(wprowadzona Zarządzeniem Dyrektora SP54 nr 18/2019 z dnia 06.05.2019 r.)

Administrator

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH w Szkole Podstawowej nr 54 im. Juliana Tuwima w Krakowie

Spis treści

1. Wstęp 4
1.1 O Polityce Bezpieczeństwa Danych Osobowych (PBDO) 4
1.2 Zakres obowiązywania 4
2. Słownik terminów 4
2.1 Definicje 4
2.2 Skróty 6
3. Organizacja wewnętrzna w zakresie ochrony danych osobowych 6
3.1 Role i odpowiedzialności w zakresie ochrony danych osobowych 6
3.1.1. Administrator (ADO) 6
3.1.2. Koordynator Ochrony Danych Osobowych (KODO) 7
3.1.3. Inspektor Ochrony Danych (IOD) 7
3.1.4. Administrator Bezpieczeństwa Fizycznego (ABF) 7
3.1.5. Administrator Systemu Informatycznego (ASI) 8
3.1.6. Użytkownik 8
4. Wymagania dotyczące zabezpieczania danych osobowych 8
4.1 Organizacyjne środki ochrony 8
4.1.1 Zasady dopuszczania do przetwarzania danych osobowych 8
4.1.2 Zarządzanie rejestrem czynności przetwarzania 9
4.1.3 Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych 10
4.1.4 Szacowanie ryzyka utraty bezpieczeństwa danych osobowych 10
4.1.5 Spełnienie obowiązku informacyjnego 10
4.1.6 Realizacja praw osoby, której dane dotyczą 11
4.1.7 Powierzenie przetwarzania danych osobowych 11
4.1.8 Udostępnianie danych osobowych 12
4.1.9 Uwzględnianie ochrony danych w fazie projektowania 12
4.1.10 Aktualizacja dokumentacji 13
1) ADO na bieżąco monitoruje aktualność dokumentacji. 13
4.2 Fizyczne środki ochrony 13
4.2.1 Strefy bezpieczeństwa 13
4.2.2 Zabezpieczenia miejsc przetwarzania danych osobowych 13
4.2.3 Identyfikacja obszary i miejsca przetwarzania danych osobowych 14
4.3 Techniczne środki ochrony 15
5. Naruszenie bezpieczeństwa informacji 15

6.	Sprawdzenia i sprawozdawczość dotycząca ochrony bezpieczeństwa informacji	15
7.	Załączniki	17
7.1	Załącznik nr 1 Zobowiązanie do zachowania w poufności informacji	17
7.2	Załącznik nr 2 Upoważnienie do przetwarzania danych osobowych	17
7.3	Załącznik nr 3 Rejestr czynności przetwarzania	17
7.4	Załącznik nr 4 Wzory obowiązków informacyjnych	17
7.5	Załącznik nr 5 Wykaz stref bezpiecznych	17
7.6	Załącznik nr 6 Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe	17
7.7	Załącznik nr 7 Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych	17
7.8	Załącznik nr 8 Instrukcja zgłaszania incydentów związanych z bezpieczeństwem danych osobowych	17
7.9	Załącznik nr 9 Procedura zarządzania incydentami bezpieczeństwa informacji	17
7.10	Załącznik nr 10 Instrukcja wydawania i zdawania kluczy do pomieszczeń	17
7.11	Załącznik nr 11 Wykaz aplikacji zastosowanych do przetwarzania danych osobowych	17
7.12	Załącznik nr 12 Wzór umowy powierzenia przetwarzania danych osobowych	17
7.13	Załącznik nr 13 Rejestr udostępnień	17
7.14	Załącznik nr 14 Regulamin użytkownika systemu informatycznego	17
7.15	Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych	17
7.16	Załącznik nr 16 Inwentaryzacja zasobów	17
7.17	Załącznik nr 17 Plan Sprawdzeń	17
7.18	Załącznik nr 18 Procedura realizacji praw osób których dane dotyczą	17
7.19	Załącznik nr 19 Procedura zarządzania systemem monitoringu wizyjnego	17
7.20	Załącznik nr 20 Rejestr upoważnień	17

1. Wstęp

1.1 O Polityce Bezpieczeństwa Danych Osobowych (PBDO)

1.2 Zakres obowiązywania

1) PBDO stanowi zbiór zasad, które obowiązują w stosunku do zbiorów danych osobowych, niezależnie od formy przetwarzania, których Administratorem w myśl Rozporządzenia Parlamentu Europejskiego w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE, jest PODMIOT. Ustanowione w niniejszej polityce zasady muszą być stosowane przez wszystkie osoby posiadające dostęp do danych osobowych.
2) Polityka określa zasady ochrony infrastruktury oraz zasobów informatycznych, służących do przetwarzania danych osobowych.
3) Niniejszy dokument dotyczy wszystkich osób zatrudnionych, współpracujących lub świadczących usługi na rzecz PODMIOTU, a także innych osób, mających dostęp do informacji, stanowiących dane osobowe.

