# POLITYKA OCHRONY DANYCH OSOBOWYCH w Stowarzyszeniu Pomocy Potrzebującym „NADZIEJA” oraz jego jednostkach organizacyjnych z dnia 25.08.2026r.

## I. Postanowienia ogólne

**Art. 1**

1. Zarząd Stowarzyszenia Pomocy Potrzebującym „NADZIEJA” [dalej: również Stowarzyszenie] świadomy wagi problemów związanych z ochroną prawa do prywatności oraz narastającej skali zagrożeń związanych z nieuprawnionym przetwarzaniem danych osobowych, dołoży szczególnej staranności w celu ich ochrony i jednocześnie deklaruje:
   1) zamiar podejmowania wszystkich działań niezbędnych dla ochrony praw i usprawiedliwionych interesów jednostki związanych z bezpieczeństwem danych osobowych,
   2) zamiar stałego podnoszenia świadomości oraz kwalifikacji osób przetwarzających dane osobowe w Stowarzyszeniu w zakresie problematyki bezpieczeństwa tych danych,
   3) zamiar podejmowania w niezbędnym zakresie współpracy z instytucjami powołanymi do ochrony danych osobowych.
2. Polityka Ochrony Danych Osobowych [dalej: Polityka] jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Administratora w celu spełnienia wymagań Rozporządzenia PE i RE 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych [dalej: RODO].
3. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z powyższym Rozporządzeniem.
4. Stowarzyszenie nie jest zobowiązane do powołania Inspektora Ochrony Danych, zatem Stowarzyszenie nie powołuje Inspektora Ochrony Danych.
5. **Polityka ma zastosowanie do Stowarzyszenia Pomocy Potrzebującym „NADZIEJA” oraz wszystkich jego jednostek organizacyjnych.**

**Art. 2**

Ilekroć w Polityce jest mowa o :

1) **administratorze** – rozumie się przez to Stowarzyszenie, w imieniu, którego działa zarząd,
2) **jednostce organizacyjnej** - rozumie się przez to jednostkę utworzoną i działającą w ramach struktury Stowarzyszenia, na podstawie Statutu, regulaminu, uchwały lub innego aktu wewnętrznego Stowarzyszenia,
3) **osobie upoważnionej do przetwarzania danych osobowych** - rozumie się przez to osobę, która została upoważniona przez administratora do przetwarzania danych osobowych,
4) **personelu** - osoby, upoważnione do przetwarzania danych osobowych, wykonujące określone czynności u administratora w szczególności: w oparciu o stosunek pracy, umowy cywilnoprawne, porozumienie o wolontariat, staż, praktykę, stosunek wynikający z członkostwa w Stowarzyszeniu,
5) **rozliczalności** – rozumie się przez to właściwość zapewniającą, że działanie podmiotu może być przypisane w sposób jednoznaczny, tylko temu podmiotowi,
6) **integralności danych** – rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
7) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom,
8) **aktywach** – środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych,

9) **naruszeniu 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 przez administratora,
10) **zagrożeniu** - potencjalne naruszenie ochrony danych osobowych,
11) **skutkach** - rezultaty potencjalnego naruszenia ochrony danych osobowych,
12) **ryzyku** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje określone skutki dla danych osobowych.

**Art. 3**

1. Celem Polityki jest ochrona danych osobowych przetwarzanych przez Administratora, w tym w ramach działalności jego jednostek organizacyjnych, w zakresie określonym przepisami prawa.
2. Stowarzyszenie zobowiązuje się chronić dane osobowe przetwarzane w kartotekach, skorowidzach, księgach, wykazach, systemach informatycznych w zakresie przewidzianym przepisami prawa.
3. Stowarzyszenie realizując Politykę dołoży szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   1) przetwarzane zgodnie z prawem,
   2) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane dalszemu przetwarzaniu niezgodnemu z tymi celami,
   3) merytorycznie poprawne i adekwatne w stosunku do celów, w jakich są przetwarzane,
   4) przechowywane w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania.

