Administratora Danych Osobowych przed przystąpieniem osoby sprzątającej do wykonywania czynności.
3. Oświadczenie o zachowaniu w tajemnicy danych osobowych może stanowić oddzielny dokument bądź zostać zawarte w treści umowy o pracę bądź innej podstawy świadczenia usług.
4. Przed rozpoczęciem sprzątania pracownicy zobowiązani są stosować się do zasady czystego biurka oraz zasady czystego ekranu oraz umożliwić wejście i rozpoczęcie wykonywanych czynności przez osobę sprzątającą.
5. Osoby sprzątające pomieszczenia, w których przetwarzane są dane osobowe, powinny wykonywać czynności sprzątania pod nadzorem i w obecności upoważnionych pracowników.
6. Administrator Danych Osobowych wprowadza zakaz opuszczania pomieszczeń w których przetwarzane są dane osobowe w trakcie ich sprzątania i pozostawiania nawet na krótką chwilę osób sprzątających bez nadzoru w trakcie wykonywanych przez nią czynności.
7. W przypadkach, gdy w związku ze świadczeniem innego typu usług na rzecz Administratora Danych Osobowych (np. usługi remontowe, serwisowe) istnieje duże prawdopodobieństwo potencjalnego wglądu osób zaangażowanych w dany proces do danych osobowych, zastosowanie mają te same zasady, które dotyczą personelu zajmującego się utrzymaniem czystości.

23. PROCEDURA ARCHIWIZACJI DOKUMENTÓW ZAWIERAJĄCYCH DANE OSOBOWE

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Celem procedury jest określenie zasad i sposobu archiwizacji dokumentów związanych z funkcjonowaniem organizacji.

1. Administrator Danych Osobowych wyznacza pomieszczenie przeznaczone na archiwum zakładowe.

2. Pomieszczenie archiwum, stanowi obszar przetwarzania danych osobowych i jest pomieszczeniem szczególnie chronionym w organizacji.
3. Dostęp do pomieszczenia archiwum mają wyłącznie osoby upoważnione.
4. Pomieszczenie archiwum wyposażone jest w środki bezpieczeństwa fizycznego podnoszące bezpieczeństwo przechowywanych tam dokumentów przynajmniej o jeden poziom wyżej, niż pozostałe pomieszczenia będące obszarem przetwarzania.
5. Zastosowano następujące środki bezpieczeństwa fizycznego:
   a. pomieszczenie znajduje się na innej kondygnacji niż 0,
   b. pomieszczenie bez okna,
   c. pomieszczenie, w oknach którego znajduje się krata lub roleta antywłamaniowa,
   d. pomieszczenie, do którego zastosowano drzwi antywłamaniowe i ogniotrwałe,
   e. pomieszczenie archiwum wyposażono w higrometr i termometr.
6. Administrator Danych Osobowych lub wyznaczony pracownik odpowiada za przeprowadzenie archiwizowania dokumentacji w przyjętych ramach czasowych.
7. Dokumenty podlegające archiwizacji umieszczane są w opisanych segregatorach lub teczkach.
8. Zabrania się umieszczania dokumentacji bezpośrednio na podłodze.
9. Po zakończeniu wymaganych okresów przechowywania (retencji), dokumenty należy poddać procedurze brakowania.

24. PROCEDURA NISZCZENIA DOKUMENTÓW NIEPODLEGAJĄCYCH PROCEDURZE ARCHIWIZACJI

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Zniszczenie danych osobowych oznacza fizyczną utylizację nośnika, na którym dane się znajdują oraz uniemożliwienie ich ponownego odtworzenia.

Celem niniejszej procedury jest określenie zasad postępowania w przypadku niszczenia dokumentów zawierających dane osobowe w sposób bezpieczny dla ich poufności.

1. Dokumenty przeznaczone do zniszczenia przechowywane są w wydzielonym i zabezpieczonym miejscu i niszczone w możliwie najkrótszym możliwym terminie.
2. Pracownik niszczy dokumentację papierową samodzielnie.
3. Dokumenty papierowe zawierające dane osobowe, niszczone są w niszczarce, w sposób uniemożliwiający ich powtórne odczytanie.
4. W przypadku korzystania z usług zewnętrznego podmiotu świadczącego usługę niszczenia dokumentów niezbędne jest uprzednie zawarcie umowy powierzenia danych osobowych lub wprowadzenie zapisów dotyczących powierzenia przetwarzania danych do samej umowy serwisowej.

5. Administrator Danych Osobowych lub wyznaczony pracownik zobowiązany jest do odebrania protokołu potwierdzającego odbiór i zniszczenie dokumentów, wystawionego przez podmiot zewnętrzny.

25. PROCEDURA PROWADZENIA BIULETYNU INFORMACJI PUBLICZNEJ

Nadzór:	ADO, IOD, osoba nadzorująca pracę redaktorów BIP
Stosowanie:	redaktorzy Biuletynu Informacji Publicznej

Celem procedury jest określenie zasad prowadzenia Biuletynu Informacji Publicznej, w związku z publikacją na jego stronach danych osobowych.

1. Osoba wskazana do prowadzenia BIP posiada pisemne upoważnienie do przetwarzania danych osobowych.
2. Redaktorzy BIP posiadają formalnie wyznaczonych zastępców.
3. W związku z obowiązkami wynikającymi z przepisów prawa, strona Biuletynu Informacji Publicznej w zakładce „Informacje o biuletynie" zawiera imiona i nazwiska oraz adresy e-mail redaktorów i numer telefonu przynajmniej jednej osoby redagującej stronę główną BIP.
4. Na stronie biuletynu zamieszczono Instrukcje korzystania z BIP, a także adres redakcyjny strony głównej.
5. Celem przetwarzania danych w procesie prowadzenia Biuletynu Informacji Publicznej jest realizacja obowiązku prawnego ciążącego na podmiotach publicznych (powszechne udostępnianie informacji publicznej, w postaci ujednoliconego systemu stron w sieci teleinformatycznej). Podstawą prawną przetwarzania danych wynikającą z RODO jest art. 6 ust. 1 lit c, czyli wypełnienie obowiązku prawnego w związku z Ustawą z dnia 6 września 2001 r. o dostępie do informacji publicznej, Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 18 stycznia 2007 r. w sprawie Biuletynu Informacji publicznej oraz Komunikat nr 23 Ministra Finansów z dnia 16 grudnia 2009 r. w sprawie standardów kontroli zarządczej dla sektora finansów publicznych.
6. Na stronach Biuletynu Informacji Publicznej przetwarzane mogą być dane następującej kategorii osób: uczestnicy zajęć lub wydarzeń kulturalnych, rodzice, opiekunowie prawni, pracownicy, kandydaci do pracy, stażyści, praktykanci, kontrahenci, oferenci, przedstawiciele jednostek kontrolujących, osoby składające petycje, osoby prowadzące działalność regulowaną, uczestnicy zamówień publicznych, najemcy, w odniesieniu do wskazanych kategorii osób w procesie przetwarzane są dane wyłącznie kategorii zwykłej.
7. Treść ogłoszenia przeznaczonego do publikacji na BIP opracowują i publikują redaktorzy.
8. Przygotowywania informacji do publikacji odbywa się z uwzględnieniem zasady minimalizacji danych oraz poufności danych (zasady anonimizacji danych).
9. Organizacja wypełnia obowiązki wynikające z art. 8 ust. 6 ustawy o dostępie do informacji publicznej w zakresie oznaczenia informacji danymi określającymi podmiot udostępniający informację, zabezpieczenia możliwości identyfikacji czasu rzeczywistego udostępnienia informacji, podania w informacji danych określających tożsamość osoby, która wytworzyła informację lub odpowiada za treść informacji, dołączenia do informacji danych określających tożsamość osoby, która wprowadziła informację do Biuletynu Informacji Publicznej.