2. Słownik terminów

2.1 Definicje

1) **Inspektor Ochrony Danych** – osoba odpowiedzialna za nadzór nad bezpieczeństwem informacji przetwarzanych w PODMIOCIE.
2) **Administrator** – PODMIOT decydujący o celach i środkach przetwarzania danych osobowych.
3) **Administrowanie danymi** – zakres funkcji i czynności obejmujący zarządzanie danymi osobowymi; te funkcję spełniają konkretni pracownicy PODMIOTU, na których przenoszone są obowiązki Administratora.
4) **Administrator Systemu Informatycznego** - osoba odpowiedzialna za ciągłość pracy, rozwój oraz bezpieczeństwo systemu informatycznego służącego do przetwarzania danych osobowych.
5) **Administrator Bezpieczeństwa Fizycznego** – osoba odpowiedzialna za ciągłość pracy, utrzymanie infrastruktury (budynki, pomieszczenia) oraz rozwój w obszarze bezpieczeństwa fizycznego.
6) **Aplikacja**– program komputerowy przetwarzający informacje, będący częścią systemu informatycznego PODMIOTU, do stosowania których PODMIOT został zobowiązany (aplikacja zewnętrzna) lub wdrożony na potrzeby własne (aplikacja wewnętrzna).
7) **Bezpieczeństwo informacji** – to zachowanie atrybutów poufności, integralności, rozliczalności oraz dostępności informacji.
8) **Dane osobowe** – 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.
9) **Dokument** – dokumentem jest każdy przedmiot lub inny zapisany nośnik informacji (np. pismo, świadectwo, plik elektroniczny, fotografia), z którym jest związane określone prawo, albo który ze względu na zawartą w nim treść stanowi dowód prawa, stosunku prawnego lub okoliczności mającej znaczenie prawne.

10) **Dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu
11) **Identyfikator użytkownika –** ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę, która jest użytkownikiem systemu informatycznego.
12) **Incydent** – pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia działań organizacji i zagrażają bezpieczeństwu informacji.
13) **Naruszenie ochrony danych osobowych -** oznacza naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
14) **Informacja** – to taki czynnik, któremu można przypisać określone znaczenie, aby móc go wykorzystywać do różnych celów.
15) **Integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności aktywów.
16) **Odbiorca danych** – każdy, komu udostępnia się dane osobowe, z wyłączeniem osoby, której dane dotyczą, osoby upoważnionej do przetwarzania danych, organów państwowych lub organów samorządu terytorialnego, którym dane są udostępniane w związku z prowadzonym postępowaniem.
17) **PODMIOT** – jednostka, dla której opracowana jest dokumentacja.
18) **Poufność** – właściwość polegająca na tym, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
19) **Pracownik** – osoba, z którą PODMIOT nawiązał stosunek pracy na podstawie umowy o pracę (umowa na czas nieokreślony, umowa na czas określony, umowa o dzieło oraz umowa zlecenie), wolontariusz, praktykant odbywający praktykę, stażysta odbywający staż na podstawie odrębnej umowy, zleceniobiorca, z którym PODMIOT podpisał umowę o dzieło lub umowę zlecenie.
20) **Przetwarzanie danych** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie .
21) **Rejestr czynności przetwarzania** – rejestr zbiorów danych osobowych przetwarzanych w PODMIOCIE lub powierzonych do przetwarzania podmiotowi zewnętrznemu, a którego Administratorem jest PODMIOT.
22) **Rejestr upoważnień** – baza danych o wydanych i odwołanych Upoważnieniach.
23) **Rozliczalność** – właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
24) **Ryzyko** – kombinacja prawdopodobieństwa zdarzenia i jego konsekwencji.
25) **System Informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.
26) **Upoważnienie** – pisemna zgoda Administratora lub osoby działającej w jego imieniu, upoważniająca do przetwarzania danych osobowych
27) **Rozporządzenie** – 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).
28) **Użytkownik** – osoba, która posiada konto w systemie informatycznym należącym do PODMIOTU.

29) **Koordynator Ochrony Danych Osobowych (KODO)** – osoba odpowiedzialna za nadzór nad bezpieczeństwem informacji przetwarzanych w PODMIOCIE.
30) **Zbiór danych osobowych** – każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie.

2.2 Skróty

1) **PBDO** – Polityka Bezpieczeństwa Danych Osobowych.
2) **IOD** – Inspektor Ochrony Danych.
3) **ADO** –Administrator.
4) **ASI** – Administrator Systemu Informatycznego.
5) **ABF** – Administrator Bezpieczeństwa Fizycznego.
6) **IZSI** – Instrukcja Zarządzania Systemem Informatycznym.
7) **KODO** - Koordynator Ochrony Danych Osobowych.
8) **SI** – System Informatyczny.
9) **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).
10) **PODMIOT** – jednostka, dla której opracowana jest dokumentacja.

3. Organizacja wewnętrzna w zakresie ochrony danych osobowych

1) W celu efektywnego zarządzania ochroną danych osobowych w PODMIOCIE funkcjonuje formalna organizacja wewnętrzna, w skład której wchodzą następujące role:
   a) Administrator (ADO)
   b) Koordynator Ochrony Danych Osobowych (KODO),
   c) Inspektor Ochrony Danych (IOD),
   d) Administrator Systemu Informatycznego (ASI),
   e) Administrator Bezpieczeństwa Fizycznego (ABF)
   f) Użytkownik.

3.1 Role i odpowiedzialności w zakresie ochrony danych osobowych

3.1.1. Administrator (ADO)

1) Pełni funkcje na zasadach i w zakresie określonym w RODO w szczególności:
   a) Definiuje i zatwierdza PBDO .
   b) Nadzoruje realizacje postanowień PBDO.
   c) Określa sposób, w jaki dane osobowe są zarządzane, zabezpieczane i przetwarzane.
   d) Zapewnia niezbędne zasoby potrzebne do odpowiedniego funkcjonowania PBDO.
   e) Wyznacza IOD i zgłasza fakt jego wyznaczenia organowi nadzorczemu tj. Prezesowi Urzędu Ochrony Danych Osobowych. ADO wyznacza także: ASI, KODO, ABF.
   f) Zatwierdza kierunki rozwoju i doskonalenia PBDO proponowane przez IOD , ASI, KODO, ABF.
   g) Prowadzi rejestr czynności przetwarzania zgodnie z przyjętym załącznikiem nr 3 do PBDO.
2) Odpowiada za zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności przez:

a) sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych,
b) nadzorowanie opracowania i aktualizowania dokumentacji, opisującej sposób przetwarzania danych oraz zapewnienia środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem,
c) nadzorowanie przestrzegania zasad określonych w dokumentacji, o której mowa w ppkt. b),
d) zapewnianie zapoznania osób upoważnionych do przetwarzania danych osobowych z przepisami o ochronie danych osobowych;