**Art. 4**

Polityka zawiera w szczególności:
1) prawa osób, których dane dotyczą,
2) zasady przygotowania analizy ryzyka,
3) wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
4) środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych [Instrukcja zarządzania],
5) regulamin ochrony danych osobowych [Szczegółowa instrukcja dla personelu].

## II. Prawa osób, których dane dotyczą

**Art. 5**

Prawa osób, których dane dotyczą:
1) Administrator zapewnia osobom, których dane osobowe są przetwarzane, realizację praw wynikających z przepisów RODO.
2) Osobie, której dane dotyczą, przysługuje w szczególności prawo do dostępu do danych osobowych, ich sprostowania, usunięcia, ograniczenia przetwarzania oraz wniesienia sprzeciwu - w zakresie przewidzianym przepisami prawa.
3) Realizacja praw następuje na wniosek osoby, której dane dotyczą, złożony w formie pisemnej lub elektronicznej.
4) Administrator udziela odpowiedzi bez zbędnej zwłoki, nie później jednak niż w terminie 1 miesiąca od dnia otrzymania wniosku.
5) Administrator może zwrócić się o dodatkowe informacje w celu potwierdzenia tożsamości osoby składającej wniosek.
6) Osobie, której dane dotyczą, przysługuje prawo wniesienia skargi do Prezesa Urzędu Ochrony Danych Osobowych.

## III. Zasady przygotowania analizy ryzyka

**Art. 6**

1. Analiza ryzyka ma na celu zabezpieczenie danych osobowych w sposób adekwatny do zdiagnozowanych zagrożeń. Analiza ryzyka przeprowadzana jest dla zbioru danych i procesów przetwarzania.
2. Administrator zgodnie z przepisem art. 30 RODO prowadzi rejestr czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka. Rejestr obejmuje czynności przetwarzania realizowane przez Stowarzyszenie, w tym czynności realizowane w ramach działalności jego jednostek organizacyjnych. **Wzór rejestru czynności przetwarzania (wykazu zbiorów danych osobowych) stanowi ZAŁĄCZNIK NR 1.**
3. Administrator określa wykaz zagrożeń, które mogą wystąpić podczas przetwarzania danych osobowych. Zagrożenia powinny być identyfikowane w odniesieniu do uprzednio zinwentaryzowanych zbiorów, aktywów oraz procesów przetwarzania.
4. **Schemat analizy ryzyka stanowi ZAŁĄCZNIK NR 2**.

**Art. 7**

1. Administrator wylicza **ryzyko (Ryz)** dla wszystkich zagrożeń i ich skutków w odniesieniu do zdarzeń historycznych według wzoru:

$$Ryz = Pr + His + Sk$$

2. Administrator określa **prawdopodobieństwo (Pr)** wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania. Proponowaną skalę prawdopodobieństwa prezentuje tabela poniżej.
3. Administrator ustala, czy w ostatnich 5 latach miało miejsca zdarzenie mogące mieć wpływ na naruszenie danych osobowych (np. zainfekowanie komputera, włamanie do biura itp.) **(His)**. Proponowaną skalę oceny prezentuje tabela poniżej.
4. Administrator określa **skutki (Sk)** ewentualnego wystąpienia zdiagnozowanego zagrożenia w odniesieniu w szczególności do utraty reputacji/zaufania przez Administratora [przy uwzględnieniu również innych potencjalnych skutków wskazanych w RODO]. Proponowaną skalę skutków prezentuje tabela poniżej.

| **PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA** | **SKALA** |
|---|---|
| zagrożenie niskie | 1 |
| zagrożenie średnie | 2 |
| zagrożenie wysokie | 3 |
| **OCENA HISTORYCZNA W CIĄGU OSTATNICH 5 LAT** | **SKALA** |
| 0 zdarzeń | 0 |
| 1 - 3 zdarzeń | 1 |
| 4 i zdarzeń | 2 |
| **POTENCJALNE SKUTKI WYSTĄPIENIA ZAGROŻENIA** | **SKALA** |
| niskie skutki (artykuł w prasie lokalnej) | 1 |
| średnie skutki (artykuł w prasie regionalnej) | 2 |
| wysokie skutki (artykuł w prasie ogólnopolskiej) | 3 |