10. Pracownicy biorący udział w procesie przechodzą regularne szkolenia z zakresu ochrony danych osobowych.
11. Organizacja tworzy kopie zapasowe danych publikowanych na BIP.

25.1. Procedura publikacji danych w BIP i ustalania okresu retencji danych

1. Osoba przygotowująca informację przeznaczoną do opublikowania w BIP sprawdza, czy informacja zawiera dane osobowe.
2. Jeżeli informacja nie zawiera danych osobowych, pracownik przekazuje jej treść do publikacji redaktorowi BIP.
3. Jeżeli informacja zawiera dane osobowe:
   a. pracownik sprawdza zgodność z obowiązującymi przepisami prawa, aby ustalić, czy zgodnie z tymi przepisami istnieje wymóg ujawnienia danych osobowych w treści informacji;
   b. pracownik sprawdza zgodność zakresu danych osobowych podanych w informacji z tym, co określają obowiązujące przepisy. W przypadku różnic, pracownik dokonuje stosownych korekt, zwłaszcza jeśli chodzi o ograniczenie zakresu danych;
   c. na podstawie przepisów prawa oraz w zgodzie z jednolitym rzeczowym wykazem akt obowiązującym w jednostce, pracownik ustala okres publikowania informacji w Biuletynie Informacji Publicznej (BIP);
   d. pracownik przekazuje jej treść (wraz ze wskazaniem podstawy prawnej oraz ustalonego okresu retencji) do Inspektora Ochrony Danych celem sprawdzenia zgodności z przepisami o ochronie danych osobowych.
4. Inspektor Ochrony Danych weryfikuje zgodność informacji z przepisami, a następnie nanosi uwagi lub przekazuje informację do akceptacji Administratora Danych Osobowych, a następnie po uzyskaniu akceptacji do publikacji.
5. Publikacji informacji dokonują redaktorzy.
6. Za usunięcie informacji po upływie okresu retencji danych odpowiada osoba nadzorująca prowadzenie BIP oraz redaktorzy BIP.

25.2. Procedura przeprowadzania okresowych przeglądów BIP

1. Okresowy przegląd danych publikowanych w BIP przeprowadzany jest cyklicznie, raz do roku w terminie ustalonym przez ADO.
2. Za dokonywanie przeglądów odpowiedzialni są:
   a. zespół redakcyjny BIP – osoba nadzorująca prowadzenie BIP oraz redaktorzy BIP;
   b. Inspektor Ochrony Danych;
   c. inne osoby indywidualnie wyznaczone przez ADO.
3. Przegląd obejmuje wszystkie treści opublikowane w BIP, w szczególności pod katem:
   a. zakresu udostępnionych danych;
   b. okresu retencji (z uwzględnieniem wymogów wynikających z przepisów prawa oraz jednolitego rzeczowego wykazu akt oraz ustalania lub nie celu przetwarzania).

4. Z okresowego przeglądu BIP sporządzany jest raport, pod którym podpisują się wszystkie osoby, które dokonały przeglądu.
5. Raport przedkładany jest Administratorowi Danych Osobowych, który zatwierdza wynik przeglądu oraz podejmuje decyzje, co do działań niezbędnych do podjęcia.

26. PROCEDURA POSTĘPOWANIA W SYTUACJI NARUSZENIA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Nadzór:	ADO, IOD
Stosowanie:	ASI, wszyscy pracownicy

Celem procedury jest określenie zasad postępowania w przypadku naruszenia bezpieczeństwa danych osobowych przetwarzanych zarówno tradycyjnie, w wersji papierowej, jak również w wersji elektronicznej. Niniejsza procedura zapewnia, że zdarzenia związane z bezpieczeństwem danych oraz zagrożenia związane z funkcjonowaniem systemu informatycznego, zgłaszane są w sposób umożliwiający niezwłoczne podjęcie działań naprawczych oraz eliminację negatywnych skutków związanych z zaistniałym incydentem.

Zasady postępowania w przypadku naruszenia ochrony danych osobowych obowiązują wszystkie osoby biorące udział w procesie przetwarzania danych.

Reakcja na incydent zależy od jego istotności, mierzonej skutkami i poziomem oddziaływania na organizację lub na osoby, których dane osobowe były objęte incydentem.

Osoby stwierdzające naruszenie zasad ochrony lub zdarzenie, które mogło skutkować takim naruszeniem, zobowiązane są do przestrzegania oraz postępowania według opracowanej i wdrożonej procedury postępowania w sytuacji naruszenia ochrony danych osobowych.

26.1. ISTOTA NARUSZENIA OCHRONY DANYCH OSOBOWYCH

Naruszenie ochrony danych osobowych oznacza naruszenie bezpieczeństwa prowadzące do:

a. "naruszenia poufności" – polegającego na nieuprawnionym lub przypadkowym ujawnieniu lub udostępnieniu danych osobowych,
b. "naruszenia integralności" – polegającego na nieuprawnionym lub przypadkowym zmodyfikowaniu danych osobowych,
c. "naruszenia dostępności" – polegającego na przypadkowej lub nieuprawnionej utracie dostępu do danych osobowych lub ich zniszczeniu.

Naruszeniem danych osobowych jest przede wszystkim każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną czy uszkodzenia jakiegokolwiek elementu systemu informatycznego.

Obowiązek zgłoszenia jest wymagany, przede wszystkim w sytuacji, gdy naruszenie polegało na:

1. Zagubieniu lub kradzieży nośnika/urządzenia.
2. Zagubieniu, kradzieży lub pozostawieniu w niebezpiecznej lokalizacji dokumentacji papierowej zawierającej dane osobowe.
3. Utracie korespondencji papierowej przez operatora pocztowego lub otwarcie przed zwróceniem jej do nadawcy.
4. Nieuprawnionemu uzyskaniu dostępu do informacji.
5. Nieuprawnionym uzyskaniu dostępu do informacji poprzez złamanie zabezpieczeń.
6. Ingerencji złośliwego oprogramowania ingerującego w poufność, integralność i dostępność danych.
7. Uzyskaniu poufnych informacji przez pozornie zaufaną osobę w oficjalnej komunikacji elektronicznej, takiej jak e-mail, czy też inny komunikator internetowy.
8. Nieprawidłowej anonimizacji danych osobowych w dokumencie.
9. Nieprawidłowym usunięciu/zniszczeniu danych osobowych z nośnika/ urządzenia elektronicznego przed jego zbyciem przez Administratora Danych Osobowych.
10. Niezamierzonej publikacji.
11. Przesłaniu danych osobowych do niewłaściwego odbiorcy.
12. Ujawnieniu danych niewłaściwej osobie.
13. Ustnym ujawnieniu danych osobowych.