3) nadzoruje i monitoruje przestrzeganie zasad ochrony przetwarzanych informacji.
4) wydaje upoważnienia do przetwarzania danych osobowych.
5) prowadzi rejestr użytkowników upoważnionych do przetwarzania danych osobowych.
6) zapoznaje pracowników z regulacjami dotyczącymi bezpieczeństwa danych osobowych.
7) realizuje proces spełnienia żądań osób, których dane dotyczą we współpracy z IOD.
8) zarządza incydentami bezpieczeństwa informacji– realizuje procedurę obsługi incydentów, analizuje incydenty, wszczyna postępowanie wyjaśniające w związku z incydentami oraz prowadzi rejestr incydentów bezpieczeństwa.
9) Odpowiada za poprawność merytoryczną danych osobowych zawartych w zbiorze danych osobowych oraz ich aktualizację.
10) Odpowiada za aktualizację informacji w rejestrze czynności przetwarzania.
11) Określa narzędzia, metody, miejsce i czas przetwarzania informacji w zbiorze danych.
12) Wyraża zgodę na udostępnianie informacji zgodnie z przepisami prawa.
13) Realizuje proces udostępniania danych osobowych oraz prowadzi rejestr udostępnień.

3.1.2. Koordynator Ochrony Danych Osobowych (KODO)

1) Odpowiada za identyfikowanie zbiorów danych osobowych, ich opisanie i zgłoszenie ADO.
2) Zastępuje podczas nieobecności Inspektora Ochrony Danych.
3) Wspiera merytoryczne Administratora.
4) Koordynuje i nadzoruje działania związane z ochroną danych osobowych.
5) Współpracuje z Administratorem oraz Inspektorem Ochrony Danych.

3.1.3. Inspektor Ochrony Danych (IOD)

1) informowanie ADO 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 RODO, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków,
3) podejmowanie działań mających na celu zwiększające świadomość, w tym szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty,
4) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania (w przypadku gdy PUODO wyda takie zalecenie),
5) współpraca organem nadzorczym,
6) pełnieni funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

3.1.4. Administrator Bezpieczeństwa Fizycznego (ABF)

1) Odpowiada za wdrażanie PBDO w obszarze fizycznych środków ochrony.
2) Odpowiada za zabezpieczenie danych osobowych przed ich fizycznym udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.
3) Prowadzi wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe oraz odpowiada za jego aktualizację.
4) Koordynuje proces wdrażania, utrzymania i konserwacji systemów zabezpieczeń fizycznych i technicznych (SSWiN, SKD, CCTV, klucze, identyfikatory pracowników).

3.1.5. Administrator Systemu Informatycznego (ASI)

1) Zarządza SI.
2) Odpowiada za aktualizację dokumentów IZSI.
3) Nadzoruje stosowanie środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych w SI , a w szczególności odpowiada za zabezpieczenie tych danych przed ich udostępnieniem osobom nieupoważnionym, uszkodzeniem lub zniszczeniem.
4) Nadzoruje prowadzenie bieżącej ewidencji wszystkich użytkowników i ich identyfikatorów wykorzystywanych w SI.
5) Odpowiada za realizację wdrożenia aplikacji.
6) Rekomenduje rozbudowę SI oraz wprowadzanie nowych technologii.
7) Administruje licencjami SI.

3.1.6. Użytkownik

1) Odpowiada za przestrzeganie postanowień oraz zasad ustanowionych w PBDO w zakresie nałożonych na niego obowiązków.
2) Odpowiada za zabezpieczenie przekazanych do przetwarzania danych przed ich udostępnieniem osobom nieupoważnionym, zabraniem przez osobę nieuprawnioną, uszkodzeniem lub zniszczeniem.
3) Odpowiada za niezwłoczne poinformowanie ADO, KODO, a w przypadku ich nieobecności osoby je zastępujące, w przypadku zidentyfikowania wszelkich naruszeń w zakresie bezpieczeństwa danych osobowych.

4. Wymagania dotyczące zabezpieczania danych osobowych

4.1 Organizacyjne środki ochrony

4.1.1 Zasady dopuszczania do przetwarzania danych osobowych

4.1.1.1 Szkolenie i zobowiązanie do zachowania w poufności

1) Wszyscy pracownicy zatrudnieni przy przetwarzaniu danych osobowych muszą zostać zapoznani z obowiązującymi w PODMIOCIE przepisami dotyczącymi ochrony danych osobowych oraz podpisać zobowiązanie do zachowania w tajemnicy informacji, do których będą mieli dostęp, zgodnie ze wzorem stanowiącym Załącznik nr 1 Zobowiązanie do zachowania w poufności ”. Zobowiązanie to przechowuje się w aktach osobowych pracownika.

2) Przedstawiciele stron trzecich z przepisami dotyczącymi ochrony danych osobowych w PODMIOCIE zapoznaje osoba odpowiedzialna za podpisanie tej umowy (tzw. opiekun umowy). Opiekun umowy pobiera od każdej osoby reprezentującej stronę trzecią, która będzie przetwarzać dane osobowe, zobowiązanie do zachowania w tajemnicy danych osobowych i przekazuje je do ADO, w celu archiwizacji.