5. Wyliczone ryzyko Administrator nakłada na skalę wskazaną w tabeli poniżej, a następnie podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.

| **SKALA WYLICZONEGO RYZYKA WG WZORU: Ryz = Pr + His + Sk** | **REAKCJA NA WYLICZONE RYZYKO** |
|---|---|
| 2-3 | akceptacja ryzyka - zabezpieczenia są wystarczające; nie ma potrzeby stosowania dodatkowych zabezpieczeń |
| 4 - 6 | akceptacja ryzyka lub obniżenie ryzyka zgodnie z decyzją administratora, administrator może zaakceptować ryzyko, lub podjąć działania obniżające ryzyko, np. przeniesienie (outsourcing, |

| | |
|---|---|
| | ubezpieczenie) i/lub unikanie ryzyka (eliminacja działań powodujących ryzyko). |
| 7-8 | obniżenie ryzyka do poziomu akceptowalnego - administrator jest zobowiązany do podjęcia działań obniżających ryzyko, a następnie ponownego przeprowadzenia analizy ryzyka |

6. W przypadku, gdy Administrator decyduje się obniżyć ryzyko lub jest zobowiązany do obniżenia ryzyka, wyznacza listę zabezpieczeń do wdrożenia, termin wdrożenia i osoby odpowiedzialne za ich wdrożenie. **Schemat planu postępowania z ryzykiem stanowi ZAŁĄCZNIK NR 3**.
7. Ponowna analiza ryzyka przeprowadzana jest po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie przez Administratora nowych zbiorów) lub po wprowadzeniu istotnych zmian prawnych.
8. Przyjęty sposób szacowania ryzyka stanowi wewnętrzny model Administratora, dostosowany do skali i charakteru przetwarzania danych osobowych w Stowarzyszeniu.

## IV. Wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe

### Art. 8

1. Obszar przetwarzania danych osobowych obejmuje siedzibę Stowarzyszenia oraz pomieszczenia wykorzystywane przez jego jednostki organizacyjne, w których przetwarzane są dane osobowe.
2. Administrator prowadzi i aktualizuje wykaz miejsc, w których przetwarzane są dane osobowe.
3. Dokumentacja zawierająca dane osobowe przechowywana jest w pomieszczeniach oraz miejscach odpowiednio zabezpieczonych przed dostępem osób nieupoważnionych.
4. Dokumentację papierową oraz elektroniczne nośniki danych przechowuje się w sposób zapewniający ich ochronę przed nieuprawnionym dostępem, utratą, zniszczeniem lub uszkodzeniem.

## V. Środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych (Instrukcja zarządzania)

### Art. 9

1. Administrator realizując Politykę stosuje odpowiednie środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń.
2. Poniższa instrukcja stanowi wykaz procedur oraz stosowanych środków technicznych i organizacyjnych mających na celu, zgodnie z przepisem art. 32 RODO, zabezpieczyć przetwarzane dane osobowe przed: przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją danych osobowych, nieuprawnionym ujawnieniem danych osobowych oraz nieuprawnionym dostępem do danych osobowych.
3. Administrator stosuje w szczególności następujące zabezpieczenia:
   1) zabezpieczenia fizyczne i techniczne;
   2) politykę haseł i zasadę tworzenia kopii zapasowych;
   3) procedurę utylizacji elektronicznych nośników danych i wydruków komputerowych;
   4) procedurę zabezpieczenia systemu informatycznego;
   5) procedurę napraw sprzętu komputerowego;
   6) procedurę nadawania/odwoływania przez administratora upoważnień do przetwarzania danych osobowych,
   7) prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych;
   8) prowadzenie ewidencji osób posiadających klucze do pomieszczeń biurowych Stowarzyszenia.
4. Instrukcja jest aktualizowana, jeśli zajdzie taka potrzeba po przeprowadzeniu analizy ryzyka.