26.2. POSTĘPOWANIE W PRZYPADKU NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.
2. W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz powiadomić odpowiednie organy/służby ochrony oraz bezpośredniego przełożonego.
3. Z każdego zdarzenia pracownik sporządza notatkę i przekazuje ją Administratorowi Danych Osobowych. W notatce należy ująć:
   a. datę i miejsce stwierdzenia naruszenia,
   b. sposób stwierdzenia naruszenia (opis sytuacji),
   c. podjęte działania (wykonane czynności po wykryciu naruszenia),
   d. wskazanie osób poinformowanych o zaistniałym incydencie,
   e. czytelny podpis osoby sporządzającej notatkę.
4. Po przedłożeniu notatki z naruszenia Administrator Danych Osobowych lub wyznaczona przez niego osoba informuje Inspektora Ochrony Danych o zaistniałym zdarzeniu oraz dokonuje jego analizy.
5. W przypadku zakwalifikowania zdarzenia jako naruszenie ochrony danych osobowych, Administrator Danych Osobowych lub osoba przez niego wyznaczona dokonuje oceny istotności naruszenia.
6. Przy ocenie istotności incydentu pod uwagę brane są następujące czynniki:

a. charakter naruszenia ochrony danych osobowych (naruszenie poufności, integralności, dostępności),
b. klasyfikacja naruszenia (na czym polegało naruszenie),
c. przyczyny naruszenia (wewnętrzne działanie niezamierzone/zamierzone, zewnętrzne działanie niezamierzone/zamierzone),
d. kategorie danych osobowych i przybliżoną liczbę osób, których dane dotyczą,
e. kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie,
f. środki bezpieczeństwa zastosowane przed naruszeniem,
g. możliwe konsekwencje naruszenia ochrony danych osobowych (naruszenie praw lub wolności osób fizycznych),
h. wpływ incydentu na ciągłość działania organizacji,
i. koszty usunięcia skutków incydentu,
j. szacowany czas naprawy skutków wywołanych incydentem.

7. Ocena istotności naruszenia prowadzi do zakwalifikowania incydentu według przyjętej skali:
   a. pomijalne,
   b. niskie,
   c. akceptowalne,
   d. wysokie,
   e. maksymalne.
8. W celu dokonania zgłoszenia Administrator Danych Osobowych stosuje formularz udostępniony przez Urząd Ochrony Danych Osobowych.
9. Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport.
10. Zgłoszenie incydentu rejestrowane jest przez Administratora Danych Osobowych lub wyznaczoną przez niego osobę w rejestrze incydentów. Wzór rejestru incydentów stanowi załącznik do niniejszej PBDO.
11. Załącznikiem do niniejszej PBDO jest skrócona instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych dla pracowników.

26.3. KONSEKWENCJE ZANIECHANIA ZGŁOSZENIA NARUSZENIA OCHRONY DANYCH

1. Wobec pracownika, który w przypadku naruszenia danych osobowych nie podjął działania określonego w niniejszym dokumencie, a w szczególności nie powiadomił Administratora Danych Osobowych lub odpowiedniej osoby, zgodnie z określonymi zasadami może zostać wszczęte postępowanie dyscyplinarne lub porządkowe.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych.
3. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia Administratora Danych Osobowych o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej oraz cywilnej zgodnie z obowiązującymi przepisami.

26.4. UDOKUMENTOWANIE SKUTKÓW ORAZ PODJĘTYCH ŚRODKÓW I DZIAŁAŃ

Pracownik, który stwierdził fakt lub uzyskał informację o naruszeniu bezpieczeństwa danych osobowych jest obowiązany niezwłocznie powiadomić Administratora Danych Osobowych i/lub Inspektora Ochrony Danych oraz osobę nadzorującą system informatyczny. ADO lub osoba przez niego wyznaczona mają obowiązek:

1. Wygenerować i wydrukować wszystkie dokumenty i raporty, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzyć je datą i godziną oraz podpisać.
2. Przystąpić do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym określić skalę zniszczeń, metody dostępu osoby nieuprawnionej do danych osobowych w systemie informatycznym służącym do przetwarzania danych osobowych.
3. Podjąć odpowiednie kroki w celu powstrzymania lub ograniczenia dostępu osoby nieuprawnionej do danych osobowych, zminimalizować szkody i zabezpieczyć przed usunięciem śladów naruszenia ochrony, w szczególności poprzez:
   a. fizyczne odłączenie urządzeń i segmentów sieci, które mogły umożliwić dostęp do danych osobowych osobie nieuprawnionej,
   b. wylogowanie użytkownika podejrzanego o naruszenie ochrony danych osobowych,
   c. zmianę hasła użytkownika, przez konto którego uzyskano nielegalny dostęp do danych osobowych w celu uniknięcia ponownej próby uzyskania takiego dostępu.
4. Dokonać szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia bezpieczeństwa danych osobowych.
5. Przywrócić prawidłowe działanie systemu informatycznego służącego przetwarzaniu danych osobowych.
6. Po przywróceniu prawidłowego stanu, należy przeprowadzić szczegółową analizę, w celu określenia przyczyn naruszenia ochrony danych osobowych lub podejrzenia takiego naruszenia oraz podjąć kroki, mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.
7. Jeżeli przyczyną zdarzenia był błąd pracownika, należy przeprowadzić szkolenie dotyczące bezpieczeństwa przetwarzania danych osobowych w organizacji.
8. Jeżeli przyczyną zdarzenia była infekcja wirusem lub innym szkodliwym oprogramowaniem, należy ustalić źródło jego pochodzenia i utworzyć zabezpieczenia antywirusowe oraz organizacyjne, wykluczające podobne zdarzenia w przyszłości.

26.5. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

1. W przypadku naruszenia ochrony danych osobowych, Administrator Danych Osobowych bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych, 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 dołącza się wyjaśnienie przyczyn opóźnienia.
2. 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 Danych Osobowych w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator Danych Osobowych dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu na zweryfikowanie przestrzegania niniejszego artykułu.

26.6. Zawiadomienie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki powiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:
   a. Administrator Danych Osobowych wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym tych danych osobowych,
   b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1,
   c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

27. Procedura rozpatrywania skarg przez Administratora Danych Osobowych

Nadzór:	ADO
Stosowanie:	wszyscy pracownicy

Celem niniejszej procedury jest ustalenie zasad postępowania w sytuacji zarejestrowania skargi z tytułu naruszenia ochrony danych osobowych.

