

Zarządzenie nr 8 /2025

Dyrektora Gminnej Biblioteki Publicznej w Słupnie

z dnia 17. 11. 2025 r.

w sprawie wprowadzenia Polityki Bezpieczeństwa Przetwarzania Danych

Osobowych w Gminnej Bibliotece Publicznej w Słupnie

Na podstawie art. 24 ust. 2 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 (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE. L Nr 119, str. 1 ze zm.) zarządzam, co następuje:

§ 1. Wprowadzam Politykę Bezpieczeństwa Przetwarzania Danych Osobowych w Gminnej Bibliotece Publicznej w Słupnie, która stanowi załącznik do niniejszego zarządzenia.

§ 2. Traci moc zarządzenie nr 5/2018 Dyrektora Gminnej Biblioteki Publicznej w Słupnie z dnia 25.05.2018 r. w sprawie wprowadzania zaktualizowanej Polityki Bezpieczeństwa Informacji oraz Instrukcji Zarządzania Systemami Komputerowymi oraz zarządzenie nr 9/2018 Dyrektora Gminnej Biblioteki Publicznej w Słupnie z dnia 27.12.2018r. w sprawie wprowadzania zmian do Polityki Bezpieczeństwa Informacji.

§ 3. Zarządzenie wchodzi w życie z dniem podpisania.

DYREKTOR BIBLIOTEKI

B. Hermik
Bożena Wernik

GMINNA BIBLIOTEKA PUBLICZNA
w Słupnie
09-472 Słupno, ul. Warszawska 26
Regon 000961716, NIP 774-28-99-330
tel. 24 266-72-80

Załącznik do Zarządzenia nr 8/2025 z dnia 17.11.2025r.
Dyrektora Gminnej Biblioteki Publicznej w Słupnie
w sprawie wprowadzenia Polityki Bezpieczeństwa
Przetwarzania Danych Osobowych

Polityka bezpieczeństwa przetwarzania danych osobowych w Gminnej Bibliotece Publicznej w Słupnie

SPIS TREŚCI

ROZDZIAŁ I. WPROWADZENIE I CEL

§ 1 Postanowienia ogólne

ROZDZIAŁ II. PODSTAWY PRAWNE

§ 2 Zakres regulacji

§ 3 Definicje

ROZDZIAŁ III. NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

§ 4 Zasady ochrony danych osobowych

§ 5 Przetwarzanie przez Administratora

ROZDZIAŁ IV. PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH I ICH OBOWIĄZKI

§ 6 Inspektor Ochrony Danych

§ 7 Osoby upoważnione

§ 8 Podmioty przetwarzające

§ 9 Odbiorcy danych osobowych

ROZDZIAŁ V. PRZETWARZANIE DANYCH

§ 10 Przestanki legalności przetwarzania danych

§ 11 Przetwarzanie danych na podstawie zgody

§ 12 Minimalizacja danych

§ 13 Przekazywanie danych osobowych do państw trzecich lub organizacji międzynarodowych

§ 14 Obowiązki informacyjne przy przetwarzaniu danych

ROZDZIAŁ VI. UPRAWNIENIA OSÓB FIZYCZNYCH

§ 15 Rodzaje uprawnień osób fizycznych

§ 16 Realizacja żądań

§ 17 Procedura realizacji żądań podmiotów danych

§ 18 Obowiązki administratora danych

§ 19 Obowiązki osób przetwarzających dane osobowe

ROZDZIAŁ VII. SYSTEM OCHRONY DANYCH OSOBOWYCH

§ 20 Polityka czystego biurka

§ 21 Polityka czystego ekranu

§ 22 Oprogramowanie

§ 23 Poczta elektroniczna

§ 24 Urządzenia i nośniki

§ 25 Prowadzenie rejestru czynności przetwarzania danych osobowych

§ 26 Zarządzanie ryzykiem

§ 27 Ocena skutków dla ochrony danych osobowych

§ 28 Uprzednie konsultacje z PUODO

§ 29 Privacy by design i privacy by default

§ 30 Inwentaryzacja

§ 31 Zbieranie danych osobowych

ROZDZIAŁ VIII. ZAGROŻENIA BEZPIECZEŃSTW

- § 32 Charakterystyka możliwych zagrożeń
- § 33 Sytuacje świadczące o naruszeniu zasad bezpieczeństwa
- § 34 Tabele form naruszenia bezpieczeństwa i sposoby postępowania
- § 35 Postępowanie w przypadku podejrzenia naruszenia lub naruszenia ochrony danych osobowych
- § 36 Postępowanie w przypadku otrzymania od podmiotu przetwarzającego zawiadomienia o podejrzeniu naruszenia lub naruszeniu ochrony danych osobowych
- § 37 Działania podejmowane po usunięciu lub zminimalizowaniu skutków naruszenia
- § 38 Zawiadamianie o naruszeniu ochrony danych osobowych
- § 39 Ocena konieczności zawiadomienia PUODO o naruszeniu
- § 40 Ocena konieczności zawiadomienia podmiotu danych o naruszeniu
- § 41 Zawiadamianie PUODO o naruszeniu
- § 42 Zawiadamianie podmiotów danych o naruszeniu

ROZDZIAŁ IX. PROCEDURY I ŚRODKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

- § 43 Zakres i cel
- § 44 Deklaracja
- § 45 Charakterystyka instytucji
- § 46 Wykaz miejsc przetwarzania
- § 47 Ewidencja osób upoważnionych do przetwarzania danych osobowych
- § 48 Środki organizacyjne i techniczne ochrony danych

ROZDZIAŁ X. INSTRUKCJA ZARZĄDZANIA SYTEMEM INFORATYCZNYM

- § 49 Charakterystyka systemu
- § 50 Ogólne zasady pracy w systemie informatycznym
- § 51 Procedury nadawania uprawnień do przetwarzania danych i rejestrowania tych uprawnień w systemie informatycznym oraz wskazanie osoby odpowiedzialnej za te czynności
- § 52 Stosowane metody i środki uwierzytelnienia oraz procedury związane z ich zarządzaniem i użytkowaniem
- § 53 Procedury rozpoczęcia, zawieszenia i zakończenia pracy
- § 54 Procedury tworzenia kopii awaryjnych zbiorów danych oraz programów i narzędzi programowych służących do ich przetwarzania
- § 55 Sposób, miejsce i okres przechowywania elektronicznych nośników informacji
- § 56 Sposób zabezpieczenia systemu przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego
- § 57 Informacje o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia
- § 58 Przesyłanie danych poza obszar przetwarzania
- § 59 Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych
- § 60 Postanowienia końcowe

RODZIAŁ I

WPROWADZENIE I CEL

§ 1

POSTANOWIENIA OGÓLNE

Niniejszy dokument zatytułowany „Polityka bezpieczeństwa przetwarzania danych osobowych” (dalej jako Polityka) stanowi mapę wymogów, zasad i regulacji ochrony danych osobowych w Gminnej Bibliotece Publicznej w Słupnie.

Niniejsza Polityka jest polityką ochrony danych osobowych w rozumieniu RODO - rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).

Polityka stanowi część składową systemu ochrony danych osobowych obowiązującego u Administratora Danych Osobowych, określając w szczególności:

- a) zasady przetwarzania danych osobowych u Administratora Danych Osobowych;
- b) zasady zapewniania ochrony przetwarzanych danych osobowych;
- c) procedury stosowane u Administratora Danych Osobowych;
- d) wzorce dokumentów i formularzy stosowanych przez Administratora Danych Osobowych.

Jest to najwyższej rangi dokument Ochrony Danych Osobowych w Gminnej Bibliotece Publicznej w Słupnie.

Niniejsza Polityka jest środkiem prawnym przewidzianym w art. 24 ust. 2 RODO.

Celem dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich ochrony w Gminnej Bibliotece Publicznej w Słupnie.

W celu zwiększenia świadomości obowiązków i odpowiedzialności pracowników, a tym samym skuteczności ochrony przetwarzanych zasobów, w dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz scharakteryzowano zagrożenia bezpieczeństwa, podając jednocześnie schematy postępowań na wypadek wystąpienia naruszenia bezpieczeństwa.

Dokument szczegółowo opisuje podstawowe zasady organizacji pracy przy danych osobowych.

Wszelkie zestawienia oraz informacje uzupełniające jego treść zebrano w formie załączników i dokumentów towarzyszących, stanowiących integralną część systemu ochrony danych osobowych funkcjonującego w jednostce.

ROZDZIAŁ II

PODSTAWY PRAWNE

§ 2

ZAKRES REGULACJI

Przepisy ochrony danych osobowych zawarte są w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) oraz ustawie o ochronie danych osobowych z dnia 10 maja 2018 r. (Dz.U. z 2019 r. poz. 1781) oraz wydanych do niej aktach wykonawczych, wytycznych i rekomendacji Urzędu Ochrony Danych Osobowych.

§ 3

DEFINICJE

W dokumencie przyjmuje się następującą terminologię:

1. Administrator Danych Osobowych – Gminna Biblioteka Publiczna w Słupnie, ul. Warszawska 26, 09-472 Słupno.
2. Administrator Systemów Informatycznych - osoba wyznaczona przez Administratora Danych Osobowych, odpowiedzialna za funkcjonowanie i bezpieczeństwo systemów informatycznych.
3. Polityka oznacza niniejszą Politykę bezpieczeństwa przetwarzanych danych osobowych, o ile co innego nie wynika wyraźnie z kontekstu.
4. RODO oznacza rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27.04.2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz.Urz. UE L 119, s. 1).
5. Dane niezidentyfikowane - Dane osobowe, których Administrator Danych Osobowych nie identyfikuje w odniesieniu do konkretnych podmiotów danych (np. zapis z monitoringu, korespondencja e-mailowa zawierająca dane osób trzecich).

6. Dane osobowe - wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; 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.

7. Dane dzieci - dane osobowe osób fizycznych poniżej 16 roku życia.

8. Dane karne - dane osobowe dotyczące wyroków skazujących i czynów zabronionych lub powiązanych środków bezpieczeństwa.

9. Dane szczególne - dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych; dane genetyczne; dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej; dane dotyczące zdrowia, seksualności lub orientacji seksualnej osoby fizycznej.

10. Dostępność - zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, kiedy jest to potrzebne.

11. Incydent - zdarzenie mogące wpłynąć na bezpieczeństwo danych osobowych w zakresie dostępności, integralności, poufności lub odporności systemów i usług przetwarzania. Incydent może prowadzić do naruszenia ochrony danych osobowych, ale nie musi.

12. Integralność - zapewnienie dokładności i kompletności informacji oraz metod przetwarzania.

13. Naruszenie ochrony danych osobowych - naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

14. Odbiorca danych osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną (osobą) trzecią. Nie uznaje się za odbiorców organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii Europejskiej lub prawem państwa członkowskiego.

15. Odporność - zdolność systemów informatycznych do prawidłowego funkcjonowania mimo dużego obciążenia.

16. Osoba upoważniona - osoba upoważniona przez Administratora Danych Osobowych do przetwarzania danych osobowych w określonym przez niego zakresie.
17. Państwo trzecie - państwo nienależące do Unii Europejskiej oraz Europejskiego Obszaru Gospodarczego.
18. Podmiot danych - osoba fizyczna, której dane osobowe dotyczą.
19. Podmiot przetwarzający osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora.
20. Poufność - zapewnienie, że dane osobowe są dostępne jedynie dla osób upoważnionych.
21. Profilowanie - dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
22. Przetwarzanie danych osobowych - operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.
23. Rozliczalność danych - rozumie się przez to właściwość zapewniającą, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi.
24. Pseudonimizacja - przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem, że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
25. Strona (osoba) trzecia - osoba fizyczna lub prawna, organ publiczny, jednostka lub podmiot inny niż:
- a) osoba, której dane dotyczą;
 - b) Administrator Danych Osobowych i współadministrator danych osobowych;
 - c) podmiot przetwarzający;
 - d) osoba upoważniona.

26. System informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
27. System ochrony danych osobowych - całokształt środków technicznych, organizacyjnych i prawnych wraz z niezbędną dokumentacją, wdrożonych przez Administratora Danych Osobowych, służących zapewnieniu, że przetwarzanie danych osobowych będzie odbywało się zgodnie z przepisami z zakresu ochrony danych osobowych.
28. Współadministrator danych osobowych - osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który wspólnie z Administratorem Danych Osobowych decyduje o celach i sposobach przetwarzania danych osobowych.
29. Zagrożenie - możliwość wystąpienia incydentu.
30. Zbiór danych osobowych - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.
31. Zgoda - dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
32. Usuwanie danych - trwałe zniszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
33. Uwierzytelnianie - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu.
34. Użytkownik/pracownik (w tym podmiotu trzeciego) - osoba przetwarzająca dane w systemie oraz poza nim (np. dokumentacji w formie tradycyjnej), niezależnie od formy zatrudnienia w Gminnej Bibliotece Publicznej w Słupnie lub formy prawnej wiążącej z tą osobą. W szczególności mogą być to osoby zatrudnione na umowę o pracę, stażyści, praktykanci, osoby realizujące zadania na podstawie podpisanej umowy cywilnoprawnej.
35. IOD lub Inspektor Ochrony Danych Osobowych - osoba wyznaczona przez Administratora Danych Osobowych do wypełniania zadań przewidzianych w art. 39 ust. 1 RODO.
36. RCPD lub Rejestr oznacza Rejestr Czynności Przetwarzania Danych Osobowych.

ROZDZIAŁ III

NAJWAŻNIEJSZE ZAGADNIENIA OCHRONY DANYCH OSOBOWYCH

§ 4

ZASADY OCHRONY DANYCH OSOBOWYCH

Filary ochrony danych osobowych w Gminnej Bibliotece Publicznej w Słupnie:

1. **Legalność** - Administrator Danych Osobowych dba o ochronę prywatności i przetwarza dane zgodnie z prawem;
2. **Bezpieczeństwo** - Administrator Danych Osobowych zapewnia odpowiedni poziom bezpieczeństwa danych podejmując stale działania w tym zakresie;
3. **Prawa Jednostki** - Administrator Danych Osobowych jak również wszystkie osoby zaangażowane w procesy przetwarzania danych osobowych, są zobowiązani ułatwić osobom fizycznym realizację ich praw związanych z ochroną danych osobowych;
4. **Rozliczalność** - Administrator Danych Osobowych dokumentuje to, w jaki sposób spełnia obowiązki, aby w każdej chwili móc wykazać zgodność;
5. **Podejście oparte na ryzyku** - Administrator Danych Osobowych jest zobowiązany zidentyfikować ryzyka towarzyszące przetwarzaniu danych osobowych oraz ustalić ich wpływ na operacje związane z danymi osobowymi, a w szczególności na prawa i wolności osób fizycznych.