4.1.1.2 Zarządzanie upoważnieniami do przetwarzania danych osobowych

1) Do przetwarzania danych osobowych mogą być dopuszczone tylko osoby posiadające ważne upoważnienie do przetwarzania danych osobowych w zbiorze danych osobowych PODMIOTU oraz w zbiorach danych osobowych powierzonych PODMIOTOWI w ramach zawartych umów.
2) Upoważnienia do przetwarzania danych osobowych w PODMIOCIE wystawia i zatwierdza ADOw oparciu o:
   a. zobowiązanie do zachowania w tajemnicy informacji.
   b. zakres danych niezbędnych do wykonywania obowiązków służbowych.
3) ADO prowadzi i aktualizuje Rejestr upoważnień w formie elektronicznej i/lub papierowej.(Załącznik nr 20 Rejestr upoważnień)
4) Rejestr upoważnień zawiera co najmniej:
   a. imię i nazwisko osoby upoważnionej
   b. datę wydania upoważnienia,
   c. zakres upoważnienia (nazwa i/lub numer zbioru danych osobowych),
   d. datę wygaśnięcia upoważnienia.
5) ADO jest obowiązany do przekazywania informacji w PODMIOCIE o wydanych i odwołanych upoważnieniach poszczególnych pracowników oraz ASI.

4.1.1.3 Wydawanie upoważnień

1) Upoważnienia są wydawane pracownikom lub przedstawicielom firm zewnętrznych, którym jest to niezbędne w celu właściwego wykonywania obowiązków służbowych.
2) Upoważnienie może zostać wydane pracownikowi, który spełnił wymagania określone w punkcie 4.1.1.1. na wzorze, który przedstawia Załącznik nr 2 Upoważnienie do przetwarzania danych osobowych.
3) Upoważnienie jest wydawane w 2 egzemplarzach - jeden dla ADO i jeden dla pracownika.

4.1.1.4 Wygaśnięcie upoważnień

1) Upoważnienie wygasa w przypadku:
   a. upływu okresu jego ważności,
   b. odwołania,
   c. ustania stosunku pracy bądź rozwiązania innej umowy (np.: o dzieło, zlecenia).
2) ADO dokonuje odpowiednich zmian w Rejestrze upoważnień, wpisując datę ustania upoważnienia oraz niezwłocznie informuje ASI oraz pracownika, którego upoważnienie dotyczy, o jego odwołaniu.

4.1.2 Zarządzanie rejestrem czynności przetwarzania

4.1.2.1 Potrzeba przetwarzania nowego zbioru danych osobowych

1) W PODMIOCIE zabronione jest przetwarzanie danych osobowych w zbiorze danych osobowych, jeśli zbiór taki nie figuruje na Rejestrze Czynności Przetwarzania, którego wzór stanowi **Błąd! Nie można odnaleźć źródła odwołania.**do niniejszej Polityki.
2) KODO zgłasza potrzebę utworzenia nowego zbioru danych osobowych do ADO oraz przekazują wszystkie stosowne informacje dotyczące nowego zbioru. Utworzenie nowego zbioru danych osobowych może być wynikiem:

a. realizacji określonego celu,
b. przyjęcia zbioru danych osobowych w wyniku zawarcia umowy o powierzeniu przetwarzania lub przekazania zbioru danych osobowych należących do innego podmiotu.

4.1.2.2 Tworzenie zbioru danych

1) ADO, po otrzymaniu zgłoszenia dotyczącego potrzeby utworzenia nowego zbioru danych osobowych, analizuje zawartość informacyjną zgłaszanego zbioru oraz określa, czy zbiór jest nowym zbiorem danych osobowych na podstawie:
   a. zakresu danych ,
   b. celu przetwarzania danych zawartych w zbiorze.
2) ADO wpisuje do Rejestru Czynności Przetwarzania, informacje o zbiorze zgodnie ze wzorem stanowiącym **Błąd! Nie można odnaleźć źródła odwołania.** do niniejszej Polityki.

4.1.2.3 Aktualizacja rejestru czynności przetwarzania

1) Aktualizacja rejestru czynności przetwarzania wymagana jest w szczególności:
   a. W przypadku powierzenia przetwarzania danych osobowych administrowanych przez PODMIOT innemu podmiotowi w wyniku podpisania umowy,
   b. W przypadku udostępnienia danych osobowych administrowanych przez PODMIOT innemu podmiotowi.
   c. W przypadku zmian w warunkach technicznych, organizacyjnych lub prawnych.
2) ADO na podstawie informacji otrzymanych od KODO oraz po analizie dokumentacji, podejmuje decyzję o konieczności aktualizacji informacji w Rejestrze Czynności Przetwarzania i taką aktualizację wprowadza.
3) ADO tworzy historię zmian w rejestrze czynności przetwarzania i odnotowuje informacje o wszelkich dokonywanych w nim zmianach w karcie rejestracji będącą integralną częścią rejestru czynności przetwarzania.

4.1.2.4 Usuwanie zbioru danych osobowych z rejestru czynności przetwarzania

1) Decyzję o usunięciu każdego zbioru danych osobowych podejmuje ADO.
2) Usunięcie zbioru danych osobowych z rejestru czynności przetwarzania następuje niezwłocznie po zaprzestaniu przetwarzania danych w zbiorze i odnotowuje ten fakt w karcie rejestracji będącej integralną częścią rejestru czynności przetwarzania.
3) ADO jest zobowiązany do podjęcia działań mających na celu wyrejestrowanie zbioru danych z rejestru czynności przetwarzania oraz fizycznego usunięcia danych, z uwzględnieniem wymogów procedur wewnętrznych oraz przepisów o archiwizacji danych.
4) ADO każdorazowo po usunięciu zbioru danych osobowych z rejestru czynności przetwarzania aktualizuje upoważnienia pracowników.

4.1.3 Inwentaryzacja zasobów wspierających przetwarzanie danych osobowych

1) ADO odpowiedzialny jest za inwentaryzację zasobów wspierających przetwarzanie informacji zgodnie z Załącznik nr 16 Inwentaryzacja zasobów.
2) Inwentaryzacja podlega okresowej aktualizacji (nie rzadziej niż raz na rok)

4.1.4 Szacowanie ryzyka utraty bezpieczeństwa danych osobowych

1) ADO odpowiedzialny jest za okresową realizację szacowania ryzyka utraty bezpieczeństwa danych osobowych.
2) Aktualizacja wyników szacowania ryzyka realizowana jest przynajmniej raz do roku.
3) Wyniki szacowania ryzyka oraz planowane działania minimalizujące ryzyko zatwierdzane są przez ADO.

