# ZARZĄDZENIE NR 4/2023

## DYREKTORA GMINNEJ BIBLIOTEKI PUBLICZNEJ W LESZNOWOLI

**z dnia 4 kwietnia 2023 r.**

**w sprawie wprowadzenia Polityki Bezpieczeństwa Danych Osobowych**

**w Gminnej Bibliotece Publicznej w Lesznowoli**

Na podstawie Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE oraz rozporządzenia 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 ze zm.) zarządza się, co następuje:

§ 1

W Gminnej Bibliotece Publicznej w Lesznowoli, w celu utrzymania podstawowych atrybutów bezpieczeństwa danych osobowych, w szczególności ich poufności, dostępności i integralności wdraża się do stosowania Politykę Bezpieczeństwa Danych Osobowych.

§ 2

Na dokumentację Polityki Bezpieczeństwa Danych Osobowych (PBDO) składają się aktualizowane procedury, wykazy, polityki i instrukcje, gwarantujące poufność, dostępność i integralność przetwarzanych w Bibliotece danych osobowych.

§ 3

Zobowiązuję wszystkich pracowników Biblioteki do zapoznania się z zapisami PBDO oraz realizacji wynikających z niej zasad i obowiązków.

§ 4

Nadzór nad stosowaniem Polityki Bezpieczeństwa Danych Osobowych powierzam Inspektorowi ochrony danych.

§ 5

Traci moc Zarządzenie Nr 8/2018 p.o. Dyrektora Gminnej Biblioteki Publicznej w Lesznowoli z dnia 05-05-2018 r. w sprawie wdrożenia dokumentacji ochrony danych osobowych.

§ 6

Zarządzenie wchodzi w życie z dniem podpisania.

z up. DYREKTORA
Joanna Konofalska

Za zgodność z przedłożonym dokumentem / oryginałem

Katarzyna Papiernik
Specjalista ds. Kadr i Płac

Gminna Biblioteka Publiczna
w Lesznowoli

# POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

## Praktyczne zasady zabezpieczania danych osobowych

## w Gminnej Bibliotece Publicznej w Lesznowoli

Zatwierdzam

GMINNA BIBLIOTEKA PUBLICZNA
W LESZNOWOLI
ul. Lipowa 28, 05-506 Magdalenka
tel./fax: 22 736-19-34, NIP: 123-09-78-483

4.04.2023 r.

z up. DYREKTORA
Joanna Konofalska

.....
(data i podpis Administratora)

Za zgodność z przedłożonym
~~dokumentem~~ / oryginałem

Katarzyna Papiernik
Specjalista ds. Kadr i Płac

# Spis treści


1 Wprowadzenie ..... 3
2 Wymagania bezpieczeństwa danych osobowych ..... 3
3 Definicje ..... 4
4 Polityki bezpieczeństwa danych osobowych ..... 5
5 Organizacja nadzoru bezpieczeństwa danych osobowych ..... 6
6 Urządzenia mobilne, nośniki danych, praca zdalna ..... 6
7 Bezpieczeństwo osobowe ..... 6
8 Rejestr czynności przetwarzania danych osobowych ..... 7
9 Kontrola dostępu ..... 7
10 Bezpieczeństwo fizyczne ..... 7
11 Ochrona przed szkodliwym oprogramowaniem ..... 8
12 Kopie zapasowe ..... 8
13 Bezpieczeństwo komunikacji ..... 8
14 Relacje z podmiotami zewnętrznymi ..... 8
15 Zarządzanie incydentami związanymi z bezpieczeństwem danych osobowych ..... 8
16 Ochrona prywatności i informacji identyfikujących osoby ..... 9
17 Przeglądy bezpieczeństwa ..... 9
18 Załączniki i dokumenty związane, zgodnie z obszarami PBDO: ..... 9

# 1. Wprowadzenie

## 1.1. Deklaracja i zakres stosowania

1.1.1. Celem niniejszej Polityki bezpieczeństwa danych osobowych (PBDO) jest wypełnienie założeń Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 roku 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, dalej też zwane RODO).