§ 5

PRZETWARZANIE PRZEZ ADMINISTRATORA

Administrator Danych Osobowych przetwarza dane osobowe z poszanowaniem następujących zasad:

1. **Zasady zgodności z prawem, rzetelności i przejrzystości** - dane osobowe są przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
2. **Zasady ograniczenia celu** - dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
3. **Zasady minimalizacji danych** - dane osobowe są adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
4. **Zasady prawidłowości** - dane osobowe są 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;

5. **Zasady czasowości** - dane osobowe są 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;
6. **Zasady integralności i poufności** - dane osobowe są 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.

ROZDZIAŁ IV

PODMIOTY TWORZĄCE SYSTEM OCHRONY DANYCH OSOBOWYCH I ICH OBOWIĄZKI

§ 6

INSPEKTOR OCHRONY DANYCH

1. W przypadkach wskazanych w art. 37 ust. 1 RODO lub w prawie polskim Administrator Danych Osobowych jest zobowiązany wyznaczyć Inspektora Ochrony Danych.
2. W przypadkach innych niż wskazane w ust. 1, Administrator Danych Osobowych może podjąć decyzję o dobrowolnym wyznaczeniu Inspektora Ochrony Danych.
3. Administrator Danych Osobowych zawiadamia Prezesa Urzędu Ochrony Danych Osobowych w terminie 14 dni o:
 - a) wyznaczeniu Inspektora Ochrony Danych, podając jego dane kontaktowe;
 - b) zmianie Inspektora Ochrony Danych, podając jego dane kontaktowe;
 - c) rezygnacji z wyznaczania Inspektora Ochrony Danych, jeżeli wcześniej był wyznaczony.
4. Inspektor Ochrony Danych ma za zadanie:
 - a) informować Administratora Danych Osobowych oraz osoby przez niego zatrudnione, które przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy prawa;
 - b) doradzać w sprawie przestrzegania przepisów z zakresu ochrony danych osobowych;
 - c) monitorować przestrzeganie przepisów z zakresu ochrony danych osobowych, niniejszej Polityki oraz innych dokumentów Administratora Danych Osobowych;
 - d) monitorować podział obowiązków;

- e) podejmować działania zwiększające świadomość w zakresie ochrony danych osobowych;
 - f) przeprowadzać szkolenia osób zatrudnionych w zakresie ochrony danych osobowych;
 - g) prowadzić audyty;
 - h) udzielać na żądanie Administratora Danych Osobowych zaleceń co do oceny skutków dla ochrony danych osobowych oraz monitorować jej wykonanie zgodnie z art. 35 RODO;
 - i) współpracować z Prezesem Urzędu Ochrony Danych Osobowych;
 - j) pełnić funkcję 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 prowadzić konsultacje we wszelkich innych sprawach.
5. Administrator Danych Osobowych jest zobowiązany zapewnić, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
6. Administrator Danych Osobowych jest zobowiązany wspierać Inspektora Ochrony Danych w wypełnianiu przez niego zadań, o których mowa w ust. 4, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.

§ 7

OSOBY UPOWAŻNIONE

1. Przetwarzania danych osobowych w ramach struktury Administratora Danych Osobowych mogą dokonywać wyłącznie osoby upoważnione przez Administratora Danych Osobowych.
2. Administrator Danych Osobowych zapewnia, aby żadna z osób upoważnionych nie miała dostępu do większej ilości danych osobowych i procesów przetwarzania danych osobowych niż jest to konieczne do prawidłowego wypełniania obowiązków i zadań.
3. Jakikolwiek spory dotyczące zakresu upoważnień do przetwarzania danych osobowych rozstrzyga Administrator Danych Osobowych.
4. Osoba upoważniona do przetwarzania danych osobowych przed przystąpieniem do czynności ma obowiązek:
 - a) zapoznać się z dokumentami z zakresu ochrony danych osobowych, w szczególności z niniejszą Polityką - w zakresie ustalonym przez Administratora Danych Osobowych;
 - b) odbyć szkolenie z zakresu ochrony danych osobowych;

- c) złożyć oświadczenie na piśmie o zapoznaniu się z dokumentami z zakresu ochrony danych osobowych oraz o odbyciu szkolenia z zakresu ochrony danych osobowych;
 - d) złożyć oświadczenie na piśmie o przestrzeganiu zasad ochrony danych osobowych oraz ustalonych procedur.
5. Administrator Danych Osobowych zapewnia osobom upoważnionym dostęp do dokumentów z zakresu ochrony danych, z wyjątkiem tych dokumentów, które nie powinny być dostępne dla wszystkich osób upoważnionych.
 6. Obowiązki określone w ust. 4 nie dotyczą osób, które są dopuszczane do przetwarzania danych osobowych incydentalnie (np. w celu naprawy sprzętu). W takiej sytuacji należy wskazać w treści zawartej umowy obowiązek przestrzegania ochrony danych osobowych oraz przekazać najważniejsze informacje na temat ochrony danych osobowych. W zależności od sytuacji z takimi osobami można zawrzeć również umowę powierzenia.
 7. Administrator Danych Osobowych prowadzi ewidencję osób upoważnionych do przetwarzania danych osobowych.

§ 8

PODMIOTY PRZETWARZAJĄCE

1. Administrator Danych Osobowych może powierzyć przetwarzanie danych osobowych podmiotowi przetwarzającemu w zależności od własnych potrzeb.
2. Administrator Danych Osobowych jest zobowiązany powierzać przetwarzanie danych osobowych tylko takim podmiotom przetwarzającym, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą. Zakazane jest korzystanie z usług podmiotów przetwarzających, które takich gwarancji nie dają.
3. W przypadku korzystania przez podmiot przetwarzający z usług innego podmiotu przetwarzającego, który nie daje analogicznych gwarancji, o jakich mowa w ust. 2, Administrator Danych Osobowych jest zobowiązany wnieść sprzeciw, a w innych przypadkach może wnieść sprzeciw, jeżeli istnieją ku niemu podstawy.
4. Administrator Danych Osobowych jest zobowiązany kontrolować przestrzeganie przez podmiot przetwarzający przepisów RODO przez cały okres trwania umowy.
5. W przypadku naruszania przez podmiot przetwarzający przepisów RODO Administrator Danych Osobowych jest zobowiązany niezwłocznie zaprzestać współpracy z podmiotem przetwarzającym.

6. Administrator Danych Osobowych prowadzi ewidencję podmiotów przetwarzających, z którymi zawarł umowy o powierzenie przetwarzania danych osobowych.
7. Wzór ewidencji podmiotów przetwarzających stanowi **załącznik nr 1**.
8. Każdy pracownik/osoba zatrudniona jest zobowiązana, w ramach wykonywania swoich obowiązków służbowych, ustalić, czy następuje powierzenie danych innemu podmiotowi i niezwłocznie poinformować o tym Inspektora Ochrony Danych.

§ 9

ODBIORCY DANYCH OSOBOWYCH

1. Administrator Danych Osobowych ujawnia dane osobowe odbiorcom danych osobowych wyłącznie po zweryfikowaniu podstawy prawnej takiego ujawnienia.
2. W przypadku braku podstawy prawnej, o której mowa w ust. 1, Administrator Danych Osobowych, odmawia ujawnienia danych osobowych jakimukolwiek odbiorcy danych osobowych.

ROZDZIAŁ V

PRZETWARZANIE DANYCH

§ 10

PRZESŁANKI LEGALNOŚCI PRZETWARZANIA DANYCH

1. Przetwarzanie danych jest dopuszczalne tylko wtedy gdy spełniony jest co najmniej jeden z wymienionych warunków:
 - a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
 - b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
 - c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
 - d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

- e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
- f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Akapit pierwszy lit. f nie ma zastosowania do przetwarzania, którego dokonują organy publiczne w ramach realizacji swoich zadań.

3. Przetwarzanie danych jest zabronione w przypadku danych ujawniających 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.

4. Przetwarzanie tych danych jest jednak dopuszczalne, jeżeli:

- a) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują inaczej;
- b) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
- c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody;
- d) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
- e) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
- f) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są

proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;

- g) przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;
- h) przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
- i) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.

§ 11

PRZETWARZANIE DANYCH OSOBOWYCH NA PODSTAWIE ZGODY

1. Administrator Danych Osobowych przetwarza dane osobowe na podstawie zgody tylko wówczas, gdy nie ma innej podstawy przetwarzania danych osobowych. Nie należy uzyskiwać zgody na przetwarzanie danych osobowych związanych z zawarciem i wykonaniem umowy lub w odniesieniu do takich danych osobowych, których obowiązek przetwarzania wynika z przepisów prawa.
2. Przed podjęciem decyzji o przetwarzaniu danych osobowych na podstawie zgody Administrator Danych Osobowych jest zobowiązany zweryfikować, czy dane osobowe są adekwatne do założonego celu przetwarzania.

3. Zabronione jest wywieranie przymusu w celu uzyskania zgody, w szczególności poprzez odmowę wykonania umowy w przypadku niewyrażenia zgody na przetwarzanie danych osobowych.
4. Zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie je odróżnić od pozostałych kwestii.
5. Zgody muszą być formułowane w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
6. Przykład klauzuli zgody stanowi **załącznik nr 2**.
7. Zgoda może być cofnięta w każdym momencie. Administrator Danych Osobowych zapewnia, aby wycofanie zgody było równie proste, jak jej złożenie.
8. Każdy pracownik zatrudniony zobowiązany jest wykonać obowiązek informacyjny zgodnie z § 14 w przypadku pozyskania danych osobowych na podstawie zgody.
9. Administrator Danych Osobowych zapewnia system zarządzania zgodami, który pozwoli zweryfikować, czy dana osoba udzieliła zgody na przetwarzanie danych osobowych, czy i kiedy ją wycofała.

§ 12

MINIMALIZACJA DANYCH

1. Administrator Danych Osobowych jest zobowiązany przestrzegać zasady minimalizacji.
2. W celu zapewnienia realizacji zasady minimalizacji Administrator Danych Osobowych, w tym wszyscy pracownicy, którzy przetwarzają dane osobowe w szczególności:
 - a) weryfikują ilość przetwarzanych danych osobowych - Administrator Danych Osobowych nie może przetwarzać większej ilości danych osobowych niż to wynika z założonego celu;
 - b) weryfikują zakres przetwarzanych danych osobowych - Administrator Danych Osobowych nie może podejmować większej liczby czynności przetwarzania niż to wynika z założonego celu;
 - c) ograniczają dostęp do danych osobowych poprzez stosowanie środków prawnych (umowy z klauzulami poufności, system upoważnień), środków fizycznych (kontrola dostępu osób do budynków, pomieszczeń i systemów) oraz środków logicznych (kontrola uprawnień w systemach informatycznych i dostępu do systemów informatycznych);

- d) ograniczają czas przetwarzania danych osobowych - Administrator Danych Osobowych nie może przetwarzać danych osobowych dłużej niż to wynika z założonego celu.

§ 13

PRZEKAZYWANIE DANYCH OSOBOWYCH DO PAŃSTW TRZECICH LUB ORGANIZACJI MIĘDZYNARODOWYCH

Administrator Danych Osobowych jest zobowiązany kontrolować, czy przekazuje jakiekolwiek dane osobowe do państw trzecich lub organizacji międzynarodowych, w szczególności w przypadku korzystania z usług innych podmiotów.

§ 14

OBOWIĄZKI INFORMACYJNE PRZY PRZETWARZANIU DANYCH

1. Zbieranie danych osobowych od osób, których dane dotyczą

W przypadku zbierania danych od osoby, której te dane dotyczą Administrator danych jest zobowiązany poinformować tę osobę o:

- a) nazwie i adresie Administratora oraz adresie poczty elektronicznej i numeru telefonu oraz gdy ma to zastosowanie, tożsamości i danych kontaktowych przedstawiciela Administratora;
- b) danych kontaktowych Inspektora Ochrony Danych, jeżeli został powołany;
- c) celu przetwarzania danych osobowych oraz podstawy prawnej przetwarzania;
- d) informacji o odbiorcach danych osobowych lub o kategoriach odbiorców;
- e) informacji o zamiarze transferu danych osobowych do państwa trzeciego, ze szczególnym uwzględnieniem:
 - przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej,
 - stwierdzenia lub braku stwierdzenia przez Komisję Europejską odpowiedniego stopnia ochrony lub - w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO - wzmianki o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
- f) okresie, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteriach ustalania tego okresu;

- g) informacji o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
- h) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a lub art. 9 ust. 2 lit. a RODO - informacji o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
- i) informacji o prawie wniesienia skargi do organu nadzorczego;
- j) informacji czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
- k) informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

Podanych wyżej zasad nie stosuje się, gdy podmiot danych już posiada te informacje.

2. Zbieranie danych osobowych nie od osób, których dane dotyczą.

W przypadku zbierania danych nie od osoby, której te dane dotyczą informacja powinna być poszerzona o:

- a) kategorie odnośnych danych osobowych;
- b) źródle pochodzenia danych osobowych, a jeżeli ma to zastosowanie, o pochodzeniu ich ze źródeł powszechnie dostępnych.

Podanych wyżej zasad nie stosuje się, jeżeli:

- a) podmiot danych dysponuje już tymi informacjami;
- b) udzielenie takich informacji okazuje się niemożliwe lub wymagałoby niewspółmiernie dużego wysiłku, w szczególności w przypadku przetwarzania do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, z zastrzeżeniem warunków i zabezpieczeń, o których mowa w art. 89 ust. 1 RODO, lub o ile wykonanie obowiązku informacyjnego może uniemożliwić lub poważnie utrudnić realizację celów takiego przetwarzania. W takich przypadkach Administrator Danych Osobowych podejmuje odpowiednie środki, by chronić prawa i wolności oraz prawnie uzasadnione interesy podmiotu danych, w tym udostępnia informacje publicznie;

- c) pozyskiwanie lub ujawnianie jest wyraźnie uregulowane prawem Unii Europejskiej lub prawem polskim;
- d) dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy zawodowej przewidzianym w prawie Unii Europejskiej lub w prawie polskim, w tym ustawowym obowiązkiem zachowania tajemnicy.

Administrator Danych Osobowych udziela informacji w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.