4.1.5 Spełnienie obowiązku informacyjnego

1) W stosunku do osób, których dane osobowe PODMIOT zbiera w celu włączenia ich do zbiorów i dalszego przetwarzania należy spełnić obowiązek informacyjny.
2) Obowiązek informacyjny należy spełnić w przypadku:
   a. zbierania danych osobowych od osoby, której one dotyczą (art. 13 RODO) w momencie pozyskiwania danych,
   b. zbierania danych osobowych nie od osoby, której one dotyczą (art. 14 RODO) najpóźniej w terminie wskazanym w art. 14 ust 3 RODO.
3) Spełnienie obowiązku informacyjnego nie jest konieczne, jeżeli:
   a. osoba, której dane dotyczą, dysponuje już tymi informacjami, co PODMIOT jest w stanie wykazać,
   b. pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii lub prawem polskim, przewidującym odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą.
4) Wykaz wzorów oświadczeń o spełnieniu obowiązku informacyjnego stanowi Załącznik nr 4 Wzory obowiązków informacyjn do niniejszej Polityki.
5) Za należyte spełnienie obowiązku informacyjnego w stosunku do osób fizycznych, których dane są przetwarzane przez PODMIOT odpowiada ADO.

4.1.6 Realizacja praw osoby, której dane dotyczą

1) Spełnienie praw osoby, której dane dotyczą obejmuje:
   a. Prawo do dostępu do danych (art. 15 RODO)
   b. Prawo do sprostowania danych (art. 16 RODO),
   c. Prawo do usunięcia danych (art. 17 RODO), z wyjątkiem gdy przetwarzanie jest niezbędne do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa polskiego, lub do wykonania zadania realizowanego w interesie publicznym, lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
   d. Prawo do ograniczenia przetwarzania (art. 18 RODO),
   e. Prawo do przenoszenia danych (art. 20 RODO),
   f. prawo do sprzeciwu w przypadkach związanych ze szczególną sytuacją osoby, które dane dotyczą, gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi (art. 21 RODO)
2) Spełnienie praw osoby następuje zgodnie z załącznikiem nr 18 Procedura realizacji praw osób których dane dotyczą.

4.1.7 Powierzenie przetwarzania danych osobowych

1) W uzasadnionych przypadkach wynikających z realizacji zadań, dopuszcza się powierzenie przetwarzania danych osobowych podmiotowi zewnętrznemu w formie umowy.
2) Treść umowy, o której mowa w p. 1, musi obejmować elementy określone w art. 28 ust. 3 RODO, w tym co najmniej:
   a. zakres i cel przetwarzania danych osobowych,
   b. zobowiązanie podmiotu, któremu powierza się dane, do zastosowania środków zabezpieczających dane osobowe oraz zapewnienie podmiotu przetwarzającego, by osoby upoważnione do przetwarzania danych osobowych zobowiązały się do zachowania ich w tajemnicy,
   c. oświadczenie o podjęciu środków wymaganych na mocy art. 32 RODO,
   d. określenie sposobu sprawowania przez PODMIOT kontroli należytego wykonania umowy w powyższym zakresie,

e. określenie sposobu dochodzenia roszczeń PODMIOTU w przypadku, gdy nastąpi naruszenie ochrony danych z przyczyn leżących po stronie podmiotu, któremu przetwarzanie danych powierzono,
f. określenie odpowiednich środków technicznych i organizacyjnych w celu wywiązania się z obowiązku odpowiadania na żądania osoby, której dane dotyczą w zakresie wykonywania jej praw określonych w rozdziale III RODO, określenie zasad informowania współpracy przy realizacji obowiązków określonych w art. 32–36 RODO,
g. określa zasady postępowania z informacjami po zakończeniu świadczenia usług związanych z przetwarzaniem danych,
h. umożliwienie administratorowi lub upoważnionemu audytorowi przeprowadzenie audytu u podmiotu przetwarzającego.

3) Każdorazowo umowę, o której mowa w p. 1, opiniuje Radca Prawny, a podpisuje ADO lub osoba upoważniona przez ADO.
4) ADO jest obowiązany do aktualizacji Rejestrze Czynności Przetwarzania o informację powierzenia danych osobowych wraz z danymi podmiotu któremu są udostępniane.

4.1.8 Udostępnianie danych osobowych

1) Wszystkie dane osobowe udostępnia się na pisemny, umotywowany wniosek, chyba że przepis prawa stanowi inaczej. Wniosek powinien zawierać informacje umożliwiające wyszukanie w zbiorze żądanych danych osobowych oraz wskazywać podstawę prawną wystąpienia z wnioskiem, zakres wnioskowanych danych i ich przeznaczenia.
2) KODO weryfikuje wniosek o udostępnienie danych osobowych pod kątem spełnienia wymagań formalnych. W szczególności sprawdza czy wniosek zawiera:
   a. dane o wnioskodawcy,
   b. zakres żądanych informacji,
   c. cel pozyskania danych,
   d. podstawę prawną upoważniającą do pozyskania informacji.
3) Jeśli wniosek nie zawiera któregoś z powyżej wskazanych elementów, wnioskodawcę wzywa się do o uzupełnienia wniosku.
4) ADO podejmuje decyzję dotyczącą udostępnienia danych osobowych. Wypracowując decyzję .
5) Jeśli wniosek spełnia wymagania, o których mowa w pkt. 2, ADO:
   a. przygotowuje pismo do wnioskodawcy informujące o negatywnym rozpatrzeniu wniosku o udostępnienie danych osobowych bądź
   b. przygotowuje żądane dane i wysyła odpowiedź do wnioskodawcy oraz odnotowuje udostępnienie w Rejestrze udostępnień, który prowadzony jest w formie elektronicznej lub papierowej, zgodnie ze wzorem przedstawionym w Załączniku nr 13.
6) Informacje zawierające dane osobowe są przekazywane uprawnionym podmiotom:
   a. listem poleconym za potwierdzeniem odbioru,
   b. w drodze teletransmisji danych, zgodnie z zasadami ochrony danych osobowych
   c. osobiście za potwierdzeniem odbioru,
   d. w inny sposób określony przepisami prawa lub umową.
7) ADO prowadzi Rejestr udostępnień (załącznik nr 13) danych osobowych obejmujący co najmniej:
   a. kolejny numer udostępnienia,
   b. oznaczenie podmiotu, któremu udostępniono dane,
   c. oznaczenie zbioru, z którego pochodzą udostępniane dane osobowe,
   d. rodzaj udostępnianych danych,