**Art. 10 [zabezpieczenia fizyczne i techniczne]**

1. Drzwi do pomieszczeń biurowych zamykane są na klucz - klucze do pomieszczenia biurowego posiadają członkowie organów administratora oraz inne osoby upoważnione do przetwarzania danych zgodnie z **ZAŁĄCZNIKIEM NR 4** (**ewidencja osób posiadających klucze do pomieszczeń biurowych**). Wejście do sekretariatu / recepcji jest zabezpieczone barierką zamykaną na klucz.
2. Pomieszczenia biurowe/sekretariat po zakończeniu pracy zamykane są przez osoby określone w ust. 1.
3. Klucz do budynku, w którym znajduje się pomieszczenie biurowe/sekretariat posiada: administracja tego budynku, osoby zarządu SPP Nadzieja oraz upoważnieni pracownicy Stowarzyszenia.
4. Dokumentację papierową i nośniki elektroniczne przechowywane w pomieszczeniach zabezpiecza się w szafach zamykanych na klucz. Klucze do szaf, w którym przechowywane są dane osobowe posiadają osoby określone w ust. 1.

**Art. 11 [polityka haseł]**

1. Do komputera administratora, na którym przetwarzane są dane osobowe mają dostęp jedynie osoby do tego uprawnione (personel).
2. Dostęp do komputera na którym przetwarzane są dane osobowe zabezpieczony jest hasłem.
3. Standard hasła: hasło co najmniej 8 -znakowe, składające się z co najmniej małych i dużych liter, cyfr i znaków specjalnych; zmienianie samodzielnie przez użytkowników nie rzadziej niż co 180 dni.
4. Hasło powinno być trudne do odgadnięcia - hasłem nie powinny być powszechnie używane słowa, w szczególności kojarzące się z administratorem.
5. Hasła nie powinny być ujawnianie osobom nieupoważnionym do przetwarzania danych osobowych.
6. Rekomenduje się zapamiętanie hasła. W przypadku jego zapisania, hasło powinno być przechowywane w bezpiecznym miejscu. Nie można: zapisywać haseł na kartkach i w notesach, naklejać haseł na monitorze komputera, przechowywać pod klawiaturą, w szufladzie lub w innych podobny sposób.
7. W przypadku ujawnienia hasła – należy go natychmiast zmienić.
8. Dostęp do pliku, w którym znajdują się dane osobowe powinien być również zabezpieczony hasłem.
9. Dyski przenośne/pendrive powinny być zabezpieczane hasłem/programem szyfrującym.
10. Urządzenia mobilne (smartfon, tablet, inne) powinny być zabezpieczone mechanizmem uwierzytelniania (np. hasło, symbol itp.).

**Art. 12 [zasady tworzenia kopii zapasowych]**

1. Komputer służący do przetwarzania danych osobowych zabezpiecza się przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej poprzez stosowanie zasilaczy awaryjnych bądź poprzez tworzenie kopii zapasowych.
2. Tworzy się kopie zapasowe dysku twardego komputera, na którym przetwarzane są dane osobowe.
3. Kopie zapasowe tworzone są na dysku zewnętrznym/przenośnym.
4. Kopie zapasowe tworzone są manualnie.
5. Kopie zapasowe tworzy się co najmniej raz w miesiącu.
6. Kopie zapasowe przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem.
7. Dostęp do kopii zapasowych mają wyłącznie osoby upoważnione przez Administratora, w zakresie wynikającym z powierzonych im obowiązków.
8. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

**Art. 13 [procedura utylizacji elektronicznych nośników danych i wydruków komputerowych]**

1. Uszkodzone lub przestarzałe nośniki danych są niszczone w sposób fizyczny.
2. Nośniki danych (dyski, pendrive, pamięci urządzeń) muszą być wyczyszczone specjalistycznym oprogramowaniem zanim zostaną przekazane poza obszar przetwarzania danych administratora.
3. Dokumentacja papierowa zawierająca dane osobowe powinna być niszczona w niszczarce lub w taki sposób, który uniemożliwia jej odtworzenie.

