POLITYKA OCHRONY DANYCH OSOBOWYCH
w Stowarzyszeniu Lokalna Grupa Działania ,,EUROGALICJA”
z siedzibą: 36-050 Sokołów Małopolski, ul. Rzeszowska 29a
z dnia 10 sierpnia 2018

Niniejsza Polityka Ochrony Danych Osobowych w Stowarzyszeniu Lokalna Grupa Działania ,,EUROGALICJA” z siedzibą: 36-050 Sokołów Małopolski, ul. Rzeszowska 29a [zwana dalej: Polityką] została sporządzona aby wykazać, że dane osobowe są przetwarzane i zabezpieczone zgodnie z wymaganiami 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) [dalej: RODO]

I. Postanowienia ogólne

Art. 1

1. Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z RODO.
   Stowarzyszenie Lokalna Grupa Działania ,,EUROGALICJA”z siedzibą: 36-050 Sokołów Małopolski, ul. Rzeszowska 29a nie jest zobowiązane do powołania inspektora ochrony danych. Stowarzyszenie Lokalna Grupa Działania ,,EUROGALICJA”z siedzibą: 36-050 Sokołów Małopolski, ul. Rzeszowska 29a nie powołuje inspektora ochrony danych.

Art. 2

Ilekroć w Polityce jest mowa o :

a) **Stowarzyszeniu** - rozumie się przez to Stowarzyszenie Stowarzyszenie Lokalna Grupa Działania ,,EUROGALICJA”z siedzibą: 36-050 Sokołów Małopolski, ul. Rzeszowska 29a,
b) **Administratorze** - rozumie się przez to Stowarzyszenie, w imieniu, którego działa zarząd,
c) **pracowniku** - osobie wykonującej czynności w szczególności w oparciu o stosunek pracy, umowy cywilnoprawne, staż, praktykę, stosunek wynikający z członkostwa w Stowarzyszeniu,
d) **osobie upoważnionej do przetwarzania danych osobowych** - rozumie się przez to pracownika, który został upoważniony przez Administratora do przetwarzania danych osobowych,
e) **rozliczalności** - rozumie się przez to właściwość zapewniającą, że działanie podmiotu może być przypisane w sposób jednoznaczny, tylko temu podmiotowi,
f) **integralności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
g) **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie są udostępniane nieupoważnionym podmiotom,
h) **aktywach** - środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych,

i) **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,
j) **zagrożeniu** - potencjalne naruszenie ochrony danych osobowych,
k) **skutkach** - rezultaty potencjalnego naruszenia ochrony danych osobowych,
l) **ryzyku** - prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje określone skutki dla danych osobowych.

Art. 3

1. Celem Polityki jest ochrona danych osobowych przetwarzanych przez Stowarzyszenie w zakresie określonym przepisami prawa.
2. Stowarzyszenie zobowiązuje się chronić dane osobowe przetwarzane w kartotekach, skorowidzach, księgach, wykazach, systemach informatycznych w zakresie przewidzianym przepisami.
3. Stowarzyszenie realizując Politykę dołoży szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane te były:
   a) przetwarzane zgodnie z prawem,
   b) zbierane dla oznaczonych, zgodnych z prawem celów i niepoddawane 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.

Art. 4

Polityka zawiera w szczególności:
a) zasady przygotowania analizy ryzyka,
b) wykaz pomieszczeń tworzących obszar, w którym przetwarzane są dane osobowe,
c) środki techniczne i organizacyjne niezbędne do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych [Instrukcja zarządzania],
d) Regulamin Ochrony Danych Osobowych [instrukcja dla pracowników].

II. Zasady przygotowania analizy ryzyka

Art. 5

1. Analiza ryzyka ma na celu zabezpieczenie danych osobowych w sposób adekwatny do zdiagnozowanych zagrożeń. Analiza ryzyka przeprowadzana jest dla zbioru lub grupy zbiorów lub dla procesów przetwarzania.
2. Administrator zgodnie z przepisem art. 30 RODO prowadzi rejestr czynności przetwarzania. Rejestr stanowi podstawę do przeprowadzenia analizy ryzyka. **Wykaz 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. 6

1. Administrator wylicza **ryzyko [RYZ]** dla wszystkich zagrożeń i ich skutków wg wzoru:
   RYZ = PR x SK
2. Administrator określa **prawdopodobieństwo [PR]** wystąpienia poszczególnych zagrożeń w zbiorze lub w procesie przetwarzania. Proponowaną skalę prawdopodobieństwa prezentuje tabela w ust. 3.
3. Administrator określa **skutki [SK]** ewentualnego wystąpienia zdiagnozowanego zagrożenia w odniesieniu do utraty reputacji/zaufania przez Administratora. Proponowaną skalę skutków prezentuje tabela poniżej.