Administrator Danych Osobowych spełnia obowiązki informacyjne:

- a) w przypadku pozyskania danych bezpośrednio od podmiotu danych - w chwili pozyskiwania tych danych;
- b) w przypadku pozyskiwania danych osobowych nie od podmiotu danych:
 - w rozsądnym terminie po pozyskaniu danych, jednak nie później niż w terminie miesiąca,
 - najpóźniej przy pierwszej komunikacji z podmiotem danych, jeżeli dane osobowe mają być wykorzystywane do komunikacji,
 - przy pierwszym ujawnieniu, jeżeli dane osobowe mają być ujawnione innemu odbiorcy.

Informacje, o której mowa powyżej każdorazowo należy przekazać indywidualnie osobie, której dane dotyczą przed podjęciem działań z jej danymi, a także dokumentować (najlepiej na piśmie podpisanym przez osobę, której dane dotyczą), że obowiązek informacyjny został wypełniony.

Jeśli zamiast formy papierowej do gromadzenia danych wykorzystuje się system informatyczny to musi on zapewniać zapisanie w trwałej i wiarygodnej formie, że osoba podająca swoje dane za jego pomocą uzyskała informacje w zakresie określonym w przepisach prawa powszechnie obowiązującego. Klauzula powinna być zrozumiała dla osób, których dane mają być gromadzone i przetwarzane. Poświadczenie wykonania obowiązku informacyjnego może polegać na wypełnieniu odpowiednich formularzy (w tym w formie elektronicznej). Istotne jest, aby pola potwierdzające wyrażenie zgody na zbieranie i przetwarzanie danych w formularzu nie były domyślnie zaznaczane.

Treść klauzuli należy skonsultować każdorazowo z Inspektorem Ochrony Danych w celu potwierdzenia zgodności z obowiązującymi przepisami prawa powszechnie obowiązującego.

Informowanie powinno się dokonać bez prośby zainteresowanego.

Wykonanie obowiązku informacyjnego jest zadaniem osoby przyjmującej dane osobowe, która po otrzymaniu potwierdzenia jego wykonania (w przypadku gdy realizowany jest on w formie

papierowej) przekazuje dowód wykonania obowiązku informacyjnego do Inspektora Ochrony Danych.

ROZDZIAŁ VI

UPRAWNIENIA OSÓB FIZYCZNYCH

§ 15

RODZAJE UPRAWNIENÍ OSÓB FIZYCZNYCH

1. Oprócz prawa do informacji, o których mowa w § 14, każdemu podmiotowi danych przysługuje prawo do:
 - a) dostępu do danych osobowych i informacji o nich;
 - b) uzyskania kopii jego danych osobowych;
 - c) sprostowania danych osobowych i uzupełnienia niekompletnych danych osobowych;
 - d) usunięcia danych osobowych (prawo do bycia zapomnianym);
 - e) ograniczenia przetwarzania danych osobowych;
 - f) uzyskania informacji o odbiorcach danych osobowych w przypadku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych;
 - g) uzyskania danych osobowych w określonym formacie i przesłania ich innemu administratorowi danych osobowych;
 - h) żądania przesłania danych osobowych innemu administratorowi danych osobowych przez Administratora Danych Osobowych;
 - i) wyrażenia sprzeciwu wobec przetwarzania danych osobowych na podstawie art. 6 ust. 1 lit. e RODO i art. 6 ust. 1 lit. f RODO, w tym profilowania;
 - j) wyrażenia sprzeciwu wobec marketingu bezpośredniego, w tym profilowania;
 - k) niepodlegania decyzji, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu.

§ 16

REALIZACJA ŻĄDAŃ

1. Prawa osób trzecich. Realizując prawa osób, których dane dotyczą, Administrator Danych Osobowych wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby o wydanie kopii danych lub prawa do przeniesienia danych może

- niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste itp.), Administrator może zwrócić się do osoby w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.
2. Nieprzetwarzanie. Administrator Danych Osobowych informuje osobę o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.
 3. Odmowa. Administrator Danych Osobowych informuje osobę, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.
 4. Dostęp do danych. Na żądanie osoby dotyczące dostępu do jej danych, Administrator Danych Osobowych informuje osobę, czy przetwarza jej dane oraz o szczegółach przetwarzania, zgodnie z art. 15 RODO (zakres odpowiada obowiązkowi informacyjnemu przy zbieraniu danych), a także udziela osobie dostępu do danych jej dotyczących. Dostęp do danych może być zrealizowany przez wydanie kopii danych, z zastrzeżeniem, że kopii danych wydanej w wykonaniu prawa dostępu do danych Administrator nie uznaje za pierwszą nieodpłatną kopię danych dla potrzeb opłat za kopie danych.
 5. Kopie danych. Na żądanie Administrator Danych Osobowych wydaje osobie kopię danych jej dotyczących i odnotowuje fakt wydania pierwszej kopii danych. Administrator Danych Osobowych wprowadza i utrzymuje cennik kopii danych, zgodnie z którym pobiera opłaty za kolejne kopie danych. Cena kopii danych skalkulowana jest w oparciu o oszacowany jednostkowy koszt obsługi żądania wydania kopii danych.
 6. Sprostowanie danych. Administrator Danych Osobowych dokonuje sprostowania nieprawidłowych danych na żądanie osoby. Administrator Danych Osobowych ma prawo odmówić sprostowania danych, chyba że osoba w rozsądny sposób wykaże nieprawidłowości danych, których sprostowania się domaga. W przypadku sprostowania danych Administrator Danych Osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.
 7. Uzupełnienie danych. Administrator Danych Osobowych uzupełnia i aktualizuje dane na żądanie osoby. Administrator Danych Osobowych ma prawo odmówić uzupełnienia danych, jeżeli uzupełnienie byłoby niezgodne z celami przetwarzania danych (np. Administrator Danych Osobowych nie musi przetwarzać danych, które są mu zbędne). Administrator Danych Osobowych może polegać na oświadczeniu osoby, co do uzupełnianych danych, chyba że będzie to niewystarczające w świetle przyjętych przez Administratora Danych Osobowych procedur (np. co do pozyskiwania takich danych), prawa lub zaistnieją podstawy, aby uznać oświadczenie za niewiarygodne.

8. Usunięcie danych. Na żądanie osoby, Administrator Danych Osobowych usuwa dane, gdy:

- a) dane nie są niezbędne do celów, w których zostały zebrane ani przetwarzane w innych celach;
- b) zgoda na ich przetwarzanie została cofnięta, a nie ma innej podstawy prawnej przetwarzania;
- c) osoba wniosła skuteczny sprzeciw względem przetwarzania tych danych;
- d) dane były przetwarzane niezgodnie z prawem;
- e) konieczność usunięcia wynika z obowiązku prawnego;
- f) żądanie dotyczy danych dziecka zebranych na podstawie zgody w celu świadczenia usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku (np. profil dziecka na portalu społecznościowym, udział w konkursie na stronie internetowej).

Jeżeli dane podlegające usunięciu zostały upublicznione przez Administratora Danych Osobowych Administrator podejmuje rozsądne działania, w tym środki techniczne, by poinformować innych administratorów przetwarzających te dane osobowe, o potrzebie usunięcia danych i dostępu do nich.

W przypadku usunięcia danych Administrator Danych Osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

9. Ograniczenie przetwarzania. Administrator Danych Osobowych dokonuje ograniczenia przetwarzania danych na żądanie osoby, gdy:

- a) osoba kwestionuje prawidłowość danych - na okres pozwalający sprawdzić ich prawidłowość;
- b) przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
- c) Administrator nie potrzebuje już danych osobowych, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
- d) Osoba wniosła sprzeciw względem przetwarzania z przyczyn związanych z jej szczególną sytuacją - do czasu stwierdzenia, czy po stronie Administratora zachodzą prawnie uzasadnione podstawy nadrzędne wobec podstaw sprzeciwu.

W trakcie ograniczenia przetwarzania Administrator Danych Osobowych przechowuje dane, natomiast nie przetwarza ich (nie wykorzystuje, nie przekazuje), bez zgody osoby, której dane dotyczą, chyba że w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego.

Administrator Danych Osobowych informuje osobę przed uchyleniem ograniczenia przetwarzania.

W przypadku ograniczenia przetwarzania danych Administrator Danych Osobowych informuje osobę o odbiorcach danych, na żądanie tej osoby.

10. Przenoszenie danych. Na żądanie osoby Administrator Danych Osobowych wydaje w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego lub przekazuje innemu podmiotowi, jeśli jest to możliwe, dane dotyczące tej osoby, które dostarczyła ona Administratorowi Danych Osobowych, przetwarzane na podstawie zgody tej osoby lub w celu zawarcia lub wykonania umowy z nią zawartej, w systemach informatycznych Administratora.

11. Sprzeciw w szczególnej sytuacji. Jeżeli osoba zgłosi umotywowany jej szczególną sytuacją sprzeciw względem przetwarzania jej danych, a dane przetwarzane są przez Administratora Danych Osobowych w oparciu o uzasadniony interes Administratora lub o powierzone Administratorowi zadanie w interesie publicznym, Administrator uwzględni sprzeciw, o ile nie zachodzą po stronie Administratora ważne prawnie uzasadnione podstawy do przetwarzania, nadrzędne wobec interesów, praw i wolności osoby zgłaszającej sprzeciw, lub podstawy do ustalenia, dochodzenia lub obrony roszczeń.

§ 17

PROCEDURA REALIZACJI ŻAŁAŃ PODMIOTÓW DANYCH

1. Procedura określająca realizację żądań podmiotów danych stanowi **załącznik nr 3**.
2. Administrator Danych Osobowych prowadzi rejestr realizacji żądań (w tym udostępnień danych osobowych) podmiotów danych osobowych.
3. Wzór rejestru realizacji żądań podmiotów danych osobowych stanowi **załącznik nr 4**.

§ 18

OBOWIĄZKI ADMINISTRATORA DANYCH

Administrator danych jest obowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności powinien zabezpieczyć dane przed ich udostępnieniem osobom nieupoważnionym, zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem. Dobór odpowiednich środków technicznych i organizacyjnych następuje w ramach procedury zarządzania ryzykiem oraz ewentualnie w oparciu o ocenę skutków dla ochrony danych osobowych.

Dobór odpowiednich środków technicznych i organizacyjnych następuje z uwzględnieniem:

- a) stanu wiedzy technicznej;
- b) kosztów wdrażania;
- c) charakteru, zakresu, kontekstu i celów przetwarzania;
- d) ryzyka naruszenia praw i wolności osób fizycznych.

Dla skutecznej realizacji Polityki ochrony danych osobowych, Administrator zapewnia:

- a) szkolenia w zakresie przetwarzania danych osobowych i sposobów ich ochrony;
- b) okresowe szacowanie ryzyka zagrożeń dla zbiorów danych;
- c) okresową ocenę skutków dla ochrony danych osobowych;
- d) kontrolę, monitoring i nadzór nad przetwarzaniem danych osobowych;
- e) monitorowanie zastosowanych środków ochrony;
- f) możliwość realizacji wytycznych zawartych w Kodeksach, o których mowa w art. 40 RODO;
- g) wdrożenie odpowiednich środków technicznych i organizacyjnych, aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku, w tym między innymi pseudonimizację i szyfrowanie danych osobowych;
- h) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
- i) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
- j) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Ponadto, Administrator danych:

- a) prowadzi dokumentację opisującą sposób przetwarzania danych oraz środki organizacyjne i techniczne służące ochronie danych;
- b) wyznacza Inspektora Ochrony Danych Osobowych, nadzorującego przestrzeganie zasad ochrony, chyba, że sam wykonuje te czynności;
- c) nadaje upoważnienia do przetwarzania danych i dopuszcza do pracy wyłącznie osoby posiadające takie upoważnienie;
- d) zapewnia kontrolę nad tym, jakie dane osobowe, kiedy i przez kogo zostały do zbioru wprowadzone oraz komu są przekazywane;
- e) prowadzi ewidencję osób upoważnionych do ich przetwarzania, która zawiera: imię i nazwisko osoby upoważnionej, stanowisko, datę nadania i ustania upoważnienia, zakres upoważnienia do przetwarzania danych osobowych, a także opcjonalnie identyfikator, jeżeli dane są przetwarzane w systemie informatycznym;

- f) współdziała z Inspektorem Ochrony Danych w zakresie zapewniającym wypełnienie przez niego obowiązków ustawowych;
- g) inicjuje i koordynuje działania, których celem jest zapewnienie w Gminnej Bibliotece Publicznej w Słupnie takiego poziomu ochrony danych osobowych, który odpowiada aktualnym kryteriom bezpieczeństwa oraz wymogom prawa.