**Art. 14 [procedura zabezpieczenia systemu informatycznego]**

1. Stosowane zabezpieczenia mają na celu zabezpieczenie systemów informatycznych przed nieautoryzowanym dostępem do sieci lokalnej np. przez programy szpiegujące.
2. W komputerze, na którym przetwarzane są dane osobowe stosuje się oprogramowanie antywirusowe oraz zaporę firewall.
3. Konfigurację urządzeń sieciowych oraz sprzętu IT dokonuje się w taki sposób, aby zabezpieczyć jej przed nieuprawnionym dostępem.
4. Stosuje się wyłącznie legalne oprogramowanie.
5. Dokonuje się systematycznej aktualizacji oprogramowania.
6. Do sieci WIFI dostęp posiadają wyłącznie osoby upoważnione do przetwarzania danych osobowych.
7. W komputerze stosuje się bezpieczny wygaszacz ekranu, aktywowany najpóźniej po 10 minutach nieaktywności użytkownika - powrót do pracy wymaga wpisania hasła.
8. Monitor komputera ustawiony jest w sposób uniemożliwiający wgląd w dane przez osoby postronne.
9. Administrator stosuje szyfrowanie protokołem SSL.
10. Na stronie internetowej administratora nie stosuje się formularza kontaktowego.
11. Administrator odpowiada za optymalizację sprzętu elektronicznego (zasobów IT).
12. Administrator odpowiada za identyfikację i przyjmowanie zgłoszeń o nieprawidłowościach oraz za poprawność działania zasobów IT
13. Naprawy sprzętu elektronicznego dokonywane w zewnętrznych serwisach wymagają usunięcia nośników danych osobowych lub usunięcia z nich danych osobowych. W przypadku naprawy sprzętu z danymi osobowymi wymagane jest zawarcie umowy powierzenia z serwisem (bezpieczna naprawa).
14. Czynności konserwacyjne i naprawcze wykonywane przez osoby nieposiadające upoważnień do przetwarzania danych (np. specjalistów z firm zewnętrznych) muszą być przeprowadzane pod nadzorem osób upoważnionych

## VI. Regulamin ochrony danych osobowych [Szczegółowa instrukcja dla personelu]

**Art. 15**

1. W przypadku, gdy w pomieszczeniu biurowym/sekretariacie, w którym następuje przetwarzanie danych osobowych znajduje się część ogólnodostępna oraz część, w której przetwarzane są dane osobowe – część, w której są przetwarzane dane osobowe powinna być wyraźnie oddzielona od ogólnodostępnej. Wydzielenie części pomieszczenia, w której przetwarza się dane osobowe może być w szczególności dokonane poprzez montaż barierek, lad, ścianek lub odpowiednie ustawienie mebli biurowych uniemożliwiające lub co najmniej ograniczające niekontrolowany dostęp osób niepowołanych do zbiorów danych osobowych przetwarzanych w danym pomieszczeniu.
2. Przebywanie osób trzecich w pomieszczeniu, gdzie są przetwarzane dane osobowe dopuszczalne jest tylko w obecności osoby upoważnionej do przetwarzania danych osobowych.
3. Pomieszczenie biurowe/sekretariat na czas nieobecności osoby upoważnionej powinno być zamykane w sposób uniemożliwiający dostęp do niego osób trzecich.

4. Opuszczenie pomieszczenia biurowego/sekretariatu musi wiązać się z zastosowaniem dostępnych środków zabezpieczających to pomieszczenie przed wejściem osób niepowołanych. W szczególności w razie planowanej, choćby chwilowej, nieobecności osoby upoważnionej do przetwarzana danych osobowych obowiązany jest on umieścić zbiory występujące w formach tradycyjnych w odpowiednio zabezpieczonym miejscu ich przechowywania.
5. W przypadku przebywania osób postronnych w pomieszczeniu biurowym, monitor stanowiska dostępu do danych osobowych przetwarzanych w formie elektronicznej powinien być ustawiony w taki sposób, aby uniemożliwić tym osobom wgląd w dane.
6. Osoba użytkująca komputer przenośny (lub inny nośnik danych) zawierający dane osobowe zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania w szczególności poza pomieszczeniem, w którym przetwarza się dane osobowe, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych danych osobowych (hasło dostępu, zabezpieczenie plików).