1. Po otrzymaniu zgłoszenia od osoby, której dane dotyczą, ADO lub wyznaczona przez niego osoba niezwłocznie, w miarę możliwości w terminie nie dłuższym niż 3 dni robocze, dokonuje oceny, w jakim trybie należy rozpatrywać zgłoszenie, np. skarga, tryb wniosku o realizację prawa, wniosek o udzielenie dostępu do informacji publicznej.
2. W przypadku zaklasyfikowania zgłoszenia jako skargi, Administrator Danych Osobowych wyznacza osobę, która ma wystarczające kompetencje do realizacji zadania.
3. O zarejestrowaniu skargi z tytułu naruszenia ochrony danych osobowych Administrator Danych Osobowych niezwłocznie, w miarę możliwości w terminie nie dłuższym niż 2 dni robocze, informuje Inspektora Ochrony Danych, który odpowiada za nadzór nad zgodnością przetwarzania z RODO, udziela administratorowi oraz pracownikom zaleceń w celu zapewnienia przetwarzania zgodnie z RODO, a także stanowi punkt kontaktowy dla osób, których dane dotyczą, w sprawach dotyczących przetwarzania ich danych.
4. IOD czynnie uczestniczy w procesie udzielania odpowiedzi na skargi osób, których dane dotyczą, w szczególności wspierając wyznaczoną osobę lub komórkę w ustaleniu stanu faktycznego, ryzyka naruszenia lub oceny czy do naruszenia faktycznie doszło.
5. IOD, jako osoba posiadająca wiedzę i doświadczenie w dziedzinie stosowania przepisów o ochronie danych osobowych, na wniosek ADO może również przygotować treść odpowiedzi na skargę osoby, której dane dotyczą.
6. Wyznaczona przez ADO osoba, komórka lub IOD, na każdym etapie rozpatrywania skargi gotowi są do podjęcia współpracy z innymi komórkami merytorycznymi, które pomogą ocenić, czy doszło do naruszenia.
7. Wprowadza się obowiązek rejestracji wszystkich skarg wpływających bezpośrednio do siedziby organizacji lub na skrzynki mailowe pracowników, poprzez wpisanie do rejestru skarg wraz ze wskazaniem daty otrzymania. Wzór rejestru skarg stanowi załącznik do niniejszej PBDO.
8. Odpowiedź na skargę zostaje udzielona bez zbędnej zwłoki, jednak nie później niż w terminie jednego miesiąca od dnia otrzymania zgłoszenia.
9. W uzasadnionych przypadkach tj. z uwagi na skomplikowany charakter sprawy lub liczbę zgłoszeń, okres udzielenie odpowiedzi może zostać wydłużony maksymalnie o kolejne dwa miesiące. W takim przypadku, informuje się osobę fizyczną o niemożności rozpoznania jej skargi w terminie, przyczynie opóźnienia oraz planowanym terminie udzielenie odpowiedzi.
10. W przypadku, gdy realizacja skargi nie jest możliwa, Administrator Danych Osobowych informuje osobę o powodach braku podjęcia działań oraz możliwości wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

28. PROCEDURA WSPÓŁPRACY Z ORGANEM NADZORCZYM

Nadzór:	ADO
Stosowanie:	osoby upoważnione przez ADO do komunikacji z organem nadzorczym

Administrator Danych Osobowych świadomy jest jakie są właściwości, zadania i uprawnienia organu nadzorczego.

Celem niniejszej procedury jest określenie zasad współpracy z organem nadzorczym, w taki sposób aby umożliwić organowi nadzorczemu realizację jego zadań.

28.1. Ogólne zasady komunikacji z Prezesem UODO

1. Każdorazowe nawiązanie kontaktu z organem nadzorczym w imieniu Administratora Danych Osobowych, niezależnie od kanału komunikacji, wymaga uzyskania akceptacji ADO w kwestii zasadności kontaktu, przedmiotu, formy kontaktu oraz jego terminu.
2. Administrator Danych Osobowych jako osoby upoważnione do wszelkich kontaktów z organem nadzorczym (składana oświadczeń, w tym kierowania pism lub prowadzenia korespondencji z organem nadzorczym) w swoim imieniu, wyznacza Inspektora Danych Osobowych lub/i wskazane osoby.
3. Inspektor Ochrony Danych w ramach sprawowania swoich obowiązków, w porozumieniu z ADO, współpracuje z organem nadzorczym oraz pełni funkcję punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem.
4. Wprowadza się nakaz podejmowania każdej korespondencji wpływającej od organu nadzorczego.
5. Wszelka korespondencja otrzymana od organu nadzorczego, ze względu na swój charakter przekazywania jest w trybie pilnym do Administratora Danych Osobowych, a następnie w możliwie najkrótszym terminie (w miarę możliwości nie dłuższym niż 24 godziny) przekazywana jest do Inspektora Ochrony Danych oraz pozostałych osób, komórek których sprawa dotyczy.
6. W przypadku postępowań kontrolnych czy wystąpień, współpraca z organem nadzorczym prowadzona jest stosowanie do wymogów i potrzeb stron, z zachowaniem wymaganej formy i wyznaczonych terminów.

28.2. Kierowanie zapytań do organu nadzorczego

1. ADO świadomy jest, że zadaniem organu nadzorczego nie jest interpretowanie przepisów prawa w zakresie ochrony danych osobowych oraz udzielanie porad prawnych.
2. W sytuacji wystąpienia sytuacji problematycznych, w pierwszej kolejności ADO oraz osoby wyznaczone przez niego do realizacji tego zadania, dokonują pogłębionej analizy, czy organem właściwym do wydania opinii w danej sprawie nie jest inny od UODO organ, np. właściwy dla charakteru działalności organizacji.
3. W sytuacji, gdy analiza wykazała, ze organem właściwym dla sprawy jest organ nadzorczy w kwestiach ochrony danych, ADO zwraca się z wnioskiem do IOD o wydanie pisemnej opinii w sprawie.
4. Jeżeli opinia IOD nie jest według ADO wystarczająca lub/i w ocenie ADO nadal zachodzi konieczność konsultacji z organem nadzorczym, kontakt z UODO nawiązuje wyznaczona przez ADO osoba, a do korespondencji obligatoryjne załączana jest pisemna opinia IOD w sprawie.

28.3. Zasady współpracy w postępowaniach wyjaśniających, kontrolnych oraz wystąpieniach UODO

1. Administrator Danych Osobowych niezwłocznie reaguje na informację organ nadzorczego i zależnie od zakresu sprawy, powołuje zespół odpowiedzialny za obsługę postępowania wyjaśniającego, kontrolnego, wystąpienia, który będzie działał pod jego kierownictwem.