e. sposób udostępnienia danych,
f. daty udostępnienia.

4.1.9 Uwzględnianie ochrony danych w fazie projektowania

1) W przypadku określania nowych sposobów przetwarzania danych osobowych (np. tworząc nowy zbiór danych osobowych, wdrażając nowy system informatyczny lub zamawiając do w drodze zamówienia publicznego tj. przy określaniu istotnych warunków zamówienia) lub modyfikacji dotychczas stosowanych sposobów i środków przetwarzania danych osobowych ADO obowiązany jest określić/zamówić, zaprojektować i wdrożyć odpowiednie środki techniczne i organizacyjne w celu ochrony danych osobowych.
2) W celu identyfikacji odpowiednich zabezpieczeń należy przeprowadzić szacowanie ryzyka zgodnie z zasadami określonymi w Załączniku nr 21.
3) Przy zakupie gotowych rozwiązań informatycznych ADO powinien wybierać te, które posiadają zaimplementowane zabezpieczenia służące zabezpieczeniu danych.
4) Do technicznych środków ochrony danych, które należy rozważyć do stosowania można zaliczyć m.in.:
   a. pseudonimizację przechowywanych danych osobowych w bazach danych,
   b. szyfrowanie danych składowanych w bazach danych,
   c. zabezpieczanie transmisji danych w sieciach publicznych (szyfrowanie transmisji),
   d. walidację pól wejściowych w formularzach aplikacji,
   e. systemy logowania i zarządzania hasłami,
   f. funkcje zarządzania uprawnieniami w aplikacjach,
   g. funkcje ograniczające dostęp do informacji przetwarzanych w aplikacjach,
   h. systemy monitorowania i rejestrowania zdarzeń i aktywności użytkowników,
   i. funkcje wykonania kopii zapasowej danych osobowych.

4.1.10 Aktualizacja dokumentacji

1) ADO na bieżąco monitoruje aktualność dokumentacji.

4.2 Fizyczne środki ochrony

3.2.1 Strefy bezpieczeństwa

1) Ustala się podział obszarów na strefy:
   a. Ogólnodostępną – dostępna dla wszystkich osób wchodzących na teren PODMIOTU lub pomieszczenia, do których dostęp został ograniczony z innych względów niż ochrona danych osobowych (np. bezpieczeństwo uczniów lub ochrona mienia) .
   b. Ograniczonego dostępu (Administracyjna) – są to pomieszczenia, do których sprawowana jest kontrola dostępu (również z rozpoznaniem tożsamości osoby). Dostęp domyślnie posiadają pracownicy PODMIOTU.
   c. Bezpieczna – to obszar do którego dostęp jest ograniczony do ściśle określonych osób. Zarówno wejścia do strefy jak i wyjścia ze strefy bezpiecznej są nadzorowane i wymagają rozpoznania tożsamości osoby. Przykładowe pomieszczenia zlokalizowane w strefie bezpiecznej to serwerownie, miejsca tymczasowego przechowywania akt (składnica akt).
2) Wykaz stref ogólnodostępnych, ograniczonego dostępu (administracyjna) oraz bezpiecznych w zajmowanych przez PODMIOT obiektach prowadzi ADO zgodnie z Załącznik nr 5 Wykaz stref bezpiecznych.

3.2.2 Zabezpieczenia miejsc przetwarzania danych osobowych

3.2.2.1 Zabezpieczanie pomieszczeń należących do strefy ograniczonego dostępu (administracyjna)

1) Pomieszczenia biurowe w strefie ograniczonego dostępu, w których znajdują się terminale systemu teleinformatycznego oraz nośniki danych osobowych w postaci papierowej powinny posiadać zamki.

3.2.2.2 Zabezpieczanie pomieszczeń należących do strefy bezpiecznej

1) W strefie bezpiecznej powinny być przechowywane: serwery, urządzenia sieci teleinformatycznej, urządzenia zapewniające zasilanie bezprzerwowe, składnice akt.
2) Wstęp do strefy bezpiecznej jest ograniczony tylko do tych osób, które uzyskały stosowne uprawnienia.
3) Pobyt osób, które nie posiadają uprawnień lub zgody do przebywania w strefie bezpiecznej musi odbywać się pod kontrolą osoby upoważnionej.
4) Pomieszczenia w strefie bezpiecznej muszą być zamykane na klucz.
5) Strefa bezpieczna jest chroniona systemem sygnalizacji włamania .
6) Monitorowane są warunki środowiskowe pomieszczeń w strefie bezpiecznej (np. wilgotność w składnicy akt)

3.2.2.3 Zarządzanie dostępem do pomieszczeń – zarządzanie kluczami

1) Za organizację zabezpieczenia oraz organizację wydawania kluczy do pomieszczeń PODMIOTU odpowiada ABF/ADO.
2) Zasady zarządzania dostępem do pomieszczeń zawiera Załącznik nr 10 Instrukcja wydawania i zdawania kluczy do pomieszczeń.