**Art. 16**

1. Osoba upoważniona do przetwarzania danych osobowych odpowiada za zabezpieczenie przed zniszczeniem, uszkodzeniem oraz utratą sprzętu elektronicznego (komputerów, urządzeń biurowych, tabletów i smartfonów).
2. Niedopuszczalne jest instalowanie, podłączanie dodatkowych urządzeń lub demontaż urządzeń już podłączonych.
3. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do usuwania tymczasowych plików z nośników/dysków z miejsc, gdzie dostęp do nich mogłyby mieć osoby nieupoważnione.

**Art. 17**

1. Zabronione jest udostępnianie komputera osobom nieupoważnionym do przetwarzania danych osobowych.
2. Użytkownik komputera rozpoczyna pracę zalogowaniem, a kończy wylogowaniem.
3. W przypadku tymczasowego odejścia od komputera użytkownik powinien włączyć tzw. bezpieczny wygaszacz lub wylogować się z systemu.
4. Zabrania się uruchamiania jakiejkolwiek aplikacji lub programu z nieznanych źródeł - w szczególności dotyczy to programów przesłanych za pomocą poczty elektronicznej lub wskazanych w formie odnośnika internetowego.
5. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć wszelkie nośniki, na których znajdują się dane osobowe.

**Art. 18**

1. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do stosowania tzw. „**zasady czystego biurka**”. Zasada ta polega na zabezpieczaniu dokumentów oraz elektronicznych nośników danych osobowych przed kradzieżą lub wglądem osób nieupoważnionych poprzez ich zamknięcie np. w szafach, biurkach. Po zakończeniu pracy nie można na biurku zostawiać żadnych dokumentów zawierających dane osobowe.
2. Osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do niszczenia dokumentacji papierowej w niszczarce lub w taki sposób, który uniemożliwia jej odtworzenie. Zabrania się wyrzucania niezniszczonych dokumentów do kosza.
3. Zabrania się pozostawiania dokumentów w miejscach dostępnych dla osób nieupoważnionych.
4. Zabrania się pozostawiania w biurze osób nie będących uprawnionymi do przetwarzania danych osobowych. W takiej sytuacji przed opuszczeniem biura należy poprosić osobę o opuszczenie biura i poczekanie na korytarzu.
5. Zabrania się pozostawiania biura bez zamknięcia.

6. Dokumentacja powinna być przechowywana w szafach zamykanych na klucz. Klucze do szaf przechowywane są w miejscu uniemożliwiającym dostęp do nich przez osoby nieupoważnione.

**Art. 19**

1. Osoby personelu nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pen-drive, płyt CD, DVD).
2. Dane osobowe wynoszone poza organizację muszą być zaszyfrowane (szyfrowane dyski przenośne, pliki zabezpieczone hasłem, zabezpieczone smartfony).
3. Dokumentację papierową należy przewozić w zamkniętych teczkach, uniemożliwiających przypadkowe zgubienie części dokumentów.

**Art. 20**

1. Zabronione jest instalowanie programów z Internetu bez konsultacji z informatykiem lub prezesem zarządu. W przypadku nie zastosowania się do tej zasady dana osoba ponosi odpowiedzialność za szkody spowodowane przez takie oprogramowanie.
2. Zabrania się wchodzenia na strony z nielegalnym oprogramowaniem oraz na strony w szczególności zagrożone atakami hackerskimi.
3. Zabronione jest włączanie w opcjach przeglądarki internetowej autouzupełniania formularzy i zapamiętywania haseł.

**Art. 21**

1. Zaleca się nie przesyłanie plików z danymi osobowymi pocztą elektroniczną. W przypadku konieczności przesłania plików z danymi osobowymi pocztą elektroniczną (plik Word, Excel, Pdf lub inne) - przed wysłaniem ich do osób trzecich powinny być zabezpieczone hasłem, hasło natomiast powinno być przekazane odbiorcy telefonicznie lub wiadomością SMS.
2. W przypadku zabezpieczenia plików hasłem, obowiązuje minimum 6 znaków: duże i małe litery i cyfry lub znaki specjalne.
3. Należy zwracać szczególną uwagę na poprawność adresu odbiorcy poczty elektronicznej.
4. Nie wolno otwierać załączników w mailach od nieznanych odbiorców.
5. Nie wolno otwierać linków w mailach od nieznanych odbiorców.
6. Należy zgłaszać prezesowi przypadki podejrzanych e-maili.
7. Nie należy korzystać z poczty służbowej do celów prywatnych.
8. Wysyłanie wiadomości e-mail do wielu adresatów jest dopuszczalne tylko z wykorzystaniem opcji - UDW (ukryte do wiadomości).
9. Należy nie rzadziej niż co 3 miesiące usuwać niepotrzebne wiadomości e-mail.