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**SKALA**
zagrożenie wysokie	3
zagrożenie średnie	2
zagrożenie niskie	1
POTENCJALNE SKUTKI WYSTĄPIENIA ZAGROŻENIA	**SKALA**
wysokie skutki (zagrożenie dla kontynuacji działania Stowarzyszenia, artykuł w prasie ogólnopolskiej)	3
średnie skutki (brak poważnego wpływu na funkcjonowanie Stowarzyszenia, artykuł w prasie regionalnej)	2
niskie skutki (nikły wpływ na funkcjonowanie Stowarzyszenia, artykuł w prasie lokalnej)	1

4. 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 x SK	**REAKCJA NA WYLICZONE RYZYKO**
9	DUŻE RYZYKO obniżamy ryzyko do poziomu akceptowalnego - Administrator jest zobowiązany do podjęcia działań obniżających ryzyko, a następnie ponownego przeprowadzenia analizy ryzyka .
3-6	ŚREDNIE RYZYKO akceptujemy ryzyko lub obniżamy ryzyko zgodnie z decyzją Administratora. Administrator może podjąć działania obniżające ryzyko, np. przeniesienie (outsourcing, ubezpieczenie) i/lub unikanie ryzyka (eliminacja działań powodujących ryzyko).
1-2	NISKIE RYZYKO akceptujemy ryzyko - zabezpieczenia są wystarczające; nie ma potrzeby stosowania dodatkowych zabezpieczeń

5. 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**.

6. Ponowna analiza ryzyka przeprowadzana jest po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie przez Administratora nowych zbiorów) lub po wprowadzeniu istotnych zmian prawnych.

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

Art. 7

1. Siedziba Stowarzyszenia znajduje się w Sokołowie Małopolskim, ul. Rzeszowska 29a.
2. Administrator danych przetwarza dane osobowe w swojej siedzibie wskazanej w ust. 1.
3. Obszar przetwarzania danych osobowych obejmuje pomieszczenia nr 3 i 4 położone na piętrze budynku mieszczącego się przy ul. Rzeszowskiej 29a w Sokołowie Małopolskim.
4. W pomieszczeniach biurowych nr 3 i 4, zamykanych na klucz, znajdują się szafki zaopatrzone w zamki, w których przechowywane są kartoteki, segregatory, skorowidze zawierające dane osobowe przetwarzane przez Stowarzyszenie.

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

Art. 8

1. Stowarzyszenie 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. Stowarzyszenie 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 naprawy 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. 9 [zabezpieczenia fizyczne i techniczne]

Drzwi do pomieszczeń biurowych i budynku zamykane są na klucz. Dodatkowo pomieszczenia biurowe zabezpieczone są alarmem Klucze do pomieszczeń biurowych i budynku oraz do skrzynki z alarmem posiadają osoby wskazane w **ewidencji osób posiadających klucze do budynku, pomieszczeń biurowych Stowarzyszenia oraz skrzynki z alarmem** stanowiącej **ZAŁĄCZNIK NR 4** do niniejszej Polityki.

1. Po zakończeniu pracy osoby określone w ust. 1 zamykają pomieszczenia biurowe, drzwi do budynku oraz za pomocą hasła włączają alarm.
2. Dokumentację papierową i nośniki elektroniczne przechowywane w pomieszczeniach zabezpiecza się w szafkach zamykanych na klucz. Klucze do szaf, w którym przechowywane są dane osobowe posiadają wyłącznie osoby upoważnione.

Art. 10 [polityka haseł]

1. Do komputerów Administratora, na których są przetwarzane dane osobowe mają dostęp jedynie osoby do tego upoważnione (pracownicy, członkowie zarządu, członkowie komisji rewizyjnej).
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 liter i cyfr; zmieniane samodzielnie przez użytkowników nie rzadziej niż co 60 dni.
4. Hasło powinno być trudne do odgadnięcia - hasłem nie powinny być powszechnie używane słowa, w szczególności kojarzące się z Administratorem.
5. Hasło nie powinno być ujawnianie osobom nie upoważnionym 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 lub w szufladzie.
7. W przypadku ujawnienia hasła – należy go natychmiast zmienić.
8. Dostęp do pliku, w którym znajdują się dane osobowe powinien być zabezpieczony hasłem.
9. Dyski przenośne/pendrive powinny być zabezpieczane hasłem/programem szyfrującym.
10. Urządzenia mobilne (smartfon, tablet, inne) powinny być zabezpieczone mechanizmem uwierzytelniania.