§ 19

OBOWIĄZKI OSÓB PRZETWARZAJĄCYCH DANE OSOBOWE

1. Pracownicy/inne osoby przetwarzające dane osobowe są zobowiązani są do przestrzegania przepisów prawa powszechnie obowiązującego i regulacji wewnętrznych dotyczących ochrony danych osobowych. W tym celu zobowiązani są do:
 - a) zapoznania się z obowiązującymi przepisami prawa z zakresu ochrony danych osobowych oraz dokumentacją dotyczącą ochrony danych osobowych;
 - b) przechodzenia szkoleń z obszaru ochrony danych osobowych;
 - c) przetwarzania danych osobowych wyłącznie w celu i zakresie wynikającym z nałożonych obowiązków służbowych;
 - d) zachowania wyjątkowej staranności przy przetwarzaniu danych osobowych, w szczególności danych wrażliwych w celu ochrony interesów osób, których dane dotyczą;
 - e) stosowania określonych w Gminnej Bibliotece Publicznej w Słupnie procedur i środków przetwarzania oraz zabezpieczania danych osobowych;
 - f) podporządkowania się poleceniom Inspektora Ochrony Danych w zakresie ochrony danych osobowych;
 - g) zachowania w poufności danych osobowych oraz danych objętych tajemnicą przedsiębiorstwa;
 - h) zabezpieczenia danych osobowych przed ich utratą, uszkodzeniem lub zniszczeniem, zmianą lub ich udostępnieniem osobom nieupoważnionym;
 - i) dopilnowania, aby przebywanie osób nieupoważnionych w pomieszczeniach, w których przetwarzane są dane osobowe, miało miejsce wyłącznie w obecności osoby upoważnionej;
 - j) dopilnowania, aby przeznaczone do usunięcia dokumenty, zawierające dane osobowe niszczone były w stopniu uniemożliwiającym ich odczytanie. Zabronione jest wyrzucanie dokumentów do koszy na śmieci bez ich właściwej anonimizacji;

- k) przestrzegania procedur właściwego użytkowania systemów informatycznych w których przetwarza się dane osobowe, w tym do nieujawniania innym użytkownikom swoich loginów i haseł;
- l) zachowania należytej staranności podczas przekazywania danych osobowych drogą telefoniczną (konieczność właściwej identyfikacji rozmówcy, konieczność ustalenia, czy rozmówca jest uprawniony do pozyskania danych osobowych, przekazywanie jedynie niezbędnych informacji);
- m) przesyłania danych osobowych za pomocą sieci Internet jedynie z użyciem metod kryptograficznych (szyfrowanie danych, kanały bezpiecznej transmisji);
- n) niewysyłania za pomocą wiadomości e-mail danych osobowych na prywatne adresy,
- o) niekopiowanie danych na inne nośniki bez uzasadnionej potrzeby;
- p) zachowania należytej ostrożności przy transporcie dokumentów oraz nośników informatycznych, zawierających dane osobowe, poza obszarem przetwarzania w Gminnej Bibliotece Publicznej w Słupnie;
- q) niepozostawiania dokumentów, zawierających dane osobowe na urządzeniach wielofunkcyjnych (drukowanie, kopiowanie);
- r) przetwarzania danych osobowych tylko w wyznaczonych do tego celu pomieszczeniach służbowych (lub wyznaczonych ich częściach);
- s) zabezpieczenia zbiorów oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w przepisach wewnętrznych dotyczących bezpieczeństwa;
- t) niszczenia wszystkich zbędnych nośników zawierających dane osobowe w sposób uniemożliwiający ich odczytanie;
- u) nieudzielania informacji o danych osobowych przetwarzanych w Gminnej Bibliotece Publicznej w Słupnie innym podmiotom i osobom, chyba, że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione;
- v) bezzwłocznego zawiadamiania w formie pisemnej administratora danych o wszelkich przypadkach naruszenia bezpieczeństwa danych osobowych i systemu informatycznego przetwarzającego dane osobowe, a także o przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe;
- w) pisemnego wnioskowania o zewidencjonowanie nowych zbiorów danych osobowych w wykazie prowadzonym przez Inspektora Ochrony Danych;
- x) bieżącej oceny funkcjonowania mechanizmów zabezpieczeń i ochrony;

- y) występowania z wnioskami w sprawie wprowadzenia niezbędnych zmian w zakresie ochrony danych osobowych;
 - z) niezwłocznego tj. nie później niż w ciągu 24 godzin od zaistnienia zdarzenia informowania Administratora Danych Osobowych i Inspektora Ochrony Danych Osobowych o naruszeniach ochrony danych osobowych w tym potencjalnych naruszeniach lub, w przypadku naruszeń bezpieczeństwa dotyczących systemów informatycznych, Administratora Systemów Informatycznych oraz niezwłocznego, nie później jednak niż w ciągu 2 dni roboczych informowania Inspektora Ochrony Danych osobowych o żądaniach podmiotów, których dane osobowe dotyczą.
 - aa) niezwłocznego informowania Inspektora Ochrony Danych o wszelkich innych zdarzeniach mających wpływ na realizację obowiązków wynikających z niniejszej Polityki.
2. Jeżeli przepisy odrębnych ustaw, które odnoszą się do przetwarzania danych osobowych, przewidują dalej idącą ich ochronę, niż to wynika z RODO, czy ustawy, stosuje się przepisy tych ustaw.
 3. Pracownicy/użytkownicy przetwarzający dane osobowe obowiązani są dołożyć należytej staranności w celu ochrony interesu osób, których dane są gromadzone i przetwarzane, a w szczególności należy przestrzegać, aby dane te były:
 - a) przetwarzane zgodnie z powszechnie obowiązującym prawem i regulacjami wewnętrznymi;
 - b) zbierane dla oznaczonych, zgodnych z prawem celów i nie poddawane dalszemu przetwarzaniu niezgodnemu z tymi celami;
 - c) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane;
 - d) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;
 - e) wypełniały obowiązek informacyjny.
 4. Naruszenie postanowień Polityki Bezpieczeństwa Przetwarzania Danych Osobowych może skutkować zablokowaniem dostępu pracownika/użytkownika do danych osobowych i systemów.
 5. W przypadku ciężkich naruszeń, takie działanie może prowadzić do wszczęcia postępowania dyscyplinarnego oraz do rozwiązania bądź wypowiedzenia umowy.
 6. W razie wykrycia naruszenia ochrony danych osobowych każdy pracownik ma obowiązek postępować zgodnie z procedurami zawartymi w Dokumentacji.

7. Osoby odpowiedzialne za zarządzanie kadrami w Gminnej Bibliotece Publicznej w Słupnie informują niezwłocznie IOD lub ADO o każdej zmianie w zakresie czynności pracowników, która wiąże się ze zmianą zakresu uprawnień do przetwarzania danych osobowych.
8. Cofnięcie upoważnień do przetwarzania danych osobowych powinno nastąpić niezwłocznie po zakończeniu wykonywania obowiązków pracownika/użytkownika.

ROZDZIAŁ VII

SYSTEM OCHRONY DANYCH OSOBOWYCH

§ 20

POLITYKA CZYSTEGO BIURKA

1. Każda osoba jest odpowiedzialna za dokumenty, z którymi pracuje.
2. Należy przestrzegać ustalonego obiegu dokumentów. Jeżeli do osoby zatrudnionej przez przypadek trafi dokument dla niego nieprzeznaczony, powinien jak najszybciej zgłosić to bezpośredniemu przełożonemu.
3. Należy chronić dokumenty oraz ich treść przed osobami nieupoważnionymi.
4. Kontakt z dokumentami zawierającymi dane osobowe może mieć wyłącznie osoba upoważniona do przetwarzania tych danych osobowych. Zakazane jest przekazywanie dokumentów osobom, nawet zatrudnionym przez Administratora Danych Osobowych, które nie mają upoważnienia do przetwarzania tych danych osobowych.
5. Nie wolno zostawiać bez nadzoru dokumentów w miejscach do tego nieprzeznaczonych, np. na korytarzu, w innym pomieszczeniu, w innym ogólnodostępnym miejscu.
6. Jeżeli dokumenty są drukowane, skanowane lub kopiowane na urządzeniu znajdującym się w miejscu, do którego mają dostęp również inne osoby, nie wolno zostawiać dokumentów w urządzeniu bez nadzoru. Zaleca się, aby drukowanie, skanowanie i kopiowanie odbywało się dopiero po podaniu PIN-u przez użytkownika.
7. Nie wolno zostawiać dokumentów w miejscu, w którym mogą ulec zniszczeniu, np. w pobliżu źródeł wody czy ognia.
8. Nie wolno spożywać lub trzymać napojów w pobliżu dokumentów, jeżeli w wyniku tego dokumenty mogłyby ulec zalaniu.
9. Jeżeli dana osoba pracuje z papierowymi dokumentami, jest zobowiązana zadbać o to, aby na biurku znajdowały się wyłącznie dokumenty potrzebne do bieżących czynności.

10. Po zakończeniu pracy należy schować wszystkie dokumenty do szafki lub szafy zamykanej na klucz - nie wolno zostawiać żadnych dokumentów na biurku, nawet jeżeli wydają się one nieistotne.
11. Nie wolno wynosić dokumentów poza budynek bez wyraźnego zezwolenia bezpośredniego przełożonego.
12. Nie wolno robić kopii dokumentów do celów niezwiązanych z wykonywaną pracą.
13. W przypadku utraty przydatności dokumentu należy go zniszczyć w niszczarce.
14. Nie wolno we własnym zakresie archiwizować dokumentów, które powinny być zniszczone.

§ 21

POLITYKA CZYSTEGO EKRANU

1. Nie wolno pracować na danych osobowych w systemach informatycznych bez otrzymania odpowiedniego upoważnienia oraz uprawnień w systemach informatycznych.
2. Jeżeli użytkownik, np. w wyniku pomyłki człowieka lub błędu systemowego, posiada zbyt dużo uprawnień (czyli posiada dostęp do zbyt wielu informacji i czynności), powinien to zgłosić do Administratora Systemów Informatycznych.
3. W trakcie pracy w systemach informatycznych użytkownik jest zobowiązany posługiwać się nadanym identyfikatorem.
4. Całkowicie zakazane jest wykonywanie pracy pod cudzym identyfikatorem, podobnie jak używanie cudzych loginów, adresów poczty elektronicznej etc.
5. Po nadaniu uprawnień w systemie użytkownik powinien przy pierwszym logowaniu zmienić hasło.
6. Nie należy tworzyć haseł według powtarzalnego schematu, który może być łatwy do odgadnięcia.
7. Nie należy wykorzystywać w hasłach prostych skojarzeń z użytkownikiem (np. wykorzystywać przy budowie hasła swojego imienia lub nazwiska).
8. Hasło nie może być identyczne lub podobne do identyfikatora użytkownika.
9. Hasło trzeba zmieniać w okresach ustalonych przez Administratora Systemów Informatycznych, jednak nie rzadziej niż raz na 30 dni.
10. Zakazuje się wykorzystywania jednego i tego samego hasła do logowania się w różnych systemach informatycznych;
11. Zakazuje się zapisywania haseł na papierze i pozostawiania ich w łatwo dostępnych miejscach.

12. Dopuszczalne jest używanie menadżerów haseł, ale wyłącznie tych, które sprawdzi i zaakceptuje Administrator Systemów Informatycznych.
13. W sytuacji, gdy użytkownik ma podejrzenie lub pewność, że jego hasło zostało ujawnione innej osobie jest zobowiązany niezwłocznie dokonać samodzielnej zmiany hasła w systemie informatycznym i zgłosić tę okoliczność Administratorowi Systemów Informatycznych.
14. Ujawnianie komukolwiek swojego hasła, w jakichkolwiek okolicznościach, jest surowo zakazane, w szczególności, gdy następuje za pośrednictwem poczty elektronicznej.
15. Użytkownik jest odpowiedzialny za zachowanie hasła w poufności.
16. Przed włączeniem komputera użytkownik powinien upewnić się, że monitor został ustawiony w sposób uniemożliwiający podgląd zawartości ekranu innym osobom.
17. Na pulpicie komputera nie powinny znajdować się żadne pliki związane z danymi osobowymi.
18. W trakcie pracy użytkownik powinien uruchamiać tylko te programy i aplikacje, które są mu potrzebne do wykonywania obowiązków służbowych. Nie jest wskazane otwieranie naraz większej liczby programów i aplikacji.
19. W przypadku konieczności opuszczenia miejsca pracy, nawet na krótko, użytkownik powinien wylogować się z używanych programów i aplikacji, aby uniemożliwić dostęp do nich osobom nieupoważnionym.
20. Na komputerze powinien być zainstalowany wygaszacz ekranu, uruchamiający się samoczynnie najpóźniej po 10 minutach braku aktywności użytkownika i odblokowywany po podaniu hasła.
21. Zakazuje się jakichkolwiek ingerencji mających na celu wyłączenie wygaszacza ekranu lub przedłużenie czasu bezczynności, po którym wygaszacz ekranu włącza się samoczynnie.
22. Komputer nie może służyć do wykonywania czynności niezwiązanych z wykonywaną pracą.
23. Komputer nie może służyć do przechowywania materiałów niezwiązanych z wykonywaną pracą.

§ 22

OPROGRAMOWANIE

1. Zakazuje się instalowania jakiegokolwiek oprogramowania bez uzgodnienia z Administratorem Systemów Informatycznych.

2. Oprogramowanie antywirusowe powinno działać w tle w sposób ciągły, przez cały okres pracy użytkownika.
3. Zakazuje się modyfikowania lub wyłączania oprogramowania antywirusowego przez użytkownika.
4. Zakazuje się dokonywania samodzielnej aktualizacji oprogramowania antywirusowego przez użytkownika.
5. Każdy użytkownik jest zobowiązany zawiadomić Administratora Systemów Informatycznych o wszystkich podejrzeniach związanych z możliwością zainstalowania szkodliwego oprogramowania na stacji roboczej lub laptopie.
6. W przypadku usterki w oprogramowaniu, jego nieprawidłowego działania etc. należy zwrócić się do Administratora Systemów Informatycznych.

§ 23

POCZTA ELEKTRONICZNA

1. Poczta elektroniczna może być wykorzystywana wyłącznie do celów służbowych, a do celów prywatnych wyłącznie za zgodą Administratora Danych Osobowych.
2. Nie należy dokonywać zmian w konfiguracji poczty elektronicznej bez uzgodnienia z Administratorem Systemów Informatycznych.
3. Użytkownik poczty elektronicznej jest zobowiązany poznawać zasady szyfrowania maili oraz odczytywania zaszyfrowanych maili.
4. Zakazuje się przysyłania pocztą elektroniczną szczególnie ważnych danych osobowych, dokumentów, projektów, haseł, innych danych identyfikacji w postaci niezaszyfrowanych maili. W takiej sytuacji użytkownik powinien stosować zasady szyfrowania maili.
5. Użytkownik nie może otwierać maili od nieznanych nadawców lub podejrzenie zatytułowanych.
6. Użytkownik nie może otwierać żadnych załączników i klikać w żadne linki w treści maili, jeżeli pochodzą one od nieznanego nadawcy lub wzbudzają jakikolwiek niepokój, związany w szczególności z brakiem polskich znaków, nieprawidłową składnią i fleksją, ludzącym podobieństwem do uznanych firm i organów.
7. Nigdy, w żadnej sytuacji, nie należy stosować się do poleceń zawartych w e-mailu, które dotyczą np. podania hasła, numeru rachunku bankowego, numeru karty kredytowej po otwarciu odnośnika w treści wiadomości.

8. W przypadku otrzymania jakiegokolwiek podejrzanego maila użytkownik powinien zawiadomić Administratora Systemów Informatycznych o tej okoliczności, a na jego polecenie skasować wiadomość.
9. W przypadku otwarcia załącznika lub kliknięcia w podejrzaną link użytkownik powinien natychmiast zawiadomić Administratora Systemów Informatycznych i podjąć działania uniemożliwiające rozprzestrzenienie się ataku.
10. W przypadku wysyłania e-maili do wielu odbiorców należy ukryć listę odbiorców.