**Art. 22**

1. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadomienia administratora w przypadku stwierdzenia lub podejrzenia naruszenia ochrony danych osobowych.
2. Do sytuacji wymagających powiadomienia, należą w szczególności:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i/lub dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu elektronicznego przed wyciekiem/kradzieżą/utratą danych osobowych;
   3) niestosowanie zasady czystego biurka;
   4) niestosowanie zasady czystego ekranu;
   5) niezamykanie biura.
3. Do incydentów wymagających powiadomienia, należą:
   1) zdarzenia losowe zewnętrzne ( np. pożar, utrata zasilania);
   2) zdarzenia losowe wewnętrzne (np. awaria sprzętu elektronicznego);
   3) inne incydenty (np. kradzież danych, atak hackerski, włamanie do sekretariatu/biura).
4. Przykłady incydentów wymagające reakcji administratora:
   1) ślady wskazujące na próbę włamania;

2) dokumentacja jest niszczona bez użycia niszczarki lub w taki sposób, który umożliwia jej odtworzenie;
3) niezabezpieczenie pomieszczeń/szaf, gdzie przechowywane są dane osobowe;\
4) ustawienie monitorów pozwalające na wgląd osób nieupoważnionych do przetwarzania danych osobowych;
5) udostępnienie danych osobowych osobom nieupoważnionym;
6) inne zachowania niezgodne z zasadami wyznaczonymi w niniejszej polityce ochrony danych osobowych.

5. W przypadku stwierdzenia wystąpienia incydentu, administrator prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki;
   2) inicjuje ewentualne działania dyscyplinarne;
   3) działa na rzecz przywrócenia działań organizacji po wystąpieniu incydentu;
   4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.
6. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. **Formularz rejestracji naruszenia ochrony danych osobowych stanowi ZAŁĄCZNIK NR 5**.
7. Zabrania się świadomego lub nieumyślnego wywoływania incydentów przez osoby upoważnione do przetwarzania danych.

**Art. 23 (osoby przetwarzające dane osobowe)**

1. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do:
   1) przetwarzania danych osobowych wyłącznie w celu i w zakresie powierzonych jej zadań;
   2) zachowania w tajemnicy danych osobowych;
   3) niewykorzystywania danych osobowych w celach niezgodnych z zakresem i celem powierzonych jej zadań;
   4) zachowania w tajemnicy sposobów zabezpieczenia danych osobowych.
2. Zabrania się przekazywania bezpośrednio lub przez telefon danych osobowych osobom nieupoważnionym lub osobom których tożsamości nie można zweryfikować lub osobom podszywającym się pod kogoś innego.
3. Zabrania się przekazywania lub ujawniania danych osobom lub instytucjom, które nie mogą wykazać się jasną podstawą prawną do dostępu do takich danych.
4. Każda z osób dopuszczonych do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych osobowych przed przypadkowym lub niezgodnym z prawem zniszczeniem, utratą, modyfikacją, nieuprawnionym ujawnieniem, nieuprawnionym dostępem do danych osobowych oraz przetwarzaniem.

**Art. 24**

1. Administrator dopuszcza do przetwarzania danych osobowych wyłącznie osoby do tego upoważnione na mocy uregulowań wewnętrznych obowiązujących w tym zakresie w Stowarzyszeniu.
2. **Wzór upoważnienia do przetwarzania danych osobowych/odwołania upoważnienia do przetwarzania danych osobowych stanowi ZAŁĄCZNIK NR 6.** Upoważnienia nadawane są do zbiorów (dla kategorii danych). Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
3. Dostęp do danych osobowych i ich przetwarzanie bez odrębnego upoważnienia administratora lub upoważnionej przezeń osoby może mieć miejsce wyłącznie w przypadku działań podmiotów upoważnionych na mocy odpowiednich przepisów prawa do dostępu i przetwarzania danych określonej kategorii.