1.1.2. Bezpieczeństwo danych osobowych osiąga się poprzez wdrożenie odpowiedniego zbioru zabezpieczeń, w tym polityk, procesów, procedur, struktur organizacyjnych oraz funkcji realizowanych przez oprogramowanie i urządzenia. Zaleca się, aby te zabezpieczenia były ustanawiane, wdrażane, monitorowane, weryfikowane i w miarę potrzeby ulepszane tak, aby zapewniały spełnienie poszczególnych celów związanych z bezpieczeństwem danych osobowych wynikających z działalności Biblioteki, jako Administratora danych osobowych.

1.1.3. Bezpieczeństwo osiągane za pomocą środków technicznych jest wspierane poprzez odpowiednie zarządzanie i procedury. Skuteczność PBDO wymaga wsparcia ze strony wszystkich pracowników i współpracowników Biblioteki. Wymaga się także współpracy oraz stosowania się do niniejszej Polityki bezpieczeństwa dostawców i innych podmiotów zewnętrznych dopuszczanych do chronionych informacji w Bibliotece.

1.1.4. Zasady, działania, kompetencje i zakresy odpowiedzialności obowiązują wszystkich pracowników i współpracowników Biblioteki.

1.1.5. Procedury i dokumenty związane z PBDO są regularnie weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa.

1.1.6. PBDO określa środki techniczne i organizacyjne stosowane u Administratora dla zapewnienia ochrony danych oraz tryb postępowania w przypadku stwierdzenia naruszenia zabezpieczenia danych w systemie informatycznym lub w kartotekach, albo w sytuacji podejrzenia o takim naruszeniu.

1.1.7. Polityka bezpieczeństwa jest opracowana z uwzględnieniem metod i środków ochrony danych, których skuteczność w czasie ich zastosowania jest powszechnie uznawana. Za priorytet uznano zagwarantowanie zgromadzonym danym osobowym, przez cały okres ich przetwarzania charakteru poufnego wraz z zachowaniem ich integralności i rozliczalności, ze szczególnym uwzględnieniem obowiązujących przepisów prawa dotyczących ochrony danych osobowych.

# 2 Wymagania bezpieczeństwa danych osobowych

2.1. Źródła wymagań związanych z bezpieczeństwem danych osobowych:

2.1.1. Szacowanie ryzyka dla ochrony danych osobowych i skutków dla osób, których dane dotyczą. Dzięki szacowaniu ryzyka można zidentyfikować zagrożenia dla aktywów, ocenić podatność na zagrożenia i prawdopodobieństwo ich wystąpienia oraz minimalizować potencjalne skutki. Polityka zarządzania ryzykiem stanowi załącznik do niniejszej Polityki.

2.1.2. Polityka Bezpieczeństwa Danych Osobowych opiera się na następujących niezaprzeczalnych zasadach ochrony danych:

2.1.3. Zasada znajomości wymagań PBDO. Każdy pracownik lub współpracownik Administratora powinien zostać zapoznany z regułami oraz z kompletnymi i aktualnymi procedurami ochrony danych i podpisać stosowne oświadczenie o zapoznaniu się z zasadami obowiązującej Polityki;

2.1.4. Zasada uprawnionego dostępu. Każdy pracownik lub współpracownik Administratora stosuje się do obowiązujących zasad ochrony danych, spełnia kryteria dopuszczenia do przetwarzania danych osobowych;

2.1.5. Zasada przywilejów koniecznych. Każdy pracownik lub współpracownik Administratora posiada prawa dostępu do danych osobowych, ograniczone wyłącznie do tych, które są konieczne do wykonywania powierzonych mu zadań;

2.1.6. Zasada wiedzy koniecznej. Każdy pracownik lub współpracownik Administratora posiada wiedzę o systemie, do którego ma dostęp, ograniczoną wyłącznie do zagadnień, które są konieczne do realizacji powierzonych mu zadań;

2.1.7. Zasada usług koniecznych. Systemy informacyjne służą świadczeniu tylko takich usług, które są konieczne do realizacji zadań Biblioteki, jako Administratora;