§ 24

URZĄDZENIA I NOŚNIKI

1. Każde urządzenie i nośnik są przypisane indywidualnie osobie zatrudnionej.
2. Zakazuje się „wymieniania” urządzeniami i nośnikami pomiędzy osobami zatrudnionymi bez powiadomienia Administratora Systemów Informatycznych.
3. Każdy użytkownik ponosi indywidualną odpowiedzialność za powierzone urządzenie lub nośnik.
4. Zakazuje się wykorzystywania w pracy prywatnych urządzeń i nośników, a w szczególności podłączania ich do sieci Administratora Danych Osobowych.
5. Zakazuje się wykorzystywania urządzeń i nośników do celów niezwiązanych z wykonywanymi zadaniami służbowymi.
6. Po zakończonej pracy użytkownik jest zobowiązany zabezpieczyć urządzenie lub nośnik przed dostępem osób nieupoważnionych i schować je do wyznaczonej szafy albo szafki zamykanej na klucz.
7. W trakcie wykonywania zadań w siedzibie Administratora Danych Osobowych użytkownik jest zobowiązany sprawować nadzór nad wykorzystywanym urządzeniem lub nośnikiem. Zakazuje się w szczególności pozostawiania nośników w miejscach ogólnodostępnych, np. na korytarzach, w pomieszczeniach odwiedzanych przez osoby z zewnątrz etc.
8. Urządzeń i nośników nie wolno pozostawiać w miejscach, w których groziłoby im zniszczenie lub uszkodzenie, np. w pobliżu źródeł wody lub innych cieczy.
9. Zakazuje się wynoszenia urządzeń lub nośników poza siedzibę bez zgody Administratora Danych Osobowych lub Administratora Systemów Informatycznych.
10. Każdy użytkownik wynoszący urządzenie lub nośnik poza siedzibę Administratora Danych Osobowych jest zobowiązany zachować szczególną ostrożność przy ich transporcie, używaniu oraz przechowywaniu.

11. Każdy użytkownik eksploatujący urządzenie przenośne lub nośnik danych osobowych poza siedzibą Administratora Danych Osobowych nie powinien pozostawiać urządzenia przenośnego lub nośnika danych bez nadzoru.

§ 25

PROWADZENIE REJESTRU CZYNNOŚCI PRZETWARZANIA DANYCH OSOBOWYCH

1. Gminna Biblioteka Publiczna w Słupnie prowadzi rejestr czynności przetwarzania danych osobowych zgodnie z wymaganiami art. 30 ust. 1 RODO w stosunku do danych których Gminna Biblioteka Publiczna w Słupnie jest administratorem,
2. Wzór rejestru czynności jest określony w **załączniku nr 5** do niniejszej Polityki.
3. Inspektor ochrony danych okresowo dokonuje przeglądów procesów przetwarzania danych w celach aktualizacji prowadzonych rejestrów.
4. Pracownicy mają obowiązek na bieżąco informować Inspektora o procesach przetwarzania danych osobowych realizowanych w Gminnej Bibliotece Publicznej w Słupnie oraz o wszelkich zmianach w tych procesach, w szczególności dotyczących:
 - a) celów przetwarzania danych, w tym realizowanych czynności;
 - b) kategorii osób, których dane są przetwarzane;
 - c) zakresów przetwarzanych danych;
 - d) podmiotów przetwarzających, którym dane są powierzane;
 - e) odbiorców danych, którym dane są udostępniane.

§ 26

ZARZĄDZANIE RYZYKIEM

1. Administrator Danych Osobowych wdraża i utrzymuje procedurę zarządzania ryzykiem.
2. Administrator Danych Osobowych jest zobowiązany uwzględniać ryzyko w planowanych i prowadzonych procesach przetwarzania danych osobowych.

§ 27

OCENA SKUTKÓW DLA OCHRONY DANYCH OSOBOWYCH

1. W przypadkach wskazanych w art. 35 ust. 1 RODO, art. 35 ust. 3 RODO oraz w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 4 RODO

Administrator Danych Osobowych jest zobowiązany przeprowadzić ocenę skutków dla ochrony danych osobowych.

2. Ocena skutków dla ochrony danych osobowych nie jest wymagana w odniesieniu do operacji przetwarzania znajdujących się w wykazie publikowanym przez Prezesa Urzędu Ochrony Danych Osobowych na podstawie art. 35 ust. 5 RODO.

§ 28

UPRZEDNIE KONSULTACJE Z PREZESEM URZĘDU OCHRONY DANYCH OSOBOWYCH

Jeżeli z oceny skutków dla ochrony danych osobowych wynika, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator Danych Osobowych nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator Danych Osobowych jest zobowiązany skonsultować się z Prezesem Urzędu Ochrony Danych Osobowych.

§ 29

PRIVACY BY DESIGN I PRIVACY BY DEFAULT

1. Administrator Danych Osobowych jest zobowiązany uwzględniać ochronę danych osobowych w fazie projektowania nowych systemów, programów, aplikacji, usług, a także w fazie projektowania nowych procesów i sposobów przetwarzania danych osobowych (privacy by design).
2. Administrator Danych Osobowych jest zobowiązany zapewnić domyślną ochronę danych osobowych, tj. domyślnie mogą być przetwarzane tylko te dane osobowe, które są niezbędne do osiągnięcia konkretnego celu przetwarzania (privacy by default). Rezygnacja z prywatności lub jej ograniczenie mogą nastąpić tylko na wyraźne żądanie podmiotu danych.

§ 30

INWENTARYZACJA

1. Administrator Danych Osobowych szczegółowo inwentaryzuje posiadane dane osobowe oraz procesy z nimi związane, ze szczególnym uwzględnieniem:
 - a) danych szczególnych;

2. W celu zapewnienia pełnej kontroli nad przetwarzaniem danych osobowych oraz zapewnienia bezpieczeństwa przetwarzania danych osobowych Administrator Danych Osobowych prowadzi:
 - a) ewidencję pomieszczeń w których przetwarzane są dane osobowe – której wzór stanowi **załącznik nr 6**;
 - b) ewidencję stacji roboczych, urządzeń przenośnych i nośników - wzór ewidencji stacji roboczych, urządzeń przenośnych i nośników stanowi **załącznik nr 7**.

§ 31

ZBIERANIE DANYCH OSOBOWYCH

1. Dane osobowe przetwarzane u Administratora Danych Osobowych mogą być pozyskiwane bezpośrednio od osób, których te dane dotyczą. W przypadku zbierania danych osobowych nie od osoby, której te dane dotyczą, należy zapewnić, że istnieje podstawa prawna przetwarzania danych.
2. Przetwarzanie i przechowywanie danych osobowych powinno odbywać się w postaci umożliwiającej identyfikację osób, których dotyczą.
3. Przetwarzanie i przechowywanie danych osobowych powinno odbywać się nie dłużej niż jest to niezbędne do realizacji celu przetwarzania.
4. Dane osobowe, które są zbierane powinny być merytorycznie poprawne.
5. Zakres danych osobowych, które są zbierane, powinien być adekwatny w stosunku do celu, w jakim dane zostały zebrane.
6. Zebrane dane po ich wykorzystaniu mogą być przechowywane w przypadku, gdy uprzednio zostaną poddane procesowi anonimizacji, czyli procesowi, który ma na celu uniemożliwienie identyfikacji osób, których dotyczą dane.

ROZDZIAŁ VIII

ZAGROŻENIA BEZPIECZEŃSTWA

§ 32

CHARAKTERYSTYKA MOŻLIWYCH ZAGROŻEŃ

1. Zagrożenia losowe zewnętrzne (np. klęski żywiołowe, przerwy w zasilaniu), których występowanie może prowadzić do utraty integralności danych, ich zniszczenia i uszkodzenia

infrastruktury technicznej systemu, a ciągłość systemu zostaje zakłócona, lecz nie dochodzi do naruszenia poufności danych.

2. Zagrożenia losowe wewnętrzne (np. niezamierzone pomyłki operatorów, administratora systemu, awarie sprzętowe, błędy oprogramowania), przy których może dojść do zniszczenia danych, a ciągłość pracy systemu może zostać zakłócona oraz może nastąpić naruszenie poufności danych.

3. Zagrożenia zamierzone, świadome i celowe - najpoważniejsze zagrożenia, gdzie występuje naruszenia poufności danych, (zazwyczaj nie następuje uszkodzenie infrastruktury technicznej i zakłócenie ciągłości pracy). Zagrożenia te możemy podzielić na: nieuprawniony dostęp do systemu z zewnątrz (włamanie do systemu), nieuprawniony dostęp do systemu z jego wnętrza, nieuprawniony przekaz danych, pogorszenie jakości sprzętu i oprogramowania, bezpośrednie zagrożenie materialnych składników systemu.

§ 33

SYTUACJE ŚWIADCZĄCE O NARUSZENIU ZASAD BEZPIECZEŃSTWA

1. Przełamane zabezpieczenia tradycyjnych - zerwane plomby na drzwiach, szafach, segregatorach.

2. Sytuacje losowe lub nieprzewidziane oddziaływanie czynników zewnętrznych na zasoby systemu jak np.: wybuch gazu, pożar, zalanie pomieszczeń, katastrofa budowlana, napad, działania terrorystyczne, niepożądana ingerencja ekipy remontowej itp.

3. Niewłaściwe parametry środowiska, jak np. nadmierna wilgotność lub wysoka temperatura, oddziaływanie pola elektromagnetycznego, wstrząsy lub wibracje pochodzące od urządzeń przemysłowych.

4. Awaria sprzętu lub oprogramowania, które wyraźnie wskazują na umyślne działanie w kierunku naruszenia ochrony danych lub wręcz sabotaż, a także niewłaściwe działanie serwisu, a w tym sam fakt pozostawienia serwisantów bez nadzoru.

5. Pojawienie się odpowiedniego komunikatu alarmowego od tej części systemu, która zapewnia ochronę zasobów lub inny komunikat o podobnym znaczeniu.

6. Jakość danych w systemie lub inne odstępstwo od stanu oczekiwanego wskazujące na zakłócenia systemu lub inną nadzwyczajną i niepożądaną modyfikację w systemie.

7. Naruszenie lub próba naruszenia integralności systemu lub bazy danych w tym systemie.

8. Próba lub modyfikacja danych oraz zmiana w strukturze danych bez odpowiedniego upoważnienia (autoryzacji).

9. Niedopuszczalna manipulacja danymi osobowymi w systemie.

10. Ujawnienie osobom nieupoważnionym danych osobowych lub objętych tajemnicą procedur ochrony przetwarzania albo innych strzeżonych elementów systemu.
11. Praca w systemie lub jego sieci komputerowej wykazująca nieprzypadkowe odstępstwa od założonego rytmu pracy oraz wskazująca na przełamanie lub zaniechanie ochrony danych osobowych - np. praca przy komputerze lub w sieci osoby, która nie jest formalnie dopuszczona do jego obsługi, sygnał o uporczywym nieautoryzowanym logowaniu, itp.
12. Ujawnienie istnienia nieautoryzowanych kont dostępu do danych lub tzw. „bocznej furtki”, itp.
13. Podmiana lub zniszczenie nośników z danymi osobowymi bez odpowiedniego upoważnienia lub w sposób niedozwolony kasowania lub kopiowanie danych.
14. Rażące naruszenia dyscypliny pracy w zakresie przestrzegania procedur bezpieczeństwa informacji (nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych osobowych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na danych osobowych w celach prywatnych, itp.).

§ 34

TABELA FORM NARUSZENIA BEZPIECZEŃSTWA I SPOSOBY POSTĘPOWANIA

Tabela przykładowych form naruszenia ochrony danych osobowych przez osoby zatrudnione przy przetwarzaniu danych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
W ZAKRESIE WIEDZY	
Ujawnianie sposobu działania aplikacji i systemu oraz jej zabezpieczeń osobom niepowołanym.	Natychmiast przerwać rozmowę lub inną czynność prowadzącą do ujawnienia informacji. Sporządzić raport z opisem, jaka informacja została ujawniona, powiadomić administratora bezpieczeństwa informacji.
Ujawnianie informacji o sprzęcie i pozostałej infrastrukturze informatycznej.	
Dopuszczanie i stwarzanie warunków, aby ktokolwiek taką wiedzę mógł pozyskać np. z obserwacji lub dokumentacji.	

W ZAKRESIE SPRZĘTU I OPROGRAMOWANIA	
Opuszczenie stanowiska pracy i pozostawienie aktywnej aplikacji umożliwiającej dostęp do bazy danych osobowych.	Niezwłocznie zakończyć działanie aplikacji. Sporządzić raport
Dopuszczenie do korzystania z aplikacji umożliwiającej dostęp do bazy danych osobowych przez jakiekolwiek inne osoby niż osoba, której identyfikator został przydzielony.	Wezwać osobę bezprawnie korzystającą z aplikacji do opuszczenia stanowiska przy komputerze. Pouczyć osobę, która dopuściła do takiej sytuacji. Sporządzić raport.
Pozostawienie w jakimkolwiek niezabezpieczonym, a w szczególności w miejscu widocznym, zapisanego hasła dostępu do bazy danych osobowych lub sieci.	Natychmiast zabezpieczyć notatkę z hasłami w sposób uniemożliwiający odczytanie. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczenie do użytkowania sprzętu komputerowego i oprogramowania umożliwiającego dostęp do bazy danych osobowych osobom nieuprawnionym.	Wezwać osobę nieuprawnioną do opuszczenia stanowiska. Ustalić jakie czynności zostały przez osoby nieuprawnione wykonane. Przerwać działające programy. Niezwłocznie powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Samodzielne instalowanie jakiegokolwiek oprogramowania.	Pouczyć osobę popełniającą wymienioną czynność, aby jej zaniechała. Wezwać służby informatyczne w celu odinstalowania programów. Sporządzić raport.
Modyfikowanie parametrów systemu i aplikacji.	Wezwać osobę popełniającą wymienioną czynność, aby jej zaniechała. Sporządzić raport.
Odczytywanie dyskietek i innych nośników przed sprawdzeniem ich programem antywirusowym.	Pouczyć osobę popełniającą wymienioną czynność o szkodliwości takiego działania. Wezwać służby informatyczne w celu wykonania kontroli antywirusowej. Sporządzić raport.

