**POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA I OCHRONYDANYCH OSOBOWYCH**

**w SPÓŁDZIELNI BUDOWLANO-MIESZKANIOWEJ "OPTYK"**

 **z siedzibą przy ul. Grochowskiej 54 w Warszawie**

**Warszawa, 2018 r.**

**SPIS TREŚCI**

[I. Wstęp 3](#_Toc515208598)

[II. Definicje 4](#_Toc515208599)

[III. Zakres stosowania 7](#_Toc515208599)

[IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe 9](#_Toc515208600)

[V. Wykaz programów zastosowanych do przetwarzania danych osobowych 10](#_Toc515208601)

[VI. Zakres danych przetwarzanych w poszczególnych aplikacjach 11](#_Toc515208602)

[VII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności, rozliczalności i dostępności przetwarzania danych 12](#_Toc515208603)

[VIII. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych 14](#_Toc515208604)

[IX. Zadania Administratora Danych 16](#_Toc515208605)

[X. Zadania Inspektora Ochrony Danych 17](#_Toc515208606)

[XI. Zadania Administratora Systemu Informatycznego 18](#_Toc515208607)

[XII. Szkolenia użytkowników 19](#_Toc515208609)

[XIII. Zarządzanie systemem informatycznym 20](#_Toc515208610)

[XIV. Postanowienia końcowe 25](#_Toc515208611)

# I. Wstęp

§ 1.

Celem Polityki Bezpieczeństwa przetwarzania i ochrony danych osobowych
w SPÓŁDZIELNI BUDOWLANO-MIESZKANIOWEJ "OPTYK" (dalej: „SBM „OPTYK””), zwanej dalej „Polityką Bezpieczeństwa”, jest uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania w SBM „OPTYK” informacji zawierających dane osobowe, a przede wszystkim zapewnienie ochrony danych osobowych przetwarzanych w SBM „OPTYK” przed wszelkiego rodzaju zagrożeniami, tak zewnętrznymi jak i wewnętrznymi.

§ 2.

Polityka Bezpieczeństwa została opracowana w oparciu o wymagania zawarte 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 (Dz. Urz. UE.L nr 119, dalej: „RODO”).

§ 3.

Obszarem przetwarzania danych osobowych w SBM „OPTYK” są wydzielone pomieszczenia w budynku, w którym mieści się Biuro, tj. przy ul. Grochowskiej 54, 04-282 Warszawa.

Kolizja z § 13.

**II. Definicje**

§ 4.

Politykę stosuje się do ochrony podstawowych praw i wolności osób fizycznych,
w szczególności ich praw do ochrony danych osobowych przetwarzanych zarówno jednorazowo jak i wielokrotnie, w formie papierowej oraz elektronicznej.

§ 5.

1. Utrzymanie bezpieczeństwa przetwarzanych danych osobowych w SBM „OPTYK” rozumiane jest jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest wielkość ryzyka związanego z ochroną danych osobowych.
2. Zastosowane zabezpieczenia mają służyć osiągnięciu powyższych celów
i zapewnić:
3. poufność danych – rozumianą jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom;
4. integralność danych – rozumianą jako właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;
5. rozliczalność danych – rozumianą jako właściwość zapewniającą, że działania osoby mogą być przypisane w sposób jednoznaczny tylko tej osobie;
6. integralność systemu - rozumianą jako nienaruszalność systemu, niemożność jakiejkolwiek manipulacji, zarówno zamierzonej, jak i przypadkowej;
7. dostępność informacji - rozumianą jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;

§ 6.

Administratorem Danych Osobowych przetwarzanych w SBM „OPTYK” jest Zarząd Spółdzielni.

§ 7.

Administrator Danych Osobowych wyznacza Uchwałą osobę do pełnienia funkcji Administratora Systemów Informatycznych (ASI) powierzając mu obowiązki zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe.

§ 8.