2.1.8. Zasada świadomości zbiorowej. Wszyscy pracownicy lub współpracownicy są świadomi konieczności ochrony zasobów informacyjnych i aktywnie uczestniczą w tym procesie;

2.1.9. Zasada indywidualnej odpowiedzialności. Za bezpieczeństwo poszczególnych elementów danego systemu odpowiadają konkretne osoby;

2.1.10. Zasada obecności koniecznej. Prawo przebywania w określonych miejscach mają tylko osoby do tego upoważnione;

2.1.11. Zasada stałej gotowości. System jest przygotowany na wszelkie zagrożenia. Niedopuszczalne jest tymczasowe wyłączanie mechanizmów zabezpieczających;

2.1.12. Zasada kompletności. Skuteczne zabezpieczenie jest tylko wtedy, gdy stosuje się podejście kompleksowe, uwzględniające wszystkie stopnie i ogniwa ogólnie pojętego procesu przetwarzania danych osobowych;

2.1.13. Zasada odpowiedniości. Używane mechanizmy muszą być adekwatne do sytuacji;

2.1.14. Zasada świadomej konwersacji. Nie zawsze i wszędzie trzeba mówić o tym, co się wie, ale zawsze i wszędzie trzeba wiedzieć co, gdzie i do kogo się mówi.

## 3 Definicje

**Administrator** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych. Administratorem jest Gminna Biblioteka Publiczna w Lesznowoli z siedzibą główną w Magdalence, reprezentowana przez Dyrektora (dalej również jako ADO – Administrator danych osobowych).

**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;

**dostępność** – właściwość bycia dostępnym i użytecznym na żądanie upoważnionego podmiotu.

**rozliczalność** – rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi;

**uwierzytelnienie** - uwiarygodnienie swojej tożsamości względem systemu teleinformatycznego;

**poufność** – właściwość polegająca na tym, że dane osobowe nie są udostępniane lub wyjawiane nieupoważnionym osobom, podmiotom lub procesom.

**integralność** – właściwość polegająca na zapewnieniu dokładności i kompletności danych osobowych.

**integralność systemu** – rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej jak i przypadkowej.

**bezpieczeństwo informacji** – zachowanie poufności, integralności i dostępności informacji; dodatkowo, mogą być brane pod uwagę inne własności, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność.

**ryzyko** – niepewność osiągnięcia zamierzonych celów.

**szacowanie ryzyka** – proces identyfikowania, analizowania i oceniania ryzyka.

**postępowanie z ryzykiem** – proces planowania i wdrażania działań wpływających na ryzyko.

**incydent bezpieczeństwa informacji** – zdarzenie albo seria niepożądanych lub niespodziewanych zdarzeń bezpieczeństwa informacji stwarzających znaczne prawdopodobieństwo zakłócenia działań biznesowych i zagrożenia bezpieczeństwa informacji.

**Inspektor ochrony danych** (IOD) – osoba nadzorująca przestrzeganie zasad i przepisów ochrony danych osobowych, wyznaczona przez Zarząd, w rozumieniu art. 37 RODO

**Administrator systemu informatycznego** (ASI) – osoba odpowiadająca za ciągłość pracy systemów informatycznych Administratora.

**Teczka ODO** – zbiór dokumentów, instrukcji, regulaminów, załączników opisujących sposób przetwarzania i ochrony danych, składający się na politykę ochrony danych osobowych, gromadzonych i nadzorowanych przez ADO.

# 4 Polityki bezpieczeństwa danych osobowych

4.1. Zbiór polityk bezpieczeństwa danych osobowych, zatwierdzony przez ADO, jest opublikowany i zakomunikowany pracownikom, współpracownikom i właściwym stronom zewnętrznym.

Politykę bezpieczeństwa danych osobowych wspierają różne polityki tematyczne, wymagające wdrożenia zabezpieczeń w określonych obszarach.