3.2.2.4 Wymagania dla systemów wspomagających (zasilanie awaryjne, klimatyzacja)

1) Wszystkie urządzenia sieci teleinformatycznej muszą być zasilane napięciem o parametrach zgodnych z wymaganiami producenta.
2) Urządzenia sieci teleinformatycznej, od ciągłości pracy których zależne jest realizowanie podstawowych zadań PODMIOTU, muszą być zasilane z gwarantowanych źródeł.
3) Gwarantowane zasilanie uzyskiwane jest przez zastosowanie dywersyfikacji zewnętrznych źródeł energii elektrycznej z samoczynnym załączaniem rezerwy (SZR) lub zastosowanie zasilaczy bezprzerwowych (UPS)lub zastosowanie awaryjnych agregatów prądotwórczych.
4) Elementy systemu zasilania gwarantowanego muszą podlegać okresowym przeglądom i konserwacjom. Szczególną uwagę należy zwrócić na konserwacje akumulatorów i bezwzględne przestrzeganie ich wymiany po okresach eksploatacji przewidzianych w instrukcjach użytkowania.
5) Agregaty prądotwórcze muszą być okresowo uruchamiane i sprawdzana pod kątem poprawności działania Wyniki przeglądów czynności konserwacyjnych muszą być dokumentowane i przedstawiane w formie raportów u ABF/dyrektora PODMIOTU.
6) Agregaty prądotwórcze, o ile są stosowane, muszą posiadać niezbędny zapas paliwa oraz muszą być opracowane procedury uzupełniania paliwa pozwalające na zasilanie z wykorzystaniem tych agregatów do momentu przywrócenia zasilania zewnętrznego. Procedury uzupełniania paliwa określają odrębne przepisy.
7) Jeżeli do prawidłowego działania infrastruktury serwerowej niezbędne jest utrzymanie odpowiednich warunków temperaturowych w pomieszczeniu, w którym znajduje się serwer należy zapewnić klimatyzację.

3.2.2.5 Wymagania dla zabezpieczeń środowiskowych

1) W obszarze zabezpieczeń środowiskowych ADO podejmuje działania zgodnie z przepisami je określającymi, w tym w szczególności przepisami: BHP, PPOŻ.

3.2.3 Identyfikacja obszary i miejsca przetwarzania danych osobowych

1) Wykaz miejsc w których Administrator zezwala na przetwarzanie danych stanowi Załącznik nr 6 Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe niniejszej Polityki powinien uwzględniać między innymi kategorie pomieszczeń wymienionych poniżej:
   a. budynki i pomieszczenia lub części pomieszczeń, w których odbywa się przetwarzanie danych osobowych,
   b. miejsca, w których wykonuje się operacje na danych osobowych (np. wpisywanie, modyfikowanie, kopiowanie),
   c. miejsca, gdzie przechowuje się wszelkie zbiory danych oraz nośniki informacji zawierające dane osobowe takie jak: pokoje z szafami z dokumentacją papierową, z komputerowymi nośnikami informacji, z kopiami zapasowymi danych, ze stacjami komputerowymi, serwerami i innymi urządzeniami komputerowymi, jak np. macierze dyskowe, na których dane osobowe są przetwarzane na bieżąco),
   d. pomieszczenia, gdzie składowane są uszkodzone komputerowe nośniki danych (np. taśmy, dyski, płyty CD, uszkodzone komputery i inne urządzenia z nośnikami zawierającymi dane osobowe),
   e. miejsca w sejfie bankowym, archiwum, itp. jeśli wykorzystywane są one np. do przechowywania elektronicznych nośników informacji zawierających kopie zapasowe danych przetwarzanych w systemie informatycznym, czy też do składowania innych nośników danych, np. dokumentów źródłowych,
   f. w przypadku, gdy dane osobowe przetwarzane są w systemie informatycznym, do którego dostęp poprzez sieć telekomunikacyjną posiada wiele podmiotów, wówczas w wykazie należy umieścić informacje o tych podmiotach (nazwa podmiotu, siedziba, pomieszczenia, w których przetwarzane są dane).

2) Jeżeli PODMIOT posiada system informatyczny (stanowiska komputerowe), do których dostęp z założenia jest dostępem publicznym i nie są one wykorzystywane do przetwarzania danych, w wykazie nie ma konieczności jego wykazywania.

4.3 Techniczne Środki ochrony

1) Wymagania bezpieczeństwa dotyczące systemu informatycznego przetwarzającego dane osobowe:
   a) ASI odpowiedzialny jest za prowadzenie wykazu programów służących do przetwarzania danych osobowych zgodnie z Załącznik nr 11 Wykaz aplikacji zastosowanych do przetwarzania danych osobowych.
   b) Wymagania bezpieczeństwa oraz zasady pracy użytkowników w systemach informatycznych określa Załącznik nr 14 Regulamin użytkownika systemu informatycznego.
   c) Wymagania bezpieczeństwa oraz zasady zarządzania systemami informatycznymi określa instrukcja opisana w Załącznik nr 7 Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych.

5. Naruszenie bezpieczeństwa informacji

1) W celu ustalenia jednolitych zasad postępowania w przypadkach stwierdzenia naruszeń zasad ochrony przetwarzanych danych osobowych wprowadza się :
    a. Zasady zgłaszania zdarzeń związanych z ochroną danych osobowych regulowane są instrukcją opisaną w Załącznik nr 8 Instrukcja zgłaszania incydentów związanych z bezpieczeństwem danych osobowychinformacji.
    b. Zasady obsługi zdarzeń związanych z ochroną danych osobowych reguluje instrukcja opisana w Załącznik nr 9 Procedura zarządzania incydentami bezpieczeństwa informacji.