 Przez użyte w Polityce Bezpieczeństwa określenia należy rozumieć:

1. **Polityka Bezpieczeństwa** – rozumie się przez to Politykę Bezpieczeństwa Przetwarzania i Ochrony Danych Osobowych w SBM „OPTYK”.
2. **Administrator Danych Osobowych (ADO) –r**ozumie się przez to Zarząd SBM „OPTYK”.
3. **Inspektor Ochrony Danych Osobowych (IOD) –** rozumie się przez to osobę wyznaczoną przez Administratora Danych Osobowych do monitorowania
i kontrolowania zasad bezpieczeństwa i ochrony danych osobowych przetwarzanych papierowo oraz w systemach informatycznych, powołany na podstawie odrębnego upoważnienia.
4. **Administrator Systemu Informatycznego (ASI) -** rozumie się przez to osobę lub osoby, upoważnione przez Administratora Danych Osobowych do administrowania i zarządzania systemami informatycznymi w SBM „OPTYK”.
5. **RODO** – rozporządzenie Parlamentu Europejskiego i Rady /UE/ 2016/679
z dnia 27 kwietnia 2016 r., w sprawie ochrony osób fizycznych w związku
z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE /Dz. Urz. UE.L nr 119 (Dz. U.UE L z dnia 4 maja 2016 r.),;
6. **Pseudonimizacja** - oznacza 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;
7. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych.
8. **System tradycyjny** - rozumie się przez to zespół procedur organizacyjnych
związanych z mechanicznym przetwarzaniem informacji i wyposażenia
i środków trwałych w celu przetwarzania danych osobowych na papierze
9. **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych
i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.
10. **Użytkownik** - rozumie się przez to upoważnionego przez Administratora danych, wyznaczonego do przetwarzania danych osobowych pracownika SBM „OPTYK”, który odbył stosowne szkolenie w zakresie ochrony tych danych i został zobowiązany do ochrony danych osobowych oraz zachowania ich w tajemnicy.
11. **Osoba upoważniona** – to osoba (najczęściej pracownik, ale niekoniecznie), która otrzymała upoważnienie do przetwarzania danych osobowych od Administratora Danych Osobowych (ADO).
12. **Osoba uprawniona** – osoba uprawniona do pracy w systemie informatycznym lub przebywania w danym pomieszczeniu (obszarze przetwarzania danych osobowych)
13. **Szacowanie ryzyka** - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które dotyczy wszystkich procesów i czynności służących do przetwarzania danych osobowych.
14. **Dane osobowe** (dane) - informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
15. **Dane osobowe szczególnych kategorii** – oznaczają dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby;
16. **Rejestr czynności przetwarzania danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie, prowadzi go administrator;
17. **Rejestr kategorii czynności przetwarzania danych osobowych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, prowadzony przez każdy podmiot dokonujący czynności przetwarzania dokonywanych w imieniu administratora;
18. **Przetwarzanie danych** - 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;
19. **Zgoda osoby której dane dotyczą** - dobrowolne, konkretne, świadome
i jednoznaczne oświadczenie woli, którym osoba, której dane dotyczą,
w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści; zgoda może być odwołana w każdym czasie.

# III. Zakres stosowania

§ 9.

1. W SBM „OPTYK” przetwarzane są dane osobowe służące do prawidłowego
zarządzania lokalami w SBM „OPTYK” oraz między pracownikami i kontrahentami SBM „OPTYK”.
2. Dane osobowe są przetwarzane zarówno w postaci dokumentacji tradycyjnej jak i elektronicznej.
3. Polityka Bezpieczeństwa zawiera dokumenty dotyczące wprowadzonych zabezpieczeń technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych.

§ 10.

Politykę Bezpieczeństwa stosuje się przede wszystkim do:

1.Danych osobowych przetwarzanych w systemie: Płatnik, programach pakietu LibreOffice (MS Office? Open Office), PROBIT?, S-BIT? oraz przetwarzanych w postaci papierowej.

2. Wszystkich informacji dotyczących lokali i członków SBM "OPTYK" oraz pracowników i kontrahentów SBM „OPTYK”.

3. Wszystkich danych kandydatów do pracy zbieranych na etapie rekrutacji.

4. Informacji dotyczących zabezpieczenia danych osobowych, w tym w szczególności

 zabezpieczenia systemów informatycznych, w których przetwarzane są dane osobowe.

5. Rejestru osób upoważnionych do przetwarzania danych osobowych.

6. Innych dokumentów zawierających dane osobowe.

§ 11.

1. Zakres ochrony danych osobowych określony przez dokumenty Polityki
 Bezpieczeństwa ma zastosowanie do systemów informatycznych SBM „OPTYK”,
 w których są przetwarzane dane osobowe, a w szczególności do:

a) wszystkich istniejących, wdrażanych obecnie lub w przyszłości systemów informatycznych oraz papierowych, w których przetwarzane są dane osobowe podlegające ochronie;

 b) wszystkich lokalizacji - budynków i pomieszczeń, w których są lub będą
 przetwarzane informacje podlegające ochronie;

 c) wszystkich pracowników w rozumieniu przepisów Kodeksu Pracy
 i innych osób mających dostęp do informacji podlegających ochronie.