**Art. 25**

1. Administrator zapewnia kontrolę nad dostępem do danych osobowych - kontrola ta w szczególności realizowana jest poprzez ewidencjonowanie osób przetwarzających dane osobowe oraz wdrożenie procedur udzielania dostępu do tych danych.
2. **Ewidencja osób upoważnionych do przetwarzania danych osobowych** stanowi **ZAŁĄCZNIK NR 7.** Ewidencja obejmuje wszystkie osoby upoważnione do przetwarzania danych osobowych w Stowarzyszeniu, w tym osoby przetwarzające dane w ramach jego jednostek organizacyjnych
3. W przypadku powierzenia przetwarzania danych do podmiotu przetwarzającego, administrator jest zobowiązany do sporządzenia z nim umowy powierzenia danych, stanowiącej podstawę upoważnienia dla osób z podmiotu przetwarzającego.

**Art. 26**

1. Administrator zapewnia zaznajomienie osób upoważnionych do przetwarzania danych osobowych z powszechnie obowiązującymi przepisami prawa, uregulowaniami wewnętrznymi, a także technikami i środkami ochrony tych danych stosowanymi u administratora.
2. **Wzór oświadczenia o zapoznaniu się z treścią polityki ochrony danych osobowych wraz ze zobowiązaniem do przestrzegania tajemnicy danych osobowych** stanowi **ZAŁĄCZNIK NR 8**.

## VII. Postanowienia końcowe

**Art. 27**

1. Stowarzyszenie przetwarza dane osobowe na podstawie powszechnie obowiązujących przepisów prawa.
2. Dane osobowe mogą być udostępniane tylko zgodnie z powszechnie obowiązującymi przepisami prawa.
3. Personel przed dopuszczeniem do przetwarzania danych osobowych zobowiązany jest do zapoznania się i stosowania zapisów niniejszej Polityki oraz przepisów prawa powszechnie obowiązującego.
4. W sprawach nieuregulowanych zastosowanie mają odpowiednie przepisy aktów prawnych powszechnie obowiązujących.
5. Organy oraz osoby kierujące jednostkami organizacyjnymi Stowarzyszenia są zobowiązane do zapewnienia stosowania niniejszej Polityki w zakresie działalności danej jednostki oraz do współpracy z Zarządem Stowarzyszenia w sprawach dotyczących ochrony danych osobowych.

**Art. 28**

1. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszej Polityki potraktowane będą jako ciężkie naruszenie obowiązków pracowniczych lub naruszenie zasad współpracy.
2. Postępowanie sprzeczne z niniejszą Polityką może być uznane przez administratora za naruszenie przepisów RODO oraz innych powszechnie obowiązujących przepisów prawa.

*Podpisy członków Zarządu*

W oryginale

Prezes
Zarządu Stowarzyszenia
Pomocy Potrzebującym „Nadzieja”

dr Roman Biskupski

| **Wykaz załączników:** | |
|---|---|
| **Załącznik 1** | Wzór rejestru czynności przetwarzania (wykazu zbiorów danych osobowych) |
| **Załącznik 2** | Schemat analizy ryzyka |
| **Załącznik 3** | Schemat planu postępowania z ryzykiem |
| **Załącznik 4** | Ewidencja osób posiadających klucze do pomieszczeń biurowych Stowarzyszenia |
| **Załącznik 5** | Formularz rejestracji naruszenia ochrony danych osobowych |
| **Załącznik 6** | Wzór upoważnienia do przetwarzania danych osobowych/ odwołania upoważnienia do przetwarzania danych osobowych |
| **Załącznik 7** | Ewidencja osób upoważnionych do przetwarzania danych osobowych |
| **Załącznik 8** | Wzór oświadczenia o zapoznaniu się z treścią polityki ochrony danych osobowych wraz ze zobowiązaniem do przestrzegania tajemnicy danych osobowych |

Zatwierdzam.

W oryginale

Prezes
Zarządu Stowarzyszenia
Pomocy Potrzebującym Nadzieja

dr Roman Biskupski