REGULAMIN OCHRONY DANYCH OSOBOWYCH
określający **politykę bezpieczeństwa danych osobowych**
w stowarzyszeniu Sieć Obywatelska Watchdog Polska
(przyjęty uchwałą zarządu nr 1/VIII/2014 z 26.08.2014 r.)

§ 1 Zakres Regulaminu

1. Niniejszy Regulamin opracowany został w oparciu o Ustawę z dnia 29 sierpnia 1997r. o ochronie danych osobowych, Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych oraz statut stowarzyszenia Sieć Obywatelska Watchdog Polska (zwane dalej Stowarzyszeniem).
2. Regulamin określa zakres, zasady oraz tryb przetwarzania i udostępniania danych osobowych, sposób zabezpieczania zbiorów danych osobowych będących w posiadaniu Stowarzyszenia, a także obowiązki administratora danych osobowych, administratora bezpieczeństwa informacji oraz praw osób, których dane Stowarzyszenie przetwarza.
3. Regulamin określa środki techniczne, organizacyjne niezbędne dla zapewnienia poufności, integralności, rozliczalności przetwarzania danych osobowych.

§2 Pojęcia używane w Regulaminie

Przez użyte w treści