2. W skład zespołu wchodzi zawsze co najmniej jedna osoba posiadająca wiedzę merytoryczną i doświadczenie w obszarze, którego sprawa dotyczy, kierownik komórki organizacyjnej, której sprawa dotyczy.
3. Ze względu na ściśle kreślony terminu udzielania odpowiedzi na żądanie organu nadzorczego, każdy z pracowników powołanych do zespołu przez ADO, ma wyznaczonego swojego zastępcę.
4. IOD czynnie uczestniczy w procesie, w szczególności doradzając i wspierając zespół w pracach.
5. W postępowaniu kontrolnym ADO wyznacza osobę, która będzie go reprezentowała przed organem nadzorczym oraz sporządza pisemne upoważnienie dla tej osoby do reprezentowania go w trakcie kontroli.
6. Osoba wyznaczona bierze udział w każdej czynności kontrolnej. ADO może podjąć decyzję o udziale IOD w czynnościach kontrolnych.
7. ADO odpowiada za umożliwienie organowi nadzorczemu realizacji jego zadań, a w postępowaniu kontrolnym prowadzonym w jego siedzibie, po zweryfikowaniu pełnomocnictw kontrolerów, w szczególności:
   a. umożliwia wstęp na teren i do lokali lub innych pomieszczeń na terenie należącym do AOO,
   b. w miarę możliwości udostępnić odrębne pomieszczenie w celu prowadzenia czynności kontrolnych,
   c. wykonuje żądane kopie lub wydruki dokumentów lub informacji utrwalonych na dowolnych nośnikach,
   d. umożliwia dostęp do wszelkich zasobów mających związek z przedmiotem kontroli, w tym w szczególności do dokumentów, informacji lub urządzeń technicznych.
8. Wszystkie osoby zatrudnione w organizacji Administratora są zobowiązane do współpracy z Kontrolującym, w tym do składania wyjaśnień, okazywania dokumentów i umożliwiania dostępu do sprzętu służącego do przetwarzania danych osobowych. Wszystkie osoby zatrudnione w organizacji zobowiązane są w szczególności:
   a. wykonywać polecenia Administratora, przełożonego w zakresie współpracy z Kontrolującym;
   b. nie utrudniać kontroli, w szczególności poprzez:
      - blokowanie fizycznego dostępu do budynków, pomieszczeń, przedmiotów lub osób;
      - usuwanie, niszczenie lub chowanie dokumentów, komputerów, dysków czy innego sprzętu bądź ich zawartości;
      - udzielanie nieprawdziwych lub nierzetelnych informacji w odpowiedzi na pytania Kontrolującego;
      - omawianie kwestii będących przedmiotem kontroli z osobami nieupoważnionymi przez ADO do udziału w postępowaniu kontrolnym, a w szczególności z osobami spoza organizacji.
9. W razie wątpliwości, czy żądanie lub polecenie Kontrolującego pozostaje w związku z przedmiotem kontroli, lub w przypadku gdy ADO odmawia spełnienia żądania albo polecenia Kontrolującego, należy zadbać o zamieszczenie odpowiedniej wzmianki w protokole kontroli ze wskazaniem przyczyn takiej decyzji.
10. W razie zażądania przez Kontrolującego dostępu do danych lub informacji stanowiących tajemnicę przedsiębiorstwa, tajemnicę zawodową lub inną tajemnicę bądź informację prawnie chronioną, takie dane lub informacje należy ujawnić w minimalnym niezbędnym uzasadnionym zakresie, jednocześnie

żądając odnotowania w protokole kontroli powyższej okoliczności. W przypadku przekazywania Kontrolującemu kopii lub odpisu dokumentu zawierającego informacje stanowiące tego rodzaju tajemnicę lub informację prawnie chronioną, należy przekazać również wersję dokumentu niezawierającą tych informacji.

11. W razie zasadności złożenia zastrzeżeń do protokołu pokontrolnego sporządzonego przez Kontrolującego członkowie powołanego zespołu niezwłocznie zgłaszają ten fakt ADO.

28.4. POSTĘPOWANIA ADMINISTRACYJNE I SĄDOWOADMINISTRACYJNE

1. Osoba lub jednostka organizacyjna odpowiadająca za obsługę prawną ADO w zakresie dotyczącym ochrony danych osobowych w razie konieczności zasięga opinii IOD, co do treści pism lub innej dokumentacji związanej z postępowaniem administracyjnym oraz sądowoadministracyjnym.
2. Oceniając zasadność wniesienia do sądu administracyjnego skargi na decyzję (postanowienie) organu nadzorczego, osoba lub jednostka organizacyjna odpowiadająca za obsługę prawną ADO w zakresie dotyczącym ochrony Danych osobowych zasięga opinii IOD.

28.5. WNIOSEK O UPRZEDNIE KONSULTACJE

1. Administrator Danych Osobowych występuje z wnioskiem o uprzednie konsultacje do organu nadzorczego w sytuacji, w której w wyniku przeprowadzonej oceny skutków dla ochrony danych na liście badanych operacji przetwarzania znajdą się operacje, dla których ryzyko naruszenia praw i wolności oszacowane zostało jako wysokie i gdy ADO nie może znaleźć środków wystarczających do zmniejszenia (zminimalizowania) tego ryzyka do dopuszczalnego poziomu.
2. Warunkiem wystąpienia z wnioskiem o Konsultacje do Organu nadzorczego jest wcześniejsze dokonanie udokumentowanej oceny skutków dla ochrony danych w celu oszacowania w szczególności źródła, charakteru, specyfiki i powagi ryzyka naruszenia praw i wolności osób fizycznych. Ocena ta powinna w szczególności obejmować planowane środki, zabezpieczenia i mechanizmy mające zminimalizować to ryzyko.
3. ADO składa wniosek o konsultacje przed rozpoczęciem przetwarzania.
4. Wniosek o uprzednie konsultacje powinien spełniać wymogi określone w przepisach Kodeksu postępowania administracyjnego, w szczególności powinien zawierać co najmniej wskazanie ADO, jego adres i żądanie, a także powinien być podpisany przez ADO. Wniosek wniesiony w formie dokumentu elektronicznego powinien być opatrzony bezpiecznym podpisem elektronicznym lub podpisem potwierdzonym profilem zaufanym ePUAP.
5. Wniosek o uprzednie konsultacje zawiera co najmniej następujące informacje:
    a. cele i sposoby zamierzonego przetwarzania;
    b. środki i zabezpieczenia mające chronić prawa i wolności podmiotów danych, zgodnie z RODO;
    c. dane kontaktowe IOD,
    d. ocenę skutków dla ochrony danych, przeprowadzoną zgodnie z art. 35 RODO;

wszelkie inne informacje, których żąda organ nadzorczy.

29. PROCEDURA PRACY ZDALNEJ

Nadzór:	ADO, ASI, IOD
Stosowanie:	wszyscy pracownicy

Niniejsza procedura została opracowana z związku z wejściem w życie w dniu 07 kwietnia 2023 r. przepisów rozdziału II c - Praca zdalna w ustawie z dnia 26 czerwca 1974 r. - Kodeks pracy (Dz. U. z 2022 r. poz. 1510, 1700 i 2140).

Celem wprowadzenia niniejszej procedury jest zapewnienie bezpiecznego procesu przetwarzania danych osobowych w trakcie pracy zdalnej, zgodnie z RODO.

Niniejsze zasady bezpiecznego przetwarzania danych osobowych mają zastosowanie zarówno do wykonywania pracy zdalnej w formie stałej jak i okazjonalnej.