Art. 11 [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.
8. Kopie zapasowe usuwa się niezwłocznie po ustaniu ich użyteczności.

Art. 12 [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. 13 [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 zapory 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 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.

V. Regulamin Ochrony Danych Osobowych [Instrukcja dla pracowników].

Art. 14

1. W przypadku, gdy w pomieszczeniu biurowym, 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. Pomieszczenia biurowe na czas nieobecności osoby upoważnionej powinny być zamykane w sposób uniemożliwiający dostęp do niego osób trzecich.
4. Opuszczenie pomieszczeń biurowych musi wiązać się z zastosowaniem dostępnych środków zabezpieczających te pomieszczenia przed wejściem osób niepowołanych. W szczególności w razie planowanej, choćby chwilowej, nieobecności pracownika upoważnionego do przetwarzania 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 innych 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. 15

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. 16

1. Zabronione jest udostępnianie komputera osobom nieupoważnionym do przetwarzania danych osobowych.
2. Użytkownik komputera rozpoczyna pracę zalogowaniem, a kończy wylogowaniem.
3. Obowiązuje zasada czystego ekranu - tj. użytkownik komputera zobowiązany jest do uniemożliwienia osobom niepowołanym wglądu do danych wyświetlanych na monitorze.
4. W przypadku tymczasowego odejścia od komputera użytkownik powinien włączyć tzw. bezpieczny wygaszacz lub wylogować się z systemu.
5. 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.
6. Po zakończeniu pracy, użytkownik zobowiązany jest wylogować się z systemu informatycznego oraz zabezpieczyć wszelkie nośniki, na których znajdują się dane osobowe.

Art. 17

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 szafkach. 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 szafkach zamykanych na klucz. Klucze do szafek przechowywane są w miejscu uniemożliwiającym dostęp do nich przez osoby nieupoważnione.

Art. 18

1. Pracownicy nie mogą wynosić na zewnątrz niezaszyfrowanych nośników z danymi osobowymi (np. przenośnych dysków twardych, pendrive, płyt CD, DVD, pamięci typu flash).
2. Dane osobowe wynoszone poza obszar przetwarzania danych Administratora muszą być zaszyfrowane (szyfrowane dyski przenośne, zahasłowane pliki, zabezpieczone smartfony).
3. Dokumentację papierową należy przewozić w zamkniętych teczkach, uniemożliwiających przypadkowe zgubienie części dokumentów.

Art. 19

1. Zabronione jest instalowanie programów z Internetu bez konsultacji z informatykiem lub prezesem zarządu. W przypadku nie zastosowania się do tej zasady pracownik 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. 20

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 przesłane do 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 e-mailach od nieznanych odbiorców.
5. Nie wolno otwierać linków w e-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 6 miesięcy usuwać niepotrzebne wiadomości e-mail.

Art. 21

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 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. 22 (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. 23

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 stanowi ZAŁĄCZNIK NR 6.** Upoważnienia nadawane są do zbiorów (dla kategorii osób). Upoważnienia określają zakres operacji na danych, np. tworzenie, usuwanie, wgląd, przekazywanie.
3. **Wzór odwołania upoważnienia do przetwarzania danych osobowych** stanowi **ZAŁĄCZNIK NR 7**.
4. 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. 24

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 8.**

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. 25

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 9**.

VI. Postanowienia końcowe

Art. 26

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. Każdy pracownik 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.

Art. 27

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 karnych zawartych w RODO.

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 pomieszczenia biurowego Stowarzyszenia
Załącznik 5	Formularz rejestracji naruszenia ochrony danych osobowych
Załącznik 6	Wzór upoważnienia do przetwarzania danych osobowych
Załącznik 7	Wzór odwołania upoważnienia do przetwarzania danych osobowych
Załącznik 8	Ewidencja osób upoważnionych do przetwarzania danych osobowych
Załącznik 9	Wzór oświadczenia o zapoznaniu się z treścią polityki ochrony danych osobowych wraz ze zobowiązaniem do przestrzegania tajemnicy danych

	osobowych