Do takich obszarów polityki należą:

1. kontrola dostępu;
2. bezpieczeństwo fizyczne i środowiskowe;
3. obszary związane z użytkownikiem końcowym, takie jak:
   - 3.1. polityka czystego biurka i czystego ekranu;
   - 3.2. przekazywanie danych osobowych;
   - 3.3. urządzenia mobilne;
   - 3.4. ograniczenia dotyczące instalacji i stosowania oprogramowania;
4. kopie zapasowe;
5. ochrona przed szkodliwym oprogramowaniem;
6. zarządzanie podatnościami technicznymi;
7. bezpieczeństwo komunikacji;
8. ochrona prywatności i informacji identyfikujących osoby (procedury realizacji praw osób, których dane dotyczą);

10 relacja z dostawcami, a w tym:

11. rejestr czynności przetwarzania danych
12. dokumentacja naruszeń ochrony danych naruszeń ochrony danych;
13. dokumentacja oceny skutków przetwarzania danych;
14. klauzule informacyjne (realizacja obowiązku informacyjnego);

15. klauzule zgody na przetwarzanie danych osobowych (mechanizmy i sposoby dokumentowania zgód na przetwarzanie danych osobowych);

16. polityka retencji danych;

17. zasady monitorowania ochrony danych (plany kontroli i audytów wewnętrznych).

Zaleca się udostępnienie tych polityk pracownikom oraz odpowiednim podmiotom zewnętrznym, uprawnionym i odpowiedzialnym za przetwarzanie danych osobowych w określonych procesach, w formie właściwej, dostępnej i zrozumiałej dla czytelników, do których jest adresowana, np. w formie szkoleń i warsztatów w zakresie bezpieczeństwa danych osobowych.

4.2. Polityki i procedury bezpieczeństwa informacji są wydane jako zestaw oddzielnych, ale powiązanych, dokumentów.

# 5 Organizacja nadzoru bezpieczeństwa danych osobowych

5.1 Za rozwój i nadzór PBDO oraz wsparcie w określaniu zabezpieczeń odpowiada wyznaczony przez ADO Inspektor ochrony danych.

# 6 Urządzenia mobilne, nośniki danych, praca zdalna

W przypadku stosowania urządzeń mobilnych zaleca się zwrócenie szczególnej uwagi na to, aby nie naruszyć ochrony danych osobowych. Zaleca się, aby polityka stosowania urządzeń mobilnych, regulamin pracy zdalnej, regulamin informatyczny uwzględniały ryzyko związane z pracą na mobilnych urządzeniach w niechronionych środowiskach. Należy zapewnić bezpieczeństwo stosowania urządzeń mobilnych. Zapobiec nieuprawnionemu ujawnieniu, modyfikacji, usunięciu lub zniszczeniu danych osobowych zapisanych na nośnikach

# 7 Bezpieczeństwo osobowe

## 7.1 Przed zatrudnieniem

Należy zapewnić, żeby pracownicy, współpracownicy i kontrahenci rozumieli swoją odpowiedzialność i byli odpowiednimi kandydatami do wypełnienia ról, do których są przewidziani.

## 7.2 Podczas zatrudnienia

7.2.1 Należy zapewnić, żeby pracownicy, współpracownicy i kontrahenci byli świadomi swoich obowiązków dotyczących bezpieczeństwa danych osobowych i wypełniali je. Kontrahenci, jako podmiot przetwarzający dane na zlecenie administratora oraz każda osoba działająca z upoważnienia administratora i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie Administratora.

Wzór upoważnienia do przetwarzania danych stanowi załącznik do niniejszej Polityki.

7.2.2. ADO wymaga i zapewnienia, że pracownicy, współpracownicy oraz kontrahenci:

1. są odpowiednio wprowadzani w swoje obowiązki i odpowiedzialność związaną z bezpieczeństwem danych osobowych przed przyznaniem im dostępu do chronionych informacji lub systemów informacyjnych;
2. otrzymują wytyczne określające wymagania w zakresie PBDO związane z ich obowiązkami w organizacji;
3. dbają o odpowiednie umiejętności i kwalifikacje i są na bieżąco szkoleni;
4. mają możliwość zgłaszania naruszeń polityki bezpieczeństwa lub procedur.