6. Sprawdzenia i sprawozdawczość dotycząca ochrony bezpieczeństwa informacji

1) Sprawdzenia realizowane są w celu:
    a. zweryfikowania zgodności przetwarzania danych osobowych z PBDO oraz z przepisami o ochronie danych osobowych,
    b. testowania zabezpieczeń, czyli sprawdzanie poprawności funkcjonowania zabezpieczeń np. poprzez:
        i. weryfikację poprawnego działania zabezpieczeń mechanicznych - zamków,
        ii. weryfikację reagowania i zgłaszania alarmów przez systemy alarmowe,
        iii. weryfikację działania systemów kontroli dostępu,
        iv. weryfikacja świadomości pracowników w zakresie ochrony danych osobowych,
        v. weryfikacja stosowania polityki czystego biurka,
        vi. weryfikacja skuteczności działania filtrów stron internetowych,
        vii. weryfikację aktualności sygnatur wirusów w systemach antywirusowych,
    c. pomiar i ocenę skuteczności zabezpieczeń.
2) IOD przygotowuje plan sprawdzeń i przedkłada je do ADO. Plan sprawdzeń tworzony jest z uwzględnieniem wyników wcześniejszych sprawdzeń i innych kontroli w zakresie ochrony informacji, wyników analiz skarg i wniosków oraz zidentyfikowanego ryzyka.
3) Formularz planu sprawdzeń zawiera Załącznik nr 17 Plan Sprawdzeń.
4) IOD w ramach swoich kompetencji może przeprowadzać sprawdzenia z przetwarzania danych.
5) ADO może wskazać i przeprowadzić sprawdzenie przy udziale pracowników jednostki.
6) Osoba przeprowadzająca sprawdzenie przygotowuje sprawozdanie ze sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych:
    a. na podstawie zatwierdzonego planu sprawdzeń, (załącznik nr 17)
    b. doraźnie, jeżeli uzyskał informacje wskazujące na występowania istotnych zagrożeń dla naruszenia ochrony danych osobowych (załącznik 15)
7) Zagadnienia objęte sprawdzeniem są zgodne z zatwierdzonym planem sprawdzeń i w zależności od przedmiotu i zakresu sprawdzenia powinny obejmować:
    a. Zasady przetwarzania danych osobowych (PBDO),
    b. Realizację obowiązków w zakresie udzielania informacji osobom, których dane są przetwarzane,
    c. Zasady przekazywania danych osobowych do państwa trzeciego,
    d. Sposób zabezpieczenia danych osobowych, w szczególności:
        i. Zasady przechowywania danych w formie papierowej oraz elektronicznej,
        ii. Mechanizmy kontroli dostępu do danych osobowych,
        iii. Zastosowane środki ochrony danych osobowych przed ich utratą na skutek awarii systemu informatycznego,

iv. Zastosowane zabezpieczenia przed zagrożeniami pochodzącymi z sieci publicznej,
v. Zastosowane zabezpieczenia przed zagrożeniami pochodzącymi z wewnętrznej sieci, w tym rozliczalności wykonanych operacji,
vi. Środki zapewniające poufność danych osobowych przy ich przesyłaniu w sieci publicznej oraz lokalnych urządzeń bezprzewodowych,
vii. Środki zapewniające poufność danych przetwarzanych przy wykorzystaniu elektronicznych przenośnych nośników informacji,
viii. Sposób zabezpieczenia danych przez podmiot, któremu dane zostały powierzone.

8) Osoba przeprowadzająca sprawdzenie ustala stan faktyczny na podstawie dowodów zebranych w toku sprawdzenia. Dowodami mogą być w szczególności dokumenty, oględziny, pisemne lub ustne wyjaśniania (osoba przeprowadzająca sprawdzenie może żądać udzielenia w wyznaczonym terminie ustnych lub pisemnych wyjaśnień) oraz utrwalone stany konfiguracji technicznych zabezpieczeń.
9) Wzór sprawozdania, o którym mowa w pkt. 1 zawiera załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych.
10) Zatwierdzone przez ADO sprawozdania przechowywane są zgodnie z przyjętym Jednolitym Rzeczowym Wykazem Akt.

7. Załączniki

7.1 Załącznik nr 1 Zobowiązanie do zachowania w poufności informacji

7.2 Załącznik nr 2 Upoważnienie do przetwarzania danych osobowych

7.3 Załącznik nr 3 Rejestr czynności przetwarzania

7.4 Załącznik nr 4 Wzory obowiązków informacyjnych

7.5 Załącznik nr 5 Wykaz stref bezpiecznych

7.6 Załącznik nr 6 Wykaz budynków, pomieszczeń lub części pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

7.7 Załącznik nr 7 Instrukcja Zarządzania Systemem Informatycznym służącym do przetwarzania danych osobowych

7.8 Załącznik nr 8 Instrukcja zgłaszania incydentów związanych z bezpieczeństwem danych osobowych

7.9 Załącznik nr 9 Procedura zarządzania incydentami bezpieczeństwa informacji

7.10 Załącznik nr 10 Instrukcja wydawania i zdawania kluczy do pomieszczeń

7.11 Załącznik nr 11 Wykaz aplikacji zastosowanych do przetwarzania danych osobowych

7.12 Załącznik nr 12 Wzór umowy powierzenia przetwarzania danych osobowych

7.13 Załącznik nr 13 Rejestr udostępnień

7.14 Załącznik nr 14 Regulamin użytkownika systemu informatycznego

7.15 Załącznik nr 15 Sprawozdanie ze sprawdzenia przestrzegania przepisów o ochronie danych osobowych

7.16 Załącznik nr 16 Inwentaryzacja zasobów

7.17 Załącznik nr 17 Plan Sprawdzeń

7.18 Załącznik nr 18 Procedura realizacji praw osób których dane dotyczą

7.19 Załącznik nr 19 Procedura zarządzania systemem monitoringu wizyjnego

7.20 Załącznik nr 20 Rejestr upoważnień