W ZAKRESIE DOKUMENTÓW I OBRAZÓW ZAWIERAJĄCYCH DANE OSOBOWE	
Pozostawienie dokumentów w otwartych pomieszczeniach bez nadzoru.	Zabezpieczyć dokumenty. Sporządzić raport.
Przechowywanie dokumentów niewłaściwie zabezpieczonych przed dostępem osób niepowołanych.	Powiadomić przełożonych. Spowodować poprawienie zabezpieczeń. Sporządzić raport.
Wyrzucanie dokumentów w stopniu zniszczenia umożliwiającym ich odczytanie.	Zabezpieczyć niewłaściwie zniszczone dokumenty. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie do kopiowania dokumentów i utraty kontroli nad kopią.	Zaprzestać kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić przełożonych. Sporządzić raport.
Dopuszczanie, aby inne osoby odczytywały zawartość ekranu monitora, na którym wyświetlane są dane osobowe.	Wezwać nieuprawnioną osobę odczytującą dane do zaprzestania czynności, wyłączyć monitor. Jeżeli ujawnione zostały ważne dane - sporządzić raport
Sporządzanie kopii danych na nośnikach danych w sytuacjach nie przewidzianych procedurą.	Spowodować zaprzestanie kopiowania. Odzyskać i zabezpieczyć wykonaną kopię. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Utrata kontroli nad kopią danych osobowych.	Podjąć próbę odzyskania kopii. Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ I INFRASTRUKTURY SŁUŻĄCYCH DO PRZETWARZANIA DANYCH OSOBOWYCH	
Opuszczanie i pozostawianie bez dozoru nie zamkniętego pomieszczenia, w którym zlokalizowany jest sprzęt komputerowy używany do przetwarzania danych osobowych, co stwarza ryzyko dokonania na sprzęcie lub oprogramowaniu	Zabezpieczyć pomieszczenie. Powiadomić przełożonych. Sporządzić raport.

modyfikacji zagrażających bezpieczeństwu danych osobowych.	
Wpuszczanie do pomieszczeń osób nieznanych i dopuszczanie do ich kontaktu ze sprzętem komputerowym.	Wezwać osoby bezprawnie przebywające w pomieszczeniach do ich opuszczenia, próbować ustalić ich tożsamość. Powiadomić przełożonych i administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczanie, aby osoby spoza służb informatycznych i telekomunikacyjnych podłączały jakiegokolwiek urządzenia do sieci komputerowej, demontowały elementy obudów gniazd i torów kablowych lub dokonywały jakiegokolwiek manipulacji.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
W ZAKRESIE POMIESZCZEŃ W KTÓRYCH ZNAJDUJĄ SIĘ KOMPUTERY CENTRALNE I URZĄDZENIA SIECI	
Dopuszczenie lub ignorowanie faktu, że osoby spoza służb informatycznych i telekomunikacyjnych dokonują jakiegokolwiek manipulacji przy urządzeniach lub okablowaniu sieci komputerowej w miejscach publicznych (hole, korytarze, itp.).	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i ew. opuszczenia pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.
Dopuszczanie do znalezienia się w pomieszczeniach komputerów centralnych lub węzłów sieci komputerowej osób spoza służb informatycznych i telekomunikacyjnych.	Wezwać osoby dokonujące zakazanych czynności do ich zaprzestania i opuszczenia chronionych pomieszczeń. Postarać się ustalić ich tożsamość. Powiadomić służby informatyczne i administratora bezpieczeństwa informacji. Sporządzić raport.

Tabela przykładowych zjawisk świadczących o możliwości naruszenia ochrony danych osobowych

FORMY NARUSZEŃ	SPOSOBY POSTĘPOWANIA
Ślady manipulacji przy układach sieci komputerowej lub komputerach.	Powiadomić niezwłocznie administratora bezpieczeństwa informacji oraz służby

	informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Obecność nowych kabli o nieznanym przeznaczeniu i pochodzeniu.	Powiadomić niezwłocznie służby informatyczne. Nie używać sprzętu ani oprogramowania do czasu wyjaśnienia sytuacji. Sporządzić raport.
Niezapowiedziane zmiany w wyglądzie lub zachowaniu aplikacji służącej do przetwarzania danych osobowych.	
Nieoczekiwane, nie dające się wyjaśnić, zmiany zawartości bazy danych.	
Obecność nowych programów w komputerze lub inne zmiany w konfiguracji oprogramowania.	
Ślady włamania do pomieszczeń, w których przetwarzane są dane osobowe.	Postępować zgodnie z właściwymi przepisami. Powiadomić niezwłocznie administratora bezpieczeństwa informacji. Sporządzić raport.

Tabela przykładowego naruszenia ochrony danych osobowych przez obsługę informatyczną w kontaktach z użytkownikiem

FORMY NARUSZEN	SPOSOBY POSTĘPOWANIA
Próba uzyskania hasła uprawniającego do dostępu do danych osobowych w ramach pomocy technicznej.	Powiadomić administratora bezpieczeństwa informacji. Sporządzić raport.
Próba nieuzasadnionego przeglądania (modyfikowania) w ramach pomocy technicznej danych osobowych za pomocą aplikacji w bazie danych identyfikatorem i hasłem użytkownika.	

POSTĘPOWANIE W PRZYPADKU PODEJRZENIA NARUSZENIA LUB NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Każdy pracownik Gminnej Biblioteki Publicznej w Słupnie, który stwierdzi lub podejrzewa naruszenie ochrony danych osobowych zobowiązany jest do niezwłocznego tj. nie później niż w ciągu 24 godzin od zaistnienia zdarzenia, poinformowania o tym swojego bezpośredniego przełożonego oraz administratora danych.

2. Administrator danych, który stwierdził lub uzyskał informację wskazującą na naruszenie ochrony danych osobowych zobowiązany jest do niezwłocznego:

1) Zapisania wszelkich informacji i okoliczności związanych z danym zdarzeniem, a w szczególności dokładnego czasu uzyskania informacji o naruszeniu ochrony danych osobowych lub samodzielnego wykrycia tego faktu;

2) Jeżeli zasoby systemu na to pozwalają, wygenerowania i wydrukowania wszystkich dokumentów i raportów, które mogą pomóc w ustaleniu wszelkich okoliczności zdarzenia, opatrzenia ich datą i podpisania;

3) Przystąpienia do zidentyfikowania rodzaju zaistniałego zdarzenia, w tym do określenia skali zniszczeń, metody dostępu osoby niepowołanej do danych, itp.;

4) Podjęcia odpowiednich kroków w celu powstrzymania lub ograniczenia dostępu osoby niepowołanej, zminimalizowania szkód i zabezpieczenia przed usunięciem śladów naruszenia ochrony danych, w tym m.in.:

a) fizycznego odłączenia urządzeń, które mogły umożliwić dostęp do danych osobie niepowołanej;

b) wylogowania użytkownika podejrzanego o naruszenie ochrony danych;

c) zmianę hasła użytkownika poprzez którego uzyskano nielegalny dostęp w celu uniknięcia ponownej próby uzyskania takiego dostępu.

5) Szczegółowej analizy stanu systemu informatycznego w celu potwierdzenia lub wykluczenia faktu naruszenia ochrony danych osobowych;

6) Przywrócenia normalnego działania systemu, przy czym, jeżeli nastąpiło uszkodzenie bazy danych, odtworzenia jej z ostatniej kopii awaryjnej z zachowaniem wszelkich środków ostrożności, mających na celu uniknięcie ponownego uzyskania dostępu przez osobę nieupoważnioną, tą samą drogą.

3. Po przywróceniu normalnego stanu bazy danych osobowych należy przeprowadzić szczegółową analizę w celu określenia przyczyn naruszenia ochrony danych osobowych lub

podejrzenia takiego naruszenia, oraz przedsięwziąć kroki mające na celu wyeliminowanie podobnych zdarzeń w przyszłości.

4. Jeżeli przyczyną zdarzenia był błąd użytkownika systemu informatycznego, należy przeprowadzić szkolenie wszystkich osób biorących udział w przetwarzaniu danych.

5. Jeżeli przyczyną zdarzenia była infekcja wirusem należy ustalić źródło jego pochodzenia i wykonać zabezpieczenia antywirusowe i organizacyjne wykluczające powtórzenie się podobnego zdarzenia w przyszłości.

6. Jeżeli przyczyną zdarzenia było zaniedbanie ze strony użytkownika należy wyciągnąć konsekwencje dyscyplinarne wynikające z kodeksu pracy oraz wewnętrznych uregulowań Gminnej Biblioteki Publicznej w Słupnie.

7. Jeżeli doszło do naruszenia ochrony danych osobowych należy ocenić, czy występuje konieczność powiadomienia Prezesa Urzędu Ochrony Danych Osobowych i/lub podmiotów danych o zaistniałym zdarzeniu.

§ 36

POSTĘPOWANIE W PRZYPADKU OTRZYMANIA OD PODMIOTU PRZETWARZAJĄCEGO ZAWIADOMIENIA O PODEJRZENIU NARUSZENIA LUB NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. Po otrzymaniu od podmiotu przetwarzającego zawiadomienia o podejrzeniu naruszenia lub naruszeniu ochrony danych osobowych należy pilnie przeanalizować opis okoliczności oraz dołączone dokumenty, jeżeli takie się pojawiają.
2. W przypadku, gdy przedstawiony opis i dokumenty będą niewystarczające, należy niezwłocznie skontaktować się z podmiotem przetwarzającym w celu uzyskania pełnego obrazu sytuacji, związanego z podejrzeniem naruszenia lub naruszeniem ochrony danych osobowych.
3. W związku z podejrzeniem naruszenia lub naruszeniem można nakazać podmiotowi przetwarzającemu podjęcie określonych czynności - w takiej sytuacji należy kontrolować ich wykonanie.
4. Jeżeli podmiot przetwarzający podjął czynności wyjaśniające, w razie konieczności należy wziąć w nich bezpośredni udział.
5. W przypadku stwierdzenia naruszenia u podmiotu przetwarzającego należy niezwłocznie ustalić:
 - a) okoliczności zdarzenia;
 - b) przyczyny zdarzenia;

- c) osobę odpowiedzialną za spowodowanie zdarzenia;
 - d) poziom naruszenia.
6. Jeżeli doszło do naruszenia ochrony danych osobowych u podmiotu przetwarzającego, należy ocenić, czy występuje konieczność powiadomienia Prezesa Urzędu Ochrony Danych Osobowych i/lub podmiotów danych o zaistniałym zdarzeniu - zgodnie z odrębną procedurą.

§ 37

DZIAŁANIA PODEJMOWANE PO USUNIĘCIU LUB ZMINIMALIZOWANIU SKUTKÓW NARUSZENIA

1. Po usunięciu lub zminimalizowaniu skutków naruszenia Administrator Danych Osobowych jest zobowiązany podjąć działania mające na celu uniknięcie podobnych zdarzeń w przyszłości.
2. Działania Administratora Danych Osobowych, o których mowa w pkt 1, mogą polegać w szczególności na:
 - a) przeprowadzeniu doraźnego audytu wewnętrznego;
 - b) zleceniu przeprowadzenia audytu zewnętrznego;
 - c) ponownym dokonaniu analizy ryzyka;
 - d) ponownym dokonaniu oceny skutków dla ochrony danych osobowych;
 - e) wprowadzeniu dodatkowych zabezpieczeń;
 - f) skierowaniu osób zatrudnionych na dodatkowe szkolenia;
 - g) zmianach organizacyjnych i personalnych;
 - h) zmianie obowiązujących procedur;
 - i) zwiększeniu efektywności procedur;
 - j) wyciągnięciu konsekwencji służbowych wobec osób winnych naruszenia - włącznie z rozwiązaniem umowy o pracę bez zachowania okresu wypowiedzenia.
3. Administrator danych przygotowuje szczegółowy raport o przyczynach, przebiegu i wnioskach ze zdarzenia.
4. Administrator Danych Osobowych dokumentuje wszystkie przypadki naruszeń w rejestrze naruszeń ochrony danych osobowych.
5. Wzór rejestru naruszeń ochrony danych osobowych stanowi **załącznik nr 8**.

§ 38

ZAWIADAMIANIE O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. W przypadku naruszenia ochrony danych osobowych Administrator Danych Osobowych zawiadamia o tym incydencie:
 - a) Prezesa Urzędu Ochrony Danych Osobowych;
 - b) podmioty danych osobowych, których dane dotyczą, chyba że zachodzi okoliczność wyłączająca obowiązek zawiadomienia.

§ 39

OCENA KONIECZNOŚCI ZAWIADOMIENIA PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH O NARUSZENIU

1. Potencjalnie każde naruszenie ochrony danych osobowych może skutkować koniecznością zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o stwierdzonym naruszeniu.
2. Zawiadomienia nie trzeba dokonywać wyłącznie wtedy, gdy istnieje małe prawdopodobieństwo, by naruszenie skutkowało naruszeniem praw lub wolności podmiotów danych.
3. Decyzję w przedmiocie zawiadomienia lub niezawiadomienia Prezesa Urzędu Ochrony Danych Osobowych podejmuje Administrator Danych Osobowych.

§ 40

OCENY KONIECZNOŚCI ZAWIADOMIENIA PODMIOTU DANYCH O NARUSZENIU

1. W przypadku, gdy naruszenie ochrony danych osobowych może, choćby potencjalnie, powodować wysokie ryzyko naruszenia praw i wolności, należy o nim zawiadomić każdy podmiot danych, którego naruszenie dotyczy.
2. Zawiadomienia dokonuje się kanałem komunikacyjnym, który zapewnia możliwość szybkiego i skutecznego poinformowania.
3. Zawiadomienia nie trzeba dokonywać wtedy, gdy:
 - a) Administrator Danych Osobowych wdrożył wcześniej odpowiednie środki zabezpieczeń w odniesieniu do tych danych osobowych (np. dane osobowe na skradzionym laptopie zostały wcześniej zaszyfrowane);
 - b) po stwierdzeniu naruszenia Administrator Danych Osobowych wdrożył odpowiednie środki, które wyeliminowały prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności podmiotów danych (np. zablokował zdalnie dostęp do danych osobowych na skradzionym laptopie);

- c) wymagałoby to niewspółmiernie dużego wysiłku.
- 4. W sytuacji, gdy zawiadomienie wymagałoby niewspółmiernie dużego wysiłku, należy wydać publiczny komunikat o naruszeniu lub użyć podobnego środka, tak, aby podmioty danych osobowych zostały poinformowane w skuteczny sposób. W szczególności można:
 - a) zamieścić komunikat na stronie internetowej Administratora Danych Osobowych;
 - b) zamieścić komunikat w mediach społecznościowych;
 - c) zamieścić komunikat w portalu branżowym;
 - d) zamieścić komunikat w prasie branżowej;
 - e) wyemitować komunikat w radiu lub telewizji.
- 5. Decyzję w przedmiocie zawiadomienia lub niezawiadomienia podmiotów danych podejmuje Administrator Danych Osobowych.