29.1. POSTANOWIENIA OGÓLNE

1. Pracownicy podczas pracy zdalnej mogą przetwarzać dane osobowe tylko w celach związanych z wykonywaniem swoich obowiązków służbowych.
2. Zabronione jest wykorzystywanie przez pracownika udostępnionych mu danych osobowych w celach niezwiązanych z wykonywaniem zadań i obowiązków służbowych.
3. Pracownik w trakcie pracy zdalnej zobowiązany jest dbać o bezpieczeństwo danych, ich poufność oraz integralność. Na pracowniku ciąży obowiązek dbałości o dobro zakładu pracy w przypadku postępowania z danymi osobowymi w trakcie pracy zdalnej.
4. Pracownik, w ramach pracy zdalnej zobowiązany jest do przetwarzania danych osobowych zgodnie z przepisami powszechnie obowiązującego prawa, w szczególności z przepisami o ochronie danych osobowych oraz innymi przepisami regulującymi pracę w zakładzie pracy zwłaszcza z Polityką Bezpieczeństwa Danych Osobowych.
5. Pracownik przed przystąpieniem do pracy zdalnej zobowiązany jest do zapoznania się z niniejszą procedurą oraz odbycia szkolenia z zasad bezpiecznego przetwarzania danych w czasie pracy zdalnej.

29.2. BEZPIECZEŃSTWO OBSZARU PRZETWARZANIA

1. Pracownik zobowiązany jest do zabezpieczania dostępu do posiadanych danych służbowych przed osobami postronnymi, w tym wspólnie z nim zamieszkującymi oraz przed ich nieuprawnionym zniszczeniem lub modyfikacją.
2. Pracownik zobowiązany jest do uniemożliwienia wglądu osobom postronnym w treści wyświetlane na ekranie sprzętu komputerowego, na przykład poprzez odpowiednie ustawienie ekranu lub zastosowanie nakładki na ekran tzw. filtru /folii prywatyzującej.
3. Pracownik zobowiązany jest do stosowania polityki czystego ekranu, tj. blokowania sprzętu komputerowego w razie oddalenia się od miejsca pracy.
4. Pracownik obowiązany jest po zakończeniu pracy na sprzęcie elektronicznym każdorazowo wylogować się z programów wykorzystywanych do pracy zdalnej oraz z systemu.

5. Pracownik zobowiązany jest do stosowania polityki czystego biurka.

29.3. Bezpieczeństwo pracy z dokumentacją papierową

1. Wynoszenie dokumentacji papierowej z siedziby Pracodawcy powinno być ograniczone do niezbędnego minimum. Pracodawca zezwala pracownikom na korzystanie z dokumentacji papierowej zawierającej dane osobowe w trakcie pracy zdalnej tylko w wyjątkowych sytuacjach. Generalną zasadą jest praca w obiegu elektronicznym.
2. W przypadku konieczności korzystania z dokumentacji papierowej poza siedzibą zakładu pracy w pierwszej kolejności należy rozważyć wykonanie kopii dokumentacji, na której pracownik będzie pracował. Kopie dokumentów z danymi osobowymi podlegają takiej samej ochronie jak oryginały.
3. Drukowanie dokumentów na potrzeby pracy (poza siedzibą organizacji) należy ograniczyć do niezbędnego minimum. W przypadku dokumentów zawierających dane osobowe należy w miarę możliwości dokonać anonimizacji danych.
4. Zabrania się drukowania dokumentów służbowych w zewnętrznych/publicznych punktach ksero lub z pomocą innych podmiotów, czy osób trzecich.
5. Podczas przenoszenia dokumentów pracownik zobowiązany jest do odpowiedniego ich zabezpieczenia i przenoszenia w taki sposób, aby były niewidoczne dla osób trzecich, na przykład w teczce wykonanej z nieprzezroczystego materiału.
6. Pracownik zobowiązany jest do odpowiedniego zabezpieczenia danych w formie papierowej w miejscu wykonywania pracy zdalnej - dokumenty i ich kopie powinny być przechowywane w zamykanych na klucz szufladach biurka lub szafach, należy zabezpieczyć dostęp do nich osób nieuprawnionych, w tym dzieci i domowników.
7. W przypadku korzystania przez pracownika z oryginałów dokumentów (lub kopii dokumentów, przechowywanych w siedzibie pracodawcy), po zakończeniu pracy powinny zostać niezwłocznie zwrócone do siedziby pracodawcy.
8. W przypadku korzystania przez pracownika z oryginałów dokumentów, pracownik przed pobraniem dokumentów podpisuje oświadczenie, na podstawie którego przyjmuje na siebie odpowiedzialność za powierzone dokumenty,
9. W przypadku korzystania z kopii dokumentacji (utworzonej na potrzeby pracy zdalnej), po zakończeniu pracy, kopie powinny zostać w całości zniszczone przez pracownika. W przypadku nieposiadania niszczarki w miejscu pracy pracownika, powinien on wykonane kopie zniszczyć niezwłocznie w siedzibie zakładu pracy.
10. Po zakończeniu pracy pracownik powinien bezwzględnie przestrzegać zasady czystego biurka.

29.4. Bezpieczeństwo nośników danych (służbowych i prywatnych)

1. Systemy, w tym system operacyjny wykorzystywany do pracy zdalnej, musi być wspierany przez producenta i regularnie aktualizowany.
2. Sprzęt wykorzystywany do pracy zdalnej musi być wyposażony w legalne i aktualne oprogramowanie antywirusowe.

3. Sprzęt komputerowy i inne urządzenia mobilne wykorzystywane w celach służbowych, w tym laptop, telefon lub tablet powinny być zabezpieczone przed dostępem osób trzecich, na przykład za pomocą silnego hasła i/lub dwustopniowego uwierzytelnienia.
4. W przypadku korzystania z prywatnego sprzętu komputerowego pracownik zobowiązany jest do utworzenia na tym sprzęcie odrębnego konta użytkownika przeznaczonego wyłącznie do celów służbowych i zabezpieczenia dostępu do tego konta silnym, znanym wyłącznie jemu hasłem.
5. Sprzęt powinien posiadać ustawione automatyczne blokowanie urządzenia po dłuższym okresie braku aktywności.
6. Zewnętrzne karty pamięci, a także inne nośniki danych, takie jak pendrive lub dysk zewnętrzny, wykorzystywane w celach służbowych powinny być zabezpieczone przed dostępem osób trzecich, na przykład za pomocą hasła.
7. W przypadku braku konieczności stosowania zewnętrznych kart pamięci i innych nośników zewnętrznych, sprzęt komputerowy wykorzystywany w celach służbowych powinien mieć zablokowane fizyczne porty USB.

29.5. Bezpieczeństwo domowej sieci

1. Sprzęt komputerowy powinien być podłączony do zabezpieczonej, domowej sieci WiFi.
2. Zabronione jest korzystanie z otwartych sieci WiFi, na przykład WiFi hotelowe, w galeriach handlowych lub hot-spot w publicznym miejscu.
3. Dostęp do panelu konfiguracyjnego urządzenia sieciowego oraz dostęp do sieci bezprzewodowej (sieci WiFi) powinien być zabezpieczony silnym hasłem. Zabronione jest pozostawianie domyślnych haseł Administratora Danych Osobowych na routerze WiFi.