2. Do stosowania zasad określonych przez dokumenty Polityki Bezpieczeństwa
zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy oraz
inne osoby mające dostęp do informacji podlegających ochronie w SBM „OPTYK”.

§ 12.

Informacje niejawne nie są objęte zakresem niniejszej Polityki Bezpieczeństwa.

# IV. Wykaz budynków, pomieszczeń lub części pomieszczeń, tworzących obszar, w którym przetwarzane są dane osobowe (może w formie załącznika?)

§ 13.

1. Polityka bezpieczeństwa przyjęta w SBM „OPTYK” obowiązuje w pomieszczeniach lub częściach pomieszczeń, w których przetwarzane są dane osobowe, a których wykaz został zamieszczony poniżej.

2. SBM „OPTYK” mieści się pod adresem:
 ul. Grochowska 54, 04-282 Warszawa.

|  |  |  |
| --- | --- | --- |
| 1. | Wykaz pomieszczeń, w których przetwarzane są dane osobowe (wskazanie konkretnych nr pomieszczeń) | Piwnica, piętro …Pokój nr …………. |
| 2. | Wykaz pomieszczeń, w których znajdują się komputery stanowiące element systemu informatycznego | Piwnica, piętro …Pokój nr …………. |
| 3. | Wykaz pomieszczeń, gdzie przechowuje się nośniki informacji zawierające dane osobowe (szafy z dokumentacją papierową, szafy zawierające kopie zapasowe danych, stacje komputerowe, serwery i inne urządzenia komputerowe) | Piwnica, piętro …Pokój nr …………. |
| 4. | Wykaz pomieszczeń archiwum | Piwnica, piętro …Pokój nr …………. |
| 5. | Wykaz programów, w których przetwarzane są dane osobowe | Płatnik, Pakiet LibreOffice |
| 6. | Wykaz podmiotów zewnętrznych, którym powierzono dane osobowe na podstawie podpisanych umów (np. informatyk) – nazwa firmy, imię, nazwisko, adres, funkcja. | 1………………2……………..3……………… |

# V. Wykaz programów zastosowanych do przetwarzania danych osobowych (może w formie załącznika?)

§ 14.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Lp.** | **Zakres danych** | **Osoba odpowiedzialna** | **Program** | **Lokalizacja bazy danych** | **Miejsce przetwarzania danych** |
| 1. | Dane właścicieli lokali | 1…………….2…………… | LibreOffice | Serwer,Archiwum,Stacje robocze, | Budynek/pomieszczenie nr: 1……………..2…………….. |
| 2. | Dane Pracowników SBM „OPTYK” | 1…………….2…………… | Płatnik | Serwer,Archiwum,Jednostki robocze | Budynek/pomieszczenie nr: 1……………..2…………….. |
| 3. | Dane kontrahentów SBM „OPTYK” | 1…………….2…………… | LibreOffice, Płatnik  | Serwer,Archiwum,Jednostki robocze | Budynek/pomieszczenie nr: 1……………..2…………….. |
| 4.  | Dane | 1…………….2…………… | PROBIT, S-Bit | Serwer,Archiwum,Jednostki robocze | Budynek/pomieszczenie nr: 1……………..2…………….. |

# VI. Zakres danych przetwarzanych w poszczególnych aplikacjach

§ 15.

W systemie „Płatnik” przetwarzane są w formie elektronicznej dane osobowe pracowników oraz osób współpracujących na podstawie umów zleceń obejmujące:

1. imiona i nazwiska,
2. adres zameldowania, zamieszkania i do korespondencji,
3. datę urodzenia,
4. numer ewidencyjny PESEL i NIP,
5. zwolnienia lekarskie,
6. wysokości wynagrodzenia,
7. posiadanych dzieci,
8. współmałżonka/współmałżonki.