7.2.3 Uświadamianie, kształcenie i szkolenia z zakresu ochrony danych osobowych

Zaleca się, aby wszyscy pracownicy, współpracownicy oraz, w stosownych wypadkach, kontrahenci, przeszli stosowne kształcenie i szkolenie uświadamiające oraz regularnie otrzymywali aktualizacje polityk i procedur związanych z ich stanowiskiem pracy.

7.2.4 Postępowanie dyscyplinarne

Zaleca się, aby postępowania dyscyplinarne wobec pracowników naruszających zasady PBDO były prowadzone na podstawie ustalonych i przedstawionych im zasad.

Zaleca się, aby postępowania dyscyplinarnego nie rozpoczynać bez uprzedniej weryfikacji potwierdzającej, że nastąpiło naruszenie bezpieczeństwa danych osobowych.

### 7.3. Zakończenie i zmiana zatrudnienia, współpracy

Zaleca się określenie i przedstawienie pracownikowi, współpracownikowi lub kontrahentowi, które odpowiedzialności i obowiązki w zakresie PBDO pozostaną aktualne po zakończeniu lub zmianie zatrudnienia, a następnie ich egzekwowanie. Zobowiązanie do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia, również po ustaniu zatrudnienia/współpracy.

## 8 Rejestr czynności przetwarzania danych osobowych

Prowadzony jest rejestr czynności przetwarzania danych osobowych zgodnie ze wzorem stanowiącym załącznik do niniejszej Polityki

## 9 Kontrola dostępu

9.1 Zaleca się zapewnienie użytkownikom dostępu wyłącznie do tych sieci i usług sieciowych, do których otrzymali wyraźne uprawnienia.
9.2 W celu umożliwienia przydzielania praw dostępu zaleca się wdrożenie formalnego procesu rejestrowania i wyrejestrowywania użytkowników.

Ewidencja osób upoważnionych do przetwarzania danych osobowych stanowi załącznik do PBDO.

9.3 Zaleca się, aby po zakończeniu zatrudnienia, umowy lub porozumienia przydzielone pracownikom i użytkownikom zewnętrznym prawa dostępu do danych osobowych i środków ich przetwarzania były odbierane, lub dostosowywane do zaistniałych zmian.

9.3 Tam, gdzie polityka kontroli dostępu tego wymaga, zaleca się kontrolowanie dostępu do systemów i aplikacji przez procedurę bezpiecznego logowania.
Zaleca się, aby systemy zarządzania hasłami były interaktywne i zapewniały wybór haseł dobrej jakości.

## 10 Bezpieczeństwo fizyczne

10.1 Zaleca się ochronę pomieszczeń stanowiących obszar przetwarzania danych przez odpowiednie zabezpieczenia wejść zapewniające dostęp wyłącznie osobom uprawnionym.

Ewidencja przydziału kluczy stanowi załącznik do PBDO

10.2 Zaleca się umieszczenie i ochronę sprzętu służącego do przetwarzania danych w taki sposób, aby zredukować ryzyka wynikające z zagrożeń i niebezpieczeństw środowiskowych oraz okazje do nieuprawnionego dostępu.

10.3 Polityka czystego biurka i czystego ekranu

Polityka czystego biurka dla dokumentów papierowych i przenośnych nośników pamięci oraz polityki czystego ekranu dla środków przetwarzania danych osobowych stanowi załącznik do niniejszej Polityki.

## 11 Ochrona przed szkodliwym oprogramowaniem

Zaleca się wdrożenie zabezpieczeń wykrywających, zapobiegających i odtwarzających, które służą ochronie przed szkodliwym oprogramowaniem, w połączeniu z właściwym uświadamianiem użytkowników.

Regulamin informatyczny określający zasady korzystania z aktywów informatycznych tj. Internetu, poczty elektronicznej, komputerów, stanowi załącznik do niniejszej Polityki

## 12 Kopie zapasowe

Zaleca się regularne wykonywanie i testowanie zapasowych kopii informacji, oprogramowania i obrazów systemów zgodnie z ustaloną polityką kopii zapasowych.