§ 41

ZAWIADAMIANIE PREZESA URZĘDU OCHRONY DANYCH OSOBOWYCH O NARUSZENIU

1. Po stwierdzeniu, że zachodzi konieczność zawiadomienia Prezesa Urzędu Ochrony Danych Osobowych o stwierdzonym naruszeniu, należy zgromadzić wszystkie informacje potrzebne do zgłoszenia naruszenia.
2. Zgłoszenia należy dokonać w terminie 72 godzin od chwili stwierdzenia naruszenia.
3. W przypadku, gdy zgłoszenia nie da się dokonać w terminie 72 godzin z uwagi na okoliczności obiektywne, zgłoszenia należy dokonać niezwłocznie, wyjaśniając Prezesowi Urzędu Ochrony Danych Osobowych przyczyny opóźnienia.
4. Jeżeli w terminie 72 godzin nie uda się zebrać wszystkich potrzebnych informacji, można je przekazywać Prezesowi Urzędu Ochrony Danych Osobowych sukcesywnie, w miarę ich zdobywania.
5. W celu dokonania zgłoszenia należy przygotować zawiadomienie o naruszeniu ochrony danych osobowych.
6. Wzór zawiadomienia o naruszeniu ochrony danych osobowych kierowanego do Prezesa Urzędu Ochrony Danych Osobowych stanowi oficjalny formularz opublikowany przez Prezesa Urzędu Ochrony Danych Osobowych.
7. Zgłoszenia można dokonać za pośrednictwem platformy www.biznes.gov.pl.
8. W przypadku, gdy Prezes Urzędu Ochrony Danych Osobowych zażąda dodatkowych informacji na temat naruszenia, należy niezwłocznie przygotować wskazane informacje i przekazać je organowi.

9. Za dokonanie zgłoszenia naruszenia odpowiada Administrator Danych Osobowych.

§ 42

ZAWIADAMIANIE PODMIOTÓW DANYCH O NARUSZENIU

1. Po stwierdzeniu, że zachodzi konieczność zawiadomienia podmiotów danych o stwierdzonym naruszeniu, należy zgromadzić wszystkie informacje potrzebne do zawiadomienia o naruszeniu oraz podjąć decyzję co do wyboru kanału komunikacyjnego, jaki będzie wykorzystywany do zawiadomienia oraz prowadzenia komunikacji z podmiotami danych.
2. Zawiadomienia należy dokonać bez zbędnej zwłoki po stwierdzeniu naruszenia.
3. W celu poinformowania podmiotów danych należy przygotować zawiadomienie o naruszeniu ochrony danych osobowych.
4. Należy na bieżąco udzielać wszystkich informacji podmiotom danych, które w związku z zawiadomieniem będą chciały uzyskać szerszą wiedzę na temat naruszenia.
5. Zakazane jest jakiegokolwiek utrudnianie podmiotom danych uzyskania dodatkowych informacji w przedmiocie naruszenia.
6. Za dokonanie zawiadomienia i komunikację z podmiotami danych odpowiada Administrator Danych Osobowych.

ROZDZIAŁ IX

PROCEDURY I ŚRODKI BEZPIECZEŃSTWA DANYCH OSOBOWYCH

§ 43

ZAKRES I CEL

Polityka bezpieczeństwa rozumiana jest jako wykaz praw, reguł i praktycznych doświadczeń regulujących sposób zarządzania, ochrony i dystrybucji danych osobowych wewnątrz instytucji. Obejmuje całokształt zagadnień związanych z problemem zabezpieczenia danych osobowych przetwarzanych zarówno tradycyjnie jak i w systemach informatycznych. Wskazuje działania przewidziane do wykonania oraz sposób ustanowienia zasad i reguł postępowania koniecznych do zapewnienia właściwej ochrony przetwarzanych danych osobowych.

§ 44

DEKLARACJA

1. Administrator danych mając świadomość, iż przetwarza dane wrażliwe klientów deklaruje dołożyć wszelkich starań, aby przetwarzanie odbywało się w zgodności z przepisami prawa.
2. W celu zabezpieczenia danych osobowych przed nieuprawnionym udostępnieniem Administrator danych wprowadza określone niniejszym dokumentem zasady przetwarzania danych.
3. W celu zapewnienia prawidłowego monitorowania przetwarzania danych wprowadza się ewidencje i rejestry, które szczegółowo charakteryzują obszary przetwarzania danych, umożliwiając pełną kontrolę nad tym, jakie dane i przez kogo są przetwarzane oraz komu udostępniane.
4. Mając świadomość, iż żadne zabezpieczenie techniczne nie gwarantuje 100%-towej szczelności systemu, konieczne jest, aby każdy pracownik upoważniony do przetwarzania danych pełen świadomej odpowiedzialności, postępował zgodnie z przyjętymi zasadami i minimalizował zagrożenia wynikające z błędów ludzkich.
5. W trosce o czytelny i uporządkowany stan materii, wprowadza się stosowne środki organizacyjne i techniczne zapewniające właściwą ochronę danych oraz nakazuje ich bezwzględne stosowanie, zwłaszcza przez osoby dopuszczone do przetwarzania danych.

§ 45

CHARAKTERYSTYKA INSTYTUCJI

Gminna Biblioteka Publiczna w Słupnie działa na podstawie przepisów ustawy z dnia 27 czerwca 1997 r. o bibliotekach, ustawy z dnia 25 października 1991 r. o organizowaniu i prowadzeniu działalności kulturalnej, ustawy z dnia 8 marca 1990 r. o samorządzie gminnym, przepisów wykonawczych oraz statutu nadanego przez Radę Gminy Słupno.

Jako samorządowa instytucja kultury Biblioteka realizuje zadania własne gminy w zakresie kultury, w szczególności wynikające z art. 4 ustawy o bibliotekach, obejmujące gromadzenie, opracowywanie, przechowywanie i udostępnianie zbiorów, prowadzenie działalności informacyjnej, edukacyjnej i kulturalnej oraz wspieranie rozwoju czytelnictwa w środowisku lokalnym. Biblioteka współuczestniczy także w animowaniu życia społeczno-kulturalnego gminy, organizowaniu wydarzeń literackich i edukacyjnych oraz wspieraniu inicjatyw twórczych mieszkańców.

Biblioteka przetwarza dane osobowe w zakresie niezbędnym do realizacji ustawowych i statutowych zadań, zgodnie z przepisami prawa powszechnie obowiązującego, w szczególności

ustawy o bibliotekach, ustawy o organizowaniu i prowadzeniu działalności kulturalnej, ustawy o samorządzie gminnym, umów związanych z działalnością biblioteczną i kulturalną, a także w zgodzie z zasadami wynikającymi z RODO oraz ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych.

§ 46

WYKAZ MIEJSC PRZETWARZANIA

Tworzy się wykaz pomieszczeń tworzących obszar fizyczny przetwarzania danych. Wyznaczają go pomieszczenia zlokalizowane w Gminnej Bibliotece Publicznej w Słupnie (ewidencję pomieszczeń w których przetwarzane są dane osobowe stanowi **załącznik nr 6**)

§ 47

EWIDENCJA OSÓB UPOWAŻNIONYCH DO PRZETWARZANIA DANYCH OSOBOWYCH

Zgodnie z art. 29 RODO osobowych wprowadza się ewidencję osób upoważnionych do przetwarzania danych, która stanowi **załącznik nr 9** do niniejszej dokumentacji.

Ewidencja zawiera: imię i nazwisko osoby upoważnionej, datę nadania i ustania uprawnień oraz ich zakres, a w przypadku kiedy dane są przetwarzane za pomocą programu komputerowego opcjonalnie również identyfikator dostępu do tego programu.

§ 48

ŚRODKI ORGANIZACYJNE I TECHNICZNE OCHRONY DANYCH

1. W celu stworzenia właściwych zabezpieczeń, które powinny bezpośrednio oddziaływać na procesy przetwarzania danych, wprowadza się następujące środki organizacyjne i techniczne:

- a) aktualizowanie oprogramowania;
- b) aktualizowanie sprzętu;
- c) automatyczna blokada systemu po bezczynności;
- d) dostęp do systemu zabezpieczony loginem i hasłem;
- e) dostęp do zbiorów na podstawie przydzielonych uprawnień;
- f) dokonywanie przeglądów technicznych budynku;
- g) dokumenty niszczone mechanicznie (niszczarka);
- h) gaśnica/system przeciwpożarowy w pomieszczeniach z danymi;
- i) kopie zapasowe danych przechowywane w zamkniętej szafie
- j) korzystanie ze zweryfikowanego oprogramowania;

- k) mechanizmy ochrony przed złośliwym oprogramowaniem;
- l) montaż czujników przeciwpożarowych;
- m) okresowe przeglądy;
- n) pomieszczenia zabezpieczone drzwiami;
- o) pomieszczenia wyposażone w alarm przeciwwłamaniowy;
- p) przechowywanie dokumentacji w zamkniętych szafkach (metalowych lub niemetalowych);
- q) przestrzeganie warunków umowy o korzystanie z aplikacji;
- r) system nadawania i ewidencji upoważnień do przetwarzania danych;
- s) szkolenia pracowników;
- t) ustawienie wygaszaczy ekranu;
- u) weryfikacja ustawień monitorów;
- v) wprowadzenie formularzy zgodnych z prawem;
- w) wprowadzenie polityki czystego biurka;
- x) wprowadzone polityki czystego ekranu;
- y) wykonywanie kopii zapasowej;
- z) zamykana szafa na papierowe cv;
- aa) zamykana szafka na akta;
- bb) zasady bezpieczeństwa dla zatrudnionych;
- cc) zabezpieczenie poczty elektronicznej;
- dd) zastosowanie wymuszonej okresowej zmiany haseł (co 30 dni);
- ee) zasilanie awaryjne (ups, generator prądu);
- ff) kontrola dostępu osób trzecich do placówki (domofon);
- gg) zasady przetwarzania danych przy okazji wydarzeń (np. imprezy okolicznościowe, zdjęcia grupowe – obowiązek zgody itp.)

2. Dla zapewnienia kontroli przestrzegania zasad określonych w niniejszej dokumentacji wyznacza się następujące zadania Inspektorowi Ochrony Danych Osobowych:

- a) nadzór nad przetwarzaniem danych zgodnie z ustawą o ochronie danych osobowych i innymi przepisami prawa;
- b) kontrola przestrzegania zasad ochrony - systematycznie, nie rzadziej niż raz w roku kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, a w szczególności kontrola pod kątem zabezpieczenia danych przed ich udostępnieniem osobom nieupoważnionym,

zabranieniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem ustawy oraz zmianą, utratą, uszkodzeniem lub zniszczeniem, w szczególności:

- kontrola dokumentacji opisującej sposób przetwarzania oraz ochrony,
 - kontrola fizycznych zabezpieczeń pomieszczeń, w których przetwarzane/przechowywane są dane,
 - kontrola poprawności zabezpieczeń danych przetwarzanych metodami tradycyjnymi,
 - kontrola nadanych upoważnień.
- c) przedstawianie administratorowi danych wyników kontroli;
 - d) systematyczna analiza dokumentacji pod kątem obszarów, zbiorów oraz zasad ochrony;
 - e) szkolenie z ochrony danych osobowych oraz aktów wykonawczych;
 - f) podjęcie natychmiastowych działań zabezpieczających w przypadku otrzymania informacji o naruszeniu bezpieczeństwa informacji;
 - g) prowadzenie monitoringu przetwarzania danych.

ROZDZIAŁ X

INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM

§ 49

CHARAKTERYSTYKA SYSTEMU

1. Sieć informatyczna ma strukturę gwiazdy ze switchem centralnym, do którego podłączony jest serwer oraz komputery stacjonarne i przenośne, a także urządzenia peryferyjne i sieciowe.
2. Sygnał internetowy dostarczany jest przez usługodawcę internetowego i odpowiednio zabezpieczony.
3. System zabezpieczony jest oprogramowaniem antywirusowym zainstalowanym na każdym stanowisku oraz zasilaczami awaryjnymi utrzymującymi stałe zasilanie. Zabezpieczony jest także urządzeniami i mechanizmami sieciowymi, w szczególności zaporą sieciową (firewallem) oraz mechanizmami rejestrowania i monitorowania zdarzeń w systemie informatycznym.

OGÓLNE ZASADY PRACY W SYSTEMIE INFORMATYCZNYM

1. Administrator Systemów Informatycznych (a w przypadku jego nie wyznaczenia Administrator Danych Osobowych) odpowiada za korygowanie niniejszej instrukcji w przypadku uzasadnionych zmian w przepisach prawnych dotyczących przetwarzania danych osobowych w systemach informatycznych, jak również zmian organizacyjno-funkcjonalnych.
2. Przetwarzanie danych w systemie informatycznym może być realizowane wyłącznie poprzez dopuszczone przez ASI do eksploatacji licencjonowane oprogramowanie.
3. ASI prowadzi ewidencję oprogramowania.
4. Do eksploatacji dopuszcza się systemy informatyczne wyposażone w:
 - a. mechanizmy kontroli dostępu umożliwiające autoryzację użytkownika oraz przypisanie indywidualnych uprawnień,
 - b. mechanizmy ochrony poufności, dostępności i integralności informacji, z uwzględnieniem potrzeby ochrony kryptograficznej;
 - c. mechanizmy umożliwiające wykonanie kopii bezpieczeństwa oraz archiwizację danych, niezbędne do przywrócenia prawidłowego działania systemu po awarii;
 - d. urządzenia niwelujące zakłócenia i podtrzymujące zasilanie;
 - e. mechanizmy monitorowania w celu identyfikacji i zapobiegania zagrożeniom, w szczególności pozwalające na wykrycie prób nieautoryzowanego dostępu do informacji lub przekroczenia przyznanych uprawnień w systemie;
 - f. mechanizmy zarządzania zmianami.
5. Systemy informatyczne rejestrują co najmniej: logowania i wylogowania użytkowników, nieudane próby logowania oraz operacje administracyjne, zgodnie z wymaganiami KRI w zakresie rejestrowania zdarzeń.
6. Użytkownikom zabrania się:
 - a. korzystania ze stanowisk komputerowych podłączonych do sieci informatycznej poza godzinami i dniami pracy placówki bez pisemnej zgody ADO;
 - b. udostępniania stanowisk roboczych osobom nieuprawnionym;
 - c. wykorzystywania sieci komputerowej placówki w celach innych niż wyznaczone przez ADO;
 - d. samowolnego instalowania i używania programów komputerowych;
 - e. korzystania z nielicencjonowanego oprogramowania oraz wykonywania jakichkolwiek działań niezgodnych z ustawą o ochronie praw autorskich;

- f. umożliwiania dostępu do zasobów wewnętrznej sieci informatycznej placówki oraz sieci Internetowej osobom nieuprawnionym;
- g. używania komputera bez zainstalowanego oprogramowania antywirusowego.