W ramach wykorzystania pakietu LibreOffice

Dane przetwarzane są w formie elektronicznej i służą do prawidłowego sporządzania list niezbędnych dla obliczania opłat za użytkowania lokali, ustanowionych hipotekach, prowadzenia rejestru lokali, dla których zostały założone księgi wieczyste z adnotacją o prowadzenia rejestru członków SBM "OPTYK",

1. imiona i nazwiska,
2. adres zamieszkania/zameldowania,
3. numer ewidencyjny PESEL/NIP,
4. serię i numer dowodu osobistego,
5. numer lokalu,
6. kwoty opłat,
7. numer księgi wieczystej,

# VII. Środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności, rozliczalności i dostępności przetwarzania danych

§ 16.

1. Zabezpieczenia organizacyjne:
2. Sporządzono i wdrożono Politykę Bezpieczeństwa.
3. Do przetwarzania danych zostały dopuszczone wyłącznie osoby posiadające upoważnienia nadane przez Administratora Danych Osobowych.
4. Stworzono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych oraz zgłaszania incydentów do organu nadzorczego.
5. Osoby zatrudnione przy przetwarzaniu danych zostały zaznajomione
z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie bezpieczeństwa systemu informatycznego.
6. Osoby zatrudnione przy przetwarzaniu danych osobowych zobowiązane zostały do zachowania ich w tajemnicy.
7. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych
i nieuprawnionych.
8. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby zatrudnionej przy przetwarzaniu danych osobowych oraz w warunkach zapewniających bezpieczeństwo danych.
9. Dokumenty i nośniki informacji zawierające dane osobowe, które podlegają zniszczeniu, neutralizuje się za pomocą urządzeń do tego przeznaczonych lub dokonując takiej ich modyfikacji, która nie pozwoli na odtworzenie ich treści, aby po dokonaniu usunięcia danych niemożliwa była identyfikacja osób.
10. Zabezpieczenia techniczne
11. Wewnętrzną sieć komputerową zabezpieczono poprzez odseparowanie od sieci publicznej za pomocą Routera posiadającego firewall oraz możliwość tworzenia ACL (Access Control List - do sprawdzenia czy ma taką opcje – do tego i ew. ustawień jest potrzebne hasło do routera).
12. Stanowiska komputerowe wyposażono w indywidualną ochronę antywirusową oraz zabezpieczony hasłem wygaszasz.
13. Komputery zabezpieczono przed możliwością użytkowania przez osoby nieuprawnione do przetwarzania danych osobowych w systemach informatycznych, za pomocą indywidualnego identyfikatora użytkowania i cykliczne wymuszanej zmiany hasła.
14. Środki ochrony fizycznej:
15. Obszar, na którym przetwarzane są dane osobowe powinien być objęty całodobowym monitoringiem wizyjnym, systemem sygnalizacji włamania i pożaru przeciwpożarowym. (sprawdzić/wykreślić/dorobić)
16. Urządzenia służące do przetwarzania danych osobowych umieszcza się
w pomieszczeniach zamykanych na zestaw kluczy, które są przechowywane przez członków Zarządu SBM „OPTYK”

# VIII. Instrukcja postępowania w przypadku zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych

§ 17.

1. Instrukcja definiuje katalog zagrożeń i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Celem instrukcji jest minimalizacja skutków wystąpienia incydentów bezpieczeństwa, ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każdy pracownik SBM „OPTYK” w przypadku stwierdzenia zagrożenia lub naruszenia ochrony danych osobowych, zobowiązany jest poinformować Administratora Danych Osobowych/Inspektora Ochrony Danych.
3. Do typowych zagrożeń bezpieczeństwa danych osobowych należą:
	1. niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
	2. niewłaściwe zabezpieczenie sprzętu, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
	3. nieprzestrzeganie zasad ochrony danych osobowych przez pracowników i inne osoby upoważnione.
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
	1. zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
	2. zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyka/ów, użytkowników, utrata/zagubienie danych),
	3. umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia zagrożenia, Inspektor Ochrony Danych przy pomocy Administratora Systemów Informatycznych oraz współpracy personelu Administratora Danych Osobowych prowadzi postępowanie wyjaśniające w toku, którego:
	1. ustala zakres i przyczyny zagrożenia oraz jego ewentualne skutki,
	2. inicjuje ewentualne działania dyscyplinarne,
	3. rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych zagrożeń w przyszłości,
	4. dokumentuje prowadzone postępowania.
6. W przypadku stwierdzenia incydentu (naruszenia), Inspektor Ochrony Danych prowadzi postępowanie wyjaśniające w toku, którego:
	1. ustala czas wystąpienia naruszenia, jego zakres, przyczyny, skutki oraz wielkość szkód, które zaistniały,
	2. zabezpiecza ewentualne dowody,
	3. ustala osoby odpowiedzialne za naruszenie,
	4. podejmuje działania naprawcze (usuwa skutki incydentu i ogranicza szkody),
	5. inicjuje działania dyscyplinarne,
	6. wyciąga wnioski i rekomenduje działania korygujące zmierzające do eliminacji podobnych incydentów w przyszłości,
	7. dokumentuje prowadzone postępowania.