29.6. Procedura bezpiecznego logowania

1. Dostęp do sprzętu lub programu wykorzystywanego do pracy zdalnej powinien być możliwy wyłącznie z wykorzystaniem indywidualnego identyfikatora (loginu) oraz hasła, na przykład poprzez ustawianie PIN-u lub innej formy uwierzytelnienia.
2. Hasło do sprzętu lub programu wykorzystywanego do pracy zdalnej powinno być odpowiednio długie i złożone. Nie powinno być ono zbudowane za pomocą ciągu znajdujących się obok siebie znaków na klawiaturze lub oparte na prostych skojarzeniach związanych z użytkownikiem, na przykład numer telefonu, data urodzenia, imiona lub nazwiska.
3. Zabronione jest udostępnianie osobom trzecim haseł oraz przechowywanie ich w miejscach nie gwarantujących ich poufności.
4. Zabronione jest domyślne zapamiętywanie hasła dostępu do programów, aplikacji wykorzystywanych w pracy zdalnej.
5. Zalecanym sposobem zabezpieczania danych logowania jest stosowanie klucza zabezpieczającego U2F (U2F security key).

29.7. PRACA Z DANYMI W OBIEGU ELEKTRONICZNYM - NA SPRZĘCIE SŁUŻBOWYM

1. Instalowanie jakiegokolwiek oprogramowania na sprzęcie służbowym jest możliwe tylko przez ASI lub za jego zgodą i zgodnie z jego wytycznymi.
2. Na sprzęcie komputerowym nie może być instalowane żadne nielegalne oprogramowanie.
3. Zabronione jest używanie prywatnego sprzętu lub prywatnych kont pocztowych do przetwarzania danych osobowych. Sprawy służbowe mogą być załatwiane tylko i wyłącznie przy użyciu służbowego sprzętu.
4. Pracownik nie może przechowywać na laptopie ani telefonie służbowym plików niezwiązanych z wykonywaną pracą lub jakichkolwiek innych plików lub programów, które nie posiadają stosownej licencji.
5. Pracownik nie może łączyć się z firmowymi systemami i dyskami sieciowymi z innego sprzętu niż sprzęt służbowy.
6. Łącząc się z zasobami sieciowymi pracodawcy, pracownik jest obowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN lub Web Dav.

29.8. PRACA Z DANYMI W OBIEGU ELEKTRONICZNYM - Z WYKORZYSTANIEM SPRZĘTU PRYWATNEGO

1. W przypadku korzystania z prywatnego sprzętu komputerowego pracownik zobowiązany jest do utworzenia na tym sprzęcie odrębnego konta użytkownika przeznaczonego wyłącznie do celów służbowych i zabezpieczenia dostępu do tego konta silnym, znanym wyłącznie jemu hasłem.
2. Na sprzęcie komputerowym wykorzystywanym do pracy zdalnej nie może być instalowane żadne nielegalne oprogramowanie.
3. Zabronione jest używanie prywatnych kont pocztowych do przetwarzania danych osobowych w celu realizacji zadań służbowych.
4. Łącząc się z zasobami sieciowymi pracodawcy, pracownik jest obowiązany korzystać z bezpiecznego połączenia za pomocą sieci VPN lub Web Dav.
5. Przechowywanie plików służbowych na komputerze prywatnym powinno być ograniczone do niezbędnego minimum.
6. Pracownik deklarując gotowość wykonywania pracy zdalnej z wykorzystaniem sprzętu prywatnego zapewnia, że spełnia on wymagania określone w punkcie „Bezpieczeństwo nośników danych" niniejszej procedury.

W przypadku utraty sprzętu (służbowego lub prywatnego) wykorzystywanego do pracy lub w przypadku identyfikacji wirusa lub jakichkolwiek podejrzanych aktywności na sprzęcie lub przetwarzanej dokumentacji (znikające pliki lub załączniki, pojawiające się lub znikające foldery, nieautoryzowana zmiana dokumentu), pracownik zobowiązany jest niezwłocznie poinformować o tym fakcie Administratora Danych Osobowych oraz Administratora Systemów Informatycznych.

29.9. ZASADY BEZPIECZNEGO PROWADZENIA WIDEOKONFERENCJI

Zasady bezpiecznego prowadzenia wideokonferencji	
Etapy wideokonferencji	**Wytyczne**
Przed rozpoczęciem wideokonferencji	▪ Zapoznaj się z ogólnymi warunkami użytkowania lub polityką prywatności programu, z którego chcesz skorzystać. ▪ Do zainstalowania aplikacji na komputerze użyj oficjalnej strony aplikacji, z której chcesz korzystać; w przypadku urządzeń mobilnych wybierz oficjalny sklep - Google Play lub App Store. ▪ Przed uruchomieniem spotkania upewnij się, że osoby postronne nie mają dostępu do Twojego ekranu oraz nie będą słyszały prowadzonych rozmów (użyj słuchawek z mikrofonem). ▪ Logując się do aplikacji, korzystaj wyłącznie z zalecanych przez pracodawcę dostępów, loginów itp. ▪ Korzystaj z aplikacji webowych, nie desktopowych. ▪ Przed udostępnieniem swojego ekranu podczas rozmowy zamknij wszystkie okna dialgowe, tak aby inni uczestnicy konferencji ich nie zobaczyli. ▪ Przy podłączeniu się do telekonferencji korzystaj z kodów dostępu PIN-ów. ▪ Użyj innego hasła, niż używane przez Ciebie w innych usługach. ▪ Przeskanuj program do telekonferencji systemem antywirusowym.
W trakcie korzystania z wideokonferencji	▪ Ogranicz ilość podawania danych osobowych do niezbędnego minimum. ▪ Nie udostępniaj linków do konferencji poza zamknięte grupy upoważnionych użytkowników. ▪ W celu wykonywania rozmów służbowych wykorzystuj dostęp do sieci za pomocą szyfrowanego połączenia VPN. ▪ Nie udostępniaj niezabezpieczonych plików. ▪ Jeżeli to możliwe, korzystaj z opcji zamazywania tła (tak żeby rozmówcy nie widzieli Twojego otoczenia). ▪ Jeżeli jesteś organizatorem spotkania, korzystaj z opcji "poczekalnia", tak abyś mógł kontrolować osoby uczestniczące w telekonferencji. ▪ Logując się do telekonferencji, wyłącz mikrofon i kamerę (włączysz je, jak będzie to potrzebne).
Po skorzystaniu z wideokonferencji	▪ Wyłącz mikrofon i kamerę. ▪ Upewnij się, że zakończyłeś spotkanie on-line i zamknąłeś aplikację. ▪ Sprawdź, czy program do telekonferencji nie działa w tle.

30. PROCEDURA AUDYTÓW

Nadzór:	ADO
Stosowanie:	IOD, ASI

Celem audytów jest dokonanie obiektywnej i bezstronnej oceny, czy opracowany w organizacji system ochrony danych jest skutecznie wdrożony i aktualizowany.