§ 51

PROCEDURY NADAWANIA UPRAWNIEN DO PRZETWARZANIA DANYCH I REJESTROWANIA TYCH UPRAWNIEN W SYSTEMIE INFORMATYCZNYM ORAZ WSKAZANIE OSOBY ODPOWIEDZIALNEJ ZA TE CZYNNOŚCI

1. Użytkowników systemu informatycznego tworzy oraz usuwa ASI na podstawie zgody ADO.
2. Nadawanie uprawnień odbywa się zgodnie z zasadą minimalnych uprawnień, tj. przyznawane są wyłącznie takie uprawnienia, które są niezbędne do wykonywania powierzonych zadań.
3. Do przetwarzania danych osobowych zgromadzonych w systemie informatycznym jak również w rejestrach tradycyjnych wymagane jest upoważnienie.
4. Uprawnienia do pracy w systemie informatycznym odbierane są czasowo, poprzez zablokowanie konta w przypadku:
 - a. nieobecności pracownika w pracy trwającej dłużej niż 30 dni kalendarzowych,
 - b. zawieszenia w pełnieniu obowiązków służbowych.
5. Uprawnienia do przetwarzania danych osobowych odbierane są trwale w przypadku ustania stosunku pracy.
6. Osoby, które zostały upoważnione do przetwarzania danych, są obowiązane zachować w tajemnicy te dane osobowe oraz sposoby ich zabezpieczenia nawet w przypadku ustania stosunku pracy.
7. ASI dokonuje okresowego przeglądu uprawnień użytkowników nie rzadziej niż raz na 12 miesięcy, w celu weryfikacji aktualności i adekwatności nadanych dostępów.

§ 52

STOSOWANE METODY I ŚRODKI UWIERZYTELNIENIA ORAZ PROCEDURY ZWIĄZANE Z ICH ZARZĄDZANIEM I UŻYTKOWANIEM

1. System informatyczny przetwarzający dane osobowe wykorzystuje mechanizm identyfikatora i hasła jako narzędzi umożliwiających bezpieczne uwierzytelnienie.
2. Każdy użytkownik systemu informatycznego powinien posiadać odrębny identyfikator.
3. W identyfikatorze pomija się polskie znaki diakrytyczne.

4. Hasło składa się z co najmniej ośmiu znaków, zawiera co najmniej jedną literę wielką, jedną cyfrę i jeden znak specjalny.
5. Zmianę hasła należy dokonywać nie rzadziej niż co 30 dni.
6. Hasła użytkowników generuje ASI i przekazuje wraz z loginem w formie papierowej w zamkniętej kopercie.
7. Po zapoznaniu się z loginem i hasłem użytkownik zobowiązany jest do ich zniszczenia.
8. Hasło nie może być zapisywane i przechowywane.
9. Użytkownik nie może udostępniać identyfikatora oraz haseł osobom nieupoważnionym.

§ 53

PROCEDURY ROZPOCZĘCIA, ZAWIESZENIA I ZAKOŃCZENIA PRACY

1. Rozpoczęcie pracy użytkownika w systemie informatycznym obejmuje wprowadzenie identyfikatora i hasła w sposób minimalizujący ryzyko podejrzenia przez osoby nieupoważnione.
2. Użytkownik systemu jest odpowiedzialny za zabezpieczenie danych wyświetlanych przez system przed osobami nie mającymi uprawnień.
3. Zawieszenie pracy polega na opuszczeniu stanowiska pracy bez wylogowania się i jest dopuszczalne tylko w przypadku pozostania w pomieszczeniu. Użytkownik jest zobowiązany w takiej sytuacji do włączenia wygaszacza ekranu odblokowywanego hasłem.
4. Zabrania się opuszczania stanowiska pracy bez wcześniejszego wylogowania z systemu z zastrzeżeniem pkt 3.
5. Zakończenie pracy polega na wylogowaniu się z systemu i wyłączeniu komputera.
6. ASI monitoruje logowanie oraz wylogowanie się użytkowników oraz nadzoruje zakres przetwarzanych przez nich zbiorów danych.
7. System informatyczny powinien być skonfigurowany w sposób zapewniający automatyczną blokadę ekranu po upływie określonego czasu bezczynności użytkownika.

§ 54

PROCEDURY TWORZENIA KOPII AWARYJNYCH ZBIORÓW DANYCH ORAZ PROGRAMÓW I NARZĘDZI PROGRAMOWYCH SŁUŻĄCYCH DO ICH PRZETWARZANIA

1. Dane osobowe zabezpiecza się poprzez wykonywanie kopii awaryjnych.
2. Ochronie poprzez wykonanie kopii podlegają także programy i narzędzia programowe służące przetwarzaniu danych. Kopie programów i narzędzi wykonywane są zaraz po

- instalacji oraz po każdej aktualizacji na zewnętrznych, elektronicznych nośnikach informacji.
3. Zabezpieczeniu poprzez wykonywanie kopii awaryjnych podlegają także dane konfiguracyjne systemu informatycznego przetwarzającego dane osobowe, w tym uprawnienia użytkowników systemu.
 4. Za proces tworzenia kopii awaryjnych na serwerze odpowiada ASI.
 5. W przypadku lokalnego przetwarzania danych osobowych na stacjach roboczych, ASI zapewnia objęcie tych danych centralnym mechanizmem wykonywania kopii bezpieczeństwa albo wprowadza inne rozwiązanie zapewniające ich odtworzenie.
 6. Kopie awaryjne mogą być wykonywane tylko na nośnikach informatycznych dostarczonych przez ASI.
 7. Kopie awaryjne mogą być sporządzane automatycznie lub manualnie z wykorzystaniem specjalistycznych urządzeń do wykonywania kopii lub standardowych narzędzi oferowanych przez stacje robocze.
 8. Kopie awaryjne przechowuje ASI w sposób zapewniający ich poufność, integralność i dostępność. Użytkownicy nie przechowują służbowych kopii awaryjnych na nośnikach prywatnych. Kopie usuwa się niezwłocznie po ustaniu ich użyteczności.
 9. ASI zobowiązany jest do okresowego wykonywania testów odtworzeniowych kopii awaryjnych.
 10. Wszelkie wydruki zawierające dane osobowe powinny być przechowywane w miejscu uniemożliwiającym ich odczyt przez osoby nieupoważnione, zaś po upływie czasu ich przydatności niszczone w niszczarkach dokumentów.
 11. Okres przechowywania kopii awaryjnych określa Polityka Bezpieczeństwa Informacji, z uwzględnieniem zasady minimalizacji danych oraz potrzeb związanych z ciągłością działania.

§ 55

SPOSÓB, MIEJSCE I OKRES PRZECHOWYWANIA ELEKTRONICZNYCH NOŚNIKÓW INFORMACJI

1. Nośniki danych oraz programów służących do przetwarzania danych osobowych, a także danych konfiguracyjnych systemu informatycznego, przechowuje ASI w odpowiednio zabezpieczonym pomieszczeniu.
2. Co do zasady dane osobowe gromadzone są na serwerze. W uzasadnionych przypadkach dopuszcza się ich przetwarzanie na innych nośnikach danych, zgodnie z ust. 3.

3. W uzasadnionych przypadkach, za zgodą ASI, dane osobowe można przetwarzać na dyskach twardych komputerów stacjonarnych lub zarejestrowanych nośnikach informacji dostarczonych przez ASI.
4. Przenośne nośniki danych powinny być zabezpieczone ochroną kryptograficzną.
5. Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do:
 - a. likwidacji - pozbawia się wcześniej zapisu tych danych, a w przypadku, gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie;
 - b. przekazania podmiotowi nieuprawnionemu do przetwarzania danych - pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie;
 - c. naprawy - pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem ASI.
6. Nośniki kopii awaryjnych, które zostały wycofane z użycia, podlegają zniszczeniu po usunięciu danych osobowych, w odpowiednim urządzeniu niszczącym przez ASI.

§ 56

SPOSÓB ZABEZPIECZENIA SYSTEMU PRZED DZIAŁALNOŚCIĄ OPROGRAMOWANIA, KTÓREGO CELEM JEST UZYSKANIE NIEUPRAWNIONEGO DOSTĘPU DO SYSTEMU INFORMATYCZNEGO

1. ASI zapewnia ochronę antywirusową oraz zarządza systemem wykrywającym i usuwającym wirusy i inne niebezpieczne kody. System antywirusowy jest skonfigurowany w następujący sposób:
 - a. skanowanie dysków zawierających potencjalnie niebezpieczne dane następuje automatycznie po włączeniu komputera;
 - b. skanowanie wszystkich informacji przetwarzanych w systemie, a zwłaszcza poczty elektronicznej jest realizowane na bieżąco;
 - c. automatycznej aktualizacji wzorców wirusów.
2. W przypadkach wystąpienia infekcji użytkownik powinien niezwłocznie powiadomić o tym fakcie ASI.
3. W przypadku wystąpienia infekcji i braku możliwości automatycznego usunięcia wirusów przez system antywirusowy, ASI podejmuje działania zmierzające do usunięcia zagrożenia. W szczególności działania te mogą obejmować:

- a. usunięcie zainfekowanych plików, o ile jest to akceptowalne ze względu na prawidłowe funkcjonowanie systemu informatycznego;
 - b. odtworzenie plików z kopii awaryjnych po uprzednim sprawdzeniu, czy dane zapisane na kopiach nie są zainfekowane;
 - c. samodzielną ingerencję w zawartość pliku - w zależności od posiadanych narzędzi i oprogramowania.
4. Użytkownicy systemu mają również obowiązek skanowania każdego zewnętrznego elektronicznego nośnika informacji, który chcą wykorzystać.
 5. ASI monitoruje stan systemu, ruch użytkowników w sieci oraz próby ingerencji z zewnątrz w system.
 6. System ochrony przed złośliwym oprogramowaniem jest regularnie aktualizowany oraz dostosowywany do aktualnych zagrożeń, zgodnie z wymaganiami KRI.

§ 57

INFORMACJE O ODBIORCACH, KTÓRYM DANE OSOBOWE ZOSTAŁY UDOSTĘPNIONE, DACIE I ZAKRESIE TEGO UDOSTĘPNIENIA

1. Informacje o udostępnieniu danych osobowych przetwarza się i przechowuje w oparciu o Rzeczowy Wykaz Akt i Instrukcję kancelaryjną.
2. Za udostępnianie danych zgodnie z przepisami prawa odpowiedzialny jest ADO.
3. Nadzór nad właściwym udostępnianiem danych prowadzi ASI.

§ 58

PRZESYŁANIE DANYCH POZA OBSZAR PRZETWARZANIA

1. Urządzenia i nośniki zawierające dane osobowe, przekazywane poza obszar przetwarzania zabezpiecza się w sposób zapewniający poufność i integralność tych danych, w szczególności poprzez zastosowanie ochrony kryptograficznej.
2. W wypadku przesyłania danych osobowych poza sieć przystosowaną do transferu danych osobowych należy zastosować szczególne środki bezpieczeństwa, które obejmują:
 - a. zatwierdzenie przez ADO zakresu danych osobowych przeznaczonych do wysłania;
 - b. zastosowanie mechanizmów szyfrowania danych osobowych;
3. w miarę potrzeb – zastosowanie mechanizmów podpisu elektronicznego lub innych mechanizmów zapewniających integralność i rozliczalność transmisji danych osobowych. Umożliwienie wysyłania danych osobowych tylko z wykorzystaniem określonej aplikacji i tylko przez określonych użytkowników.

4. ASI tworzy konfigurację mechanizmów kryptograficznych w sposób:
 - a. zapewniający wykorzystanie obowiązujących wymagań w zakresie kryptograficznej ochrony danych osobowych;
 - b. umożliwiający, w miarę technicznych możliwości, automatyczne szyfrowanie danych osobowych wysyłanych poza obszar przetwarzania danych;
 - c. informujący użytkownika o dołączeniu do wysyłanych danych osobowych elektronicznego podpisu i wymagający przed wysłaniem informacji potwierdzenia podpisywanej treści.
5. Administrator bezpieczeństwa informacji jest odpowiedzialny za realizację procesów związanych z zarządzaniem aplikacjami kryptograficznymi oraz generowanie kluczy dostępowych do tych aplikacji.

§ 59

PROCEDURY WYKONYWANIA PRZEGLĄDÓW I KONSERWACJI SYSTEMÓW ORAZ NOŚNIKÓW INFORMACJI SŁUŻĄCYCH DO PRZETWARZANIA DANYCH

1. Przeglądy i konserwacje systemu oraz nośników informacji służących do przetwarzania danych mogą być wykonywane jedynie przez osoby posiadające upoważnienie wydane przez ADO.
2. Wszelkie prace związane z naprawami i konserwacją systemu informatycznego przetwarzającego dane osobowe muszą uwzględniać zachowanie wymaganego poziomu zabezpieczenia tych danych przed dostępem do nich osób nieupoważnionych, w szczególności poprzez bezpośredni nadzór prowadzony przez ASI.
3. W przypadku uszkodzenia zestawu komputerowego, nośniki danych, na których są przechowywane dane osobowe powinny zostać zabezpieczone przez ASI.
4. W przypadku konieczności przeprowadzenia prac serwisowych poza placówką, dane osobowe znajdujące się w naprawianym urządzeniu muszą zostać w sposób trwały usunięte.
5. Jeżeli nie ma możliwości usunięcia danych z nośnika na czas naprawy komputera, należy zapewnić stały nadzór nad tym nośnikiem przez osobę upoważnioną do przetwarzania danych osobowych na nim zgromadzonych.
6. ASI wykonuje okresowy przegląd nośników danych osobowych eliminując te, które nie zapewniają odpowiedniego poziomu bezpieczeństwa oraz niezawodności.

§ 60

POSTANOWIENIA KOŃCOWE

1. Polityka jest dokumentem wewnętrznym i nie może być udostępniania osobom nieupoważnionym w żadnej formie.
2. W sprawach nieuregulowanych w niniejszej Polityce mają zastosowanie przepisy powszechnie obowiązującego prawa.
3. Pracownicy i współpracownicy Gminnej Biblioteki Publicznej w Słupnie zobowiązani są do bezwzględnego stosowania zasad określonych w Polityce.
4. Załączniki do niniejszej Polityki stanowią jej integralną część.

DYREKTOR BIBLIOTEKI


Bożena Wernik