Jednoczenie zgodnie z Art. 33 ust. 1 RODO, w przypadku naruszenia ochrony danych osobowych, ADO bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

W zgłoszeniu ADO zobowiązany jest:

a) opisać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;

b) zawrzeć imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;

c) opisać możliwe konsekwencje naruszenia ochrony danych osobowych;

d) opisać środki zastosowane lub proponowane przez ADO w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki
w celu zminimalizowania jego ewentualnych negatywnych skutków.

# IX. Zadania Administratora Danych

§ 18.

Do najważniejszych obowiązków Administratora Danych należy:

1. Organizacja bezpieczeństwa i ochrony danych osobowych zgodnie
z wymogami RODO
2. Zapewnienie przetwarzania danych zgodnie z uregulowaniami Polityki Bezpieczeństwa
3. Wydawanie i anulowanie upoważnień do przetwarzania danych osobowych
4. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych
5. Prowadzenie ewidencji osób uprawnionych do przebywania w obszarach przetwarzania danych osobowych (monitorowanie wykazu osób uprawnionych do pobrania klucza)
6. Prowadzenie rejestrów stanowiących załączniki do Polityki Bezpieczeństwa.
7. Uczestnictwo w prowadzeniu przez IOD postępowania wyjaśniającego
w przypadku naruszenia ochrony danych osobowych
8. Uczestnictwo w nadzorze nad bezpieczeństwem danych osobowych
9. Podejmowanie działań i rozwiązań organizacyjnych będących następstwem wniosków z kontroli komórek organizacyjnych pod względem zgodności przetwarzania danych z przepisami o ochronie danych osobowych, przedstawionych przez IOD
10. Podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych zainicjowanych przez IOD, ASI oraz osoby upoważnione.

# X. Zadania Inspektora Ochrony Danych

§ 19.

Zadania inspektora ochrony danych zostały opisane w art. 39 RODO:

1. Inspektor ochrony danych ma następujące zadania:

a) informowanie administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania zgodnie z art. 35 RODO;

d) współpraca z organem nadzorczym;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

2. Inspektor ochrony danych wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.

# XI. Zadania Administratora Systemu Informatycznego

§ 20.

1. Administrator Systemu Informatycznego odpowiedzialny jest za:
2. bieżący monitoring i zapewnienie ciągłości działania systemu informatycznego oraz baz danych;
3. optymalizację wydajności systemu informatycznego, baz danych, instalacje i konfiguracje sprzętu sieciowego i serwerowego;
4. instalacje i konfiguracje oprogramowania systemowego, sieciowego, oprogramowania bazodanowego;
5. konfigurację i administrowanie oprogramowaniem systemowym, sieciowym oraz bazodanowym zabezpieczającym dane chronione przed nieupoważnionym dostępem;
6. nadzór nad zapewnieniem awaryjnego zasilania komputerów oraz innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych;
7. współpracę z dostawcami usług oraz sprzętu sieciowego i serwerowego oraz zapewnienie zapisów dotyczących ochrony danych osobowych;
8. zarządzanie kopiami awaryjnymi konfiguracji oprogramowania systemowego, sieciowego;
9. zarządzanie kopiami awaryjnymi danych osobowych oraz zasobów umożliwiających ich przetwarzanie;
10. przeciwdziałanie próbom naruszenia bezpieczeństwa informacji;
11. Przyznawanie na wniosek Administratora Danych Osobowych lub Inspektora Ochrony Danych ściśle określonych praw dostępu do informacji w danym systemie;
12. wnioskowanie do Administratora Danych Osobowych w sprawie zmian lub usprawnienia procedur bezpieczeństwa i standardów zabezpieczeń;
13. zarządzanie licencjami, procedurami ich dotyczącymi;
14. prowadzenie profilaktyki antywirusowej.
15. Praca Administratora Systemu Informatycznego jest nadzorowana pod względem przestrzegania zapisów wynikających z RODO oraz umowy cywilno-prawnej.