Wprowadza się następujące reguły dotyczące przeprowadzania audytów systemu ochrony danych osobowych:

1. Przyjmuje się, że audyty wewnętrzne przeprowadzane będą nie rzadziej niż jeden raz w ciągu 2 lat.
2. Za opracowanie planu oraz programu audytów odpowiada Administrator Danych Osobowych i Inspektor Ochrony Danych.
3. Audyt systemu ochrony danych przeprowadzany jest przez wyznaczonego w tym celu pracownika lub zlecony do wykonania przez podmiot zewnętrzny.
4. W przypadku wyznaczenia pracownika do przeprowadzenia audytu, stosuje się zasadę, że audytor nie kontroluje własnej pracy.
5. Jeżeli audyt ma przeprowadzić podmiot zewnętrzny, należy ustalić kryteria wyboru takiego podmiotu i podpisać umowę o świadczenie usług audytowych z uwzględnieniem powierzenia danych oraz zachowania w poufności informacji uzyskanych w toku czynności kontrolnych.
6. Przed rozpoczęciem zewnętrznego audytu, zespół pracowników ADO odpowiedzialnych za audyt zobowiązany jest do weryfikacji tożsamości audytora oraz sprawdzenia czy audytor posiada stosowne upoważnienie do wykonania usługi.
7. Administrator Danych Osobowych zapewnia audytorowi możliwość szczegółowego zapoznania się z audytowanymi obszarami, obowiązującą dokumentacją, wynikami poprzednich audytów oraz przeprowadzenia czynności kontrolnych mających na celu zebranie dowodów potwierdzających praktyczne przestrzeganie wdrożonych zasad, regulaminów i polityk.
8. Wynik audytu dokumentowany jest w postaci raportu, który przedkładany jest do Administratora Danych Osobowych.
9. Administrator Danych Osobowych i Inspektor Ochrony Danych dokonują analizy raportu ze szczególnym zwróceniem uwagi na stwierdzone uchybienia.
10. W przypadku stwierdzenia uchybień w funkcjonowaniu systemu ochrony danych, Administrator Danych Osobowych i Inspektor Ochrony Danych opracowują i wdrażają plan naprawczy.

31. POSTANOWIENIA KOŃCOWE

1. Administrator Danych Osobowych zobowiązany jest zapoznać z dokumentem wszystkie osoby przetwarzające dane osobowe oraz odebrać od nich pisemne oświadczenie o zapoznaniu się z treścią dokumentu.
2. Niezależnie od odpowiedzialności określonej w przepisach prawa powszechnie obowiązującego, naruszenie zasad określonych w niniejszej Polityce Bezpieczeństwa Danych Osobowych może być podstawą rozwiązania stosunku pracy bez wypowiedzenia z osobą, która dopuściła się naruszenia.
3. W sprawach nieuregulowanych w Polityce Bezpieczeństwa Danych Osobowych mają zastosowanie przepisy RODO oraz przepisy Ustawy.
4. Pracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce Bezpieczeństwa Danych Osobowych. W wypadku odrębnych od zawartych w niniejszej PBDO uregulowań występujących w innych procedurach obowiązujących w organizacji pracownicy mają obowiązek stosowania zapisów dalej idących, których stosowanie zapewni wyższy poziom ochrony danych osobowych.
5. W sprawach nieokreślonych w niniejszym dokumencie należy stosować instrukcje obsługi i zalecenia producentów aktualnie wykorzystywanych urządzeń i programów.
6. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest zapoznać się przed dopuszczeniem do przetwarzania danych z niniejszą Polityką Bezpieczeństwa Danych Osobowych oraz złożyć stosowne oświadczenie, potwierdzające znajomość jej treści.
7. Integralną częścią Polityki Bezpieczeństwa Danych Osobowych są jej załączniki, opisane w wykazie. Zmiana załączników lub ich aktualizacja nie wymaga zmiany dokumentu PBDO.
8. Polityka Bezpieczeństwa Danych Osobowych wchodzi w życie z dniem podpisania

32. WYKAZ ZAŁĄCZNIKÓW

Załącznikami do Polityki Bezpieczeństwa Danych Osobowych są:

- Załącznik nr 1 – Skrócona klauzula informacyjna
- Załącznik nr 2 – Pełna klauzula informacyjna – Przewodnik ochrony danych
- Załącznik nr 3 – Skrócona klauzula informacyjna do monitoringu wizyjnego
- Załącznik nr 4 – Procedura postępowania w sytuacji naruszenia ochrony danych osobowych – wersja skrócona
- Załącznik nr 5 – Wzór upoważnienia do przetwarzania danych osobowych
- Załącznik nr 6 – Wzór oświadczenia o zachowaniu w poufności oraz zapoznaniu się z dokumentacją dla osoby przetwarzającej dane
- Załącznik nr 7 – Wzór oświadczenia o zachowaniu w poufności oraz zapoznaniu się z dokumentacją dla osoby nie przetwarzającej danych
- Załącznik nr 8 – Oświadczenie pracodawcy i pracownika o stosowanych formach monitoringu
- Załącznik nr 9 – Wzór rejestru kategorii czynności przetwarzania, rejestru incydentów, rejestru upoważnień do przetwarzania danych osobowych, rejestru szkoleń, rejestru umów powierzenia, rejestru obsługi praw osób fizycznych
- Załącznik nr 10 – Wzór rejestru czynności przetwarzania danych

- Załącznik nr 11 – Wzór umowy powierzenia danych osobowych
- Załącznik nr 12 – Wzór Ankiety dla podmiotu przetwarzającego
- Załącznik nr 13 – Metodologia analizy ryzyka w procesach przetwarzania danych osobowych
- Załącznik nr 14 – Lista osób zapoznanych z PBDO
- Załącznik nr 15 – Wzór umowy o współadministrowanie

Dokument sporządzono: Data: 19.01.2024 r. Miejsce: Lublin	**Opracował**	**Sprawdził**	**Zatwierdził (ADO)**
	POLSKIE CENTRUM AUDYTU Inspektor Ochrony Danych		

Opracowano wg stanu prawnego na dzień 19.07.2024 r.

Autor opracowania:

Karol Górny prowadzący działalność gospodarczą pod firmą: GÓRNY KAROL SPEED COM z siedzibą w Lublinie /kod: 20-127/, przy ul. Walecznych 4/118, na podstawie wpisu do Centralnej Ewidencji i Informacji o Działalności Gospodarczej prowadzonej przez Ministra Gospodarki, NIP 946-246-10-88, REGON 060319864, będący właścicielem marki Polskie Centrum Audytu (PCA).

Polskie Centrum Audytu (PCA)


www.pca.pl


ul. Juliusza Ligonia 1, 20-805 Lublin


biuro@pca.pl


518 99 99 65

PLAN SPRAWDZEŃ: Data	**Sprawdził** (AW lub IOD)	**Zatwierdził** (ADO)
.....2025 r.		
.....2026 r.		
.....2027 r.		