## 13 Bezpieczeństwo komunikacji

13.1 Zaleca się, aby sieci były zarządzane i nadzorowane w celu ochrony informacji w systemach i aplikacjach.

13.2 Utrzymać bezpieczeństwo danych osobowych przesyłanych wewnątrz organizacji i wymienianych z podmiotami zewnętrznymi.

## 14 Relacje z podmiotami zewnętrznymi

14.1 Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi bezpieczeństwa i chroniło prawa osób, których dane dotyczą.

Polityka korzystania z usług podmiotów zewnętrznych stanowi załącznik do PBDO.

14.2 Zaleca się, aby regularnie monitorowano, przeglądano i audytowano dostarczanie usług zewnętrznych.

14.3 Rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu innych administratorów - W przypadku przetwarzania danych osobowych powierzonych przez innych administratorów prowadzony jest rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora.

## 15 Zarządzanie incydentami związanymi z bezpieczeństwem danych osobowych

15.1 Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu - W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu, 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.

15.2. Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu (zgodnie z procedurą postępowania w przypadku naruszenia ochrony danych osobowych)

15.3. Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych stanowi załącznik do niniejszej Polityki.

## 16 Ochrona prywatności i informacji identyfikujących osoby

16.1 Zasady dotyczące przetwarzania danych osobowych

Dane osobowe muszą być:

16.1.1 przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość");

16.1.2 zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami; („ograniczenie celu");

16.1.3 adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych");

16.1.4 prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość");

16.1.5 przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania");

16.1.6 przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

## 17 Przeglądy bezpieczeństwa

Procedury i dokumenty związane z PBDO będą weryfikowane i dostosowywane w celu zapewnienia odpowiedniego poziomu bezpieczeństwa. Przeglądy dokumentacji powinny odbywać się nie rzadziej niż raz w roku.

## 18 Załączniki i dokumenty związane, zgodnie z obszarami PBDO:

I. **Organizacja i nadzór bezpieczeństwa danych osobowych**
   1. Wyznaczenie IOD;

II. **Bezpieczeństwo IT**
   2. Regulamin informatyczny (Zasady korzystania z Internetu, poczty elektronicznej, komputerów stacjonarnych i przenośnych);
   3. Wykaz kluczowych aplikacji;

III. **Bezpieczeństwo osobowe**
   4. Upoważnienia do przetwarzania danych osobowych;
   5. Karta szkolenia wstępnego;
   6. Ewidencja osób upoważnionych do przetwarzania danych osobowych

IV. **Czynności przetwarzania danych**
   7. Rejestr czynności przetwarzania danych osobowych;

V. **Bezpieczeństwo fizyczne**
   8. Polityka czystego biurka i ekranu;
   9. Wykaz pomieszczeń i zastosowane fizyczne środki ochrony danych;
   10. Ewidencja przydziału kluczy;

VI. **Podmioty zewnętrzne**
   11. Polityka korzystania z usług podmiotów przetwarzających;

VII. **Zarządzanie incydentami**
   12. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych;

VIII. **Prawa podmiotów danych**
   13. Polityka prywatności;

IX. **Przeglądy bezpieczeństwa**
   14. Polityka zarządzania ryzykiem w obszarze ochrony danych osobowych;
   15. Arkusze weryfikacji zgodności z RODO;

Przedstawione powyżej dokumenty wewnętrzne nie stanowią katalogu zamkniętego dokumentacji składającej się na Politykę bezpieczeństwa danych osobowych. Każda dodatkowa, nowa procedura, instrukcja czy wytyczna ADO dotycząca obszaru ochrony danych osobowych stanowi integralną część niniejszej Polityki, a ich dodanie nie wymaga zmiany niniejszego dokumentu PBDO.

Wypełnione załączniki przechowywane są w Teczce Ochrony Danych Osobowych.