# XII. Szkolenia użytkowników

§ 21.

Każdy użytkownik przed dopuszczeniem do pracy z systemem informatycznym przetwarzającym dane osobowe lub zbiorami danych osobowych w wersji papierowej winien być poddany przeszkoleniu w zakresie ochrony danych osobowych.

1. Za zlecenie przeprowadzenia szkolenia odpowiada Administrator Danych Osobowych.
2. Zakres szkolenia powinien obejmować zaznajomienie użytkownika z przepisami wynikającymi z RODO oraz instrukcjami obowiązującymi u Administratora Danych Osobowych, a także o zobowiązaniu się do ich przestrzegania.
3. Szkolenie zostaje zakończone podpisaniem przez słuchacza oświadczenia o wzięciu udziału w szkoleniu, jego zrozumieniu oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych. Wzór oświadczenia stanowi załącznik nr 1.
4. Dokument ten jest przechowywany razem z dokumentacją dotyczącą ochrony danych osobowych prowadzoną przez ADO i stanowi podstawę do podejmowania działań w celu nadania im uprawnień do korzystania z systemu informatycznego przetwarzającego dane osobowe.

# XIV. Zarządzanie systemem informatycznym

§ 22.

**Procedury nadawania uprawnień do przetwarzania danych w systemie informatycznym i rejestrowania tych uprawnień.**

1. Upoważnienia do przetwarzania danych osobowych nadawane są w związku
z wykonywaniem przez osobę upoważnioną obowiązków lub zadań związanych z przetwarzaniem danych osobowych.
2. Upoważnienie nadaje i odwołuje Administrator Danych Osobowych. Upoważnienie sporządzane jest na piśmie, w dwóch jednobrzmiących egzemplarzach – jeden przeznaczony jest dla osoby upoważnionej, której nadano lub odebrano upoważnienie, drugi – dla ADO.
3. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3. Odwołanie (anulowanie) upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 8.
4. Upoważnienia nie sporządza się dla ADO. Upoważnienia nadane przed dniem wprowadzenia Polityki Bezpieczeństwa pozostają w mocy do czasu ich aktualizacji.
5. Upoważnienia do przetwarzania danych osobowych rejestrowane są
w rejestrze osób upoważnionych do przetwarzania danych osobowych. Wzór rejestru stanowi załącznik nr 9. Rejestr prowadzi administrator danych.

§ 23.

**Stosowane metody i środki uwierzytelniania oraz procedury związane z ich zarządzaniem i użytkowaniem**

1. Środki uwierzytelniania dostępu do systemu informatycznego służącego do przetwarzania danych osobowych to identyfikator użytkownika i hasło dostępu.
2. Każdy identyfikator użytkownika zabezpieczony jest hasłem.
3. W DBFO obowiązują następujące zasady tworzenia hasła:
4. hasło nie może składać się z żadnych danych personalnych (imienia, nazwiska, adresu zamieszkania użytkownika lub najbliższych osób) lub ich fragmentów,
5. hasło musi składać się z co najmniej 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne,
6. hasło nie może składać się z identycznych znaków lub ciągu znaków z klawiatury,
7. hasło nie może być jednakowe z identyfikatorem użytkownika,
8. hasło musi być unikalne, tj. takie, które nie było poprzednio stosowane przez użytkownika.
9. Hasło, w trakcie wpisywania, nie może być wyświetlane na ekranie. Użytkownik jest zobowiązany do utrzymania hasła w tajemnicy, również po utracie jego ważności.
10. Hasło musi być zmieniane nie rzadziej niż co 30 dni. Jeżeli zmiana hasła nie jest możliwa w wymaganym czasie, należy jej dokonać w najbliższym możliwym terminie.
11. W przypadku złamania poufności hasła, użytkownik zobowiązany jest niezwłocznie zmienić hasło i poinformować o tym fakcie administratora danych.
12. Identyfikator użytkownika nie powinien być zmieniany, a po wyrejestrowaniu użytkownika z systemu informatycznego służącego do przetwarzania danych osobowych nie powinien być przydzielany innej osobie.
13. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych osobowych, należy niezwłocznie zablokować w systemie informatycznym służącym do przetwarzania danych osobowych oraz unieważnić przypisane mu hasło.

§ 24.

**Procedury rozpoczęcia, zawieszenia i zakończenia pracy przeznaczone dla użytkowników systemu informatycznego służącego do przetwarzania danych osobowych**

1. Przed rozpoczęciem przetwarzania danych osobowych użytkownik powinien sprawdzić, czy nie ma oznak fizycznego naruszenia zabezpieczeń.
W przypadku wystąpienia jakichkolwiek nieprawidłowości, należy powiadomić IOD/ADO.
2. Przystępując do pracy w systemie informatycznym służącym do przetwarzania danych osobowych, użytkownik jest zobowiązany wprowadzić swój identyfikator oraz hasło dostępu.
3. Zabrania się wykonywania jakichkolwiek operacji w systemie informatycznym służącym do przetwarzania danych osobowych
z wykorzystaniem identyfikatora i hasła dostępu innego użytkownika.
4. W przypadku czasowego opuszczenia stanowiska pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego służącego do przetwarzania danych osobowych.
5. Zakończenie pracy w systemie służącym do przetwarzania danych osobowych powinno być poprzedzone sporządzeniem, w miarę potrzeb, kopii zapasowej danych oraz zabezpieczeniem przed nieuprawnionym dostępem dodatkowych nośników danych tj. płyty CD, pendrive i innych, zawierających dane osobowe.
6. Zakończenie pracy w systemie informatycznym służącym do przetwarzania danych osobowych następuje poprzez zamknięcie systemu.

§ 25.

**Procedury tworzenia kopii zapasowych zbiorów danych oraz programów
i narzędzi programowych służących do ich przetwarzania**

1. Za sporządzanie kopii zapasowych zbiorów danych odpowiedzialny jest użytkownik systemu informatycznego służącego do przetwarzania danych osobowych.
2. Kopie awaryjne może tworzyć jedynie ASI.
3. Kopie zapasowe powinny być kontrolowane przez ASI, w szczególności pod kątem prawidłowości ich wykonania poprzez częściowe lub całkowite odtworzenie na wydzielonym sprzęcie komputerowym.
4. Nośniki informatyczne zawierające dane osobowe lub kopie systemów informatycznych służących do przetwarzania danych osobowych są przechowywane w sposób uniemożliwiający ich utratę, uszkodzenie lub dostęp osób nieuprawnionych.
5. W przypadku likwidacji nośników informatycznych zawierających dane osobowe lub kopie zapasowe systemów informatycznych służących do przetwarzania danych osobowych należy przed ich likwidacją usunąć dane osobowe lub uszkodzić je w sposób uniemożliwiający odczyt danych osobowych.

§ 26.

**Sposób, miejsce i okres przechowywania elektronicznych nośników informacji zawierających dane osobowe oraz kopii zapasowych**

1. Nie należy przechowywać zbędnych nośników informacji zawierających dane osobowe oraz kopii zapasowych, a także wydruków i innych dokumentów zawierających dane osobowe. Po upływie okresu ich użyteczności lub przechowywania, dane osobowe powinny zostać skasowane lub zniszczone tak, aby nie było możliwe ich odczytanie.
2. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe nie mogą być wynoszone bez zgody ADO poza pomieszczenia stanowiące obszar przetwarzania danych osobowych, określony w § 13.
3. Elektroniczne nośniki informacji zawierające dane osobowe oraz kopie zapasowe, a także wydruki i inne dokumenty zawierające dane osobowe przechowywane są poza miejscem bieżącego przetwarzania w zamykanych na klucz szafach w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w § 13,
4. W przypadku uszkodzenia lub zużycia nośnika informacji zwierających dane osobowe należy go fizycznie zniszczyć tak, aby nie było możliwe odczytanie danych osobowych.

§ 27.

**Sposób zabezpieczenia systemu informatycznego służącego do przetwarzania danych osobowych przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych**

1. Do ochrony przed działalnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego służącego do przetwarzania danych osobowych stosowane jest oprogramowanie antywirusowe.
2. Każdy zbiór wczytywany do komputera, w tym także wiadomość e-mail, musi być przetestowany programem antywirusowym.
3. Na każdym stanowisku wyposażonym w dostęp do sieci Internet musi być zainstalowanie oprogramowanie antywirusowe.
4. Niedopuszczalne jest stosowanie dostępu do sieci Internet bez aktywnej ochrony antywirusowej oraz zabezpieczenia przed dostępem szkodliwego oprogramowania.

§ 28.

**Sposób zapewnienia odnotowania informacji o odbiorcach, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia**

1. W systemie informatycznym służącym do przetwarzania danych osobowych odnotowywane są informacje o odbiorcach danych, a w szczególności: imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia.
2. W przypadku, gdy w systemie informatycznym służącym do przetwarzania danych osobowych nie jest możliwe odnotowywanie takich informacji, ADO odnotowuje je w rejestrze odbiorców danych osobowych, w którym odnotowywane są: imię i nazwisko lub nazwa odbiorcy, data udostępnienia oraz zakres udostępnienia. Wzór rejestru stanowi załącznik nr 10.

§ 29.

**Procedury wykonywania przeglądów i konserwacji systemów oraz nośników informacji służących do przetwarzania danych osobowych**

1. Przeglądy i konserwacje sprzętu komputerowego oraz nośników informacji służących do przetwarzania danych osobowych, przeprowadzane są
w pomieszczeniach stanowiących obszar przetwarzania danych osobowych, określony w §13, przez firmy zewnętrzne na podstawie zawartych umów, które zawierają zapisy dotyczące powierzenia danych osobowych.
2. W przypadku przekazywania do naprawy sprzętu komputerowego
z zainstalowanym systemem informatycznym służącym do przetwarzania danych osobowych lub nośnikiem informacji służących do przetwarzania danych osobowych, powinien on zostać pozbawiony danych osobowych przez fizyczne wymontowanie dysku lub skasowanie danych. W szczególnych przypadkach naprawa powinna zostać przeprowadzona w obecności Administratora Systemów Informatycznych.
3. Przeglądy techniczne wykonywane muszą być nie rzadziej niż raz w roku.
4. Nadzór nad przeprowadzaniem przeglądów technicznych, konserwacji i napraw sprzętu komputerowego, na którym zainstalowano system informatyczny służący do przetwarzania danych osobowych, systemu informatycznego służącego do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych pełni Administrator Systemów Informatycznych. ADO prowadzi dokumentację potwierdzającą wykonanie napraw, przeglądów i konserwacji.
5. Zabronione jest wykonywanie przeglądów i konserwacji systemów informatycznych służących do przetwarzania danych osobowych oraz nośników informacji służących do przetwarzania danych osobowych samodzielnie przez użytkownika z DBFO.

§ 30.

1. Administrator Systemów Informatycznych na polecenie Administratora Danych Osobowych ma prawo do kontroli stanu zabezpieczeń oraz przestrzegania zasad ochrony danych osobowych w dowolnym terminie.
2. Administrator Systemów Informatycznych zobowiązany jest do instalowania zalecanych przez producentów programów i aktualizacji oprogramowania oraz uaktualnienia systemu informatycznego służącego do przetwarzania danych osobowych celem wyeliminowania błędów w działaniu lub poprawienia wydajności.

# XV. Postanowienia końcowe

§ 31.

1. Polityka Bezpieczeństwa jest dokumentem wewnętrznym i nie może być udostępniania osobom postronnym w żadnej formie.
2. Administrator Danych Osobowych ma obowiązek zapoznać z treścią Polityki Bezpieczeństwa każdego użytkownika.
3. Wszystkie regulacje dotyczące systemów informatycznych, określone w Polityce Bezpieczeństwa dotyczą również przetwarzania danych osobowych w bazach prowadzonych w jakiejkolwiek innej formie.
4. Użytkownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce Bezpieczeństwa.
5. Wobec osoby, która w przypadku naruszenia zabezpieczeń systemu informatycznego lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności materialnej tej osoby oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. W sprawach nieuregulowanych w Polityce Bezpieczeństwa mają zastosowanie przepisy wynikające z RODO, ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych oraz Kodeksu Cywilnego.

**Załączniki:**

1.Oświadczenie pracownika o znajomości obowiązków odnośnie ochrony danych
osobowych.

3. Upoważnienie pracownika do przetwarzania danych osobowych.

2. Wzór klauzuli informacyjnej o przetwarzaniu danych osobowych.

4. Wyrażenie zgody na przetwarzanie danych osobowych.

5. Wzór umowy powierzenia przetwarzania danych osobowych.

6. Rejestr czynności przetwarzania SBM „OPTYK”.

7. Rejestr kategorii czynności przetwarzania SBM „OPTYK”.

8. Odwołanie upoważnienia do przetwarzania danych osobowych.

9. Rejestr osób upoważnionych do przetwarzania danych osobowych.

10. Rejestr odbiorców danych osobowych.

11. Rejestr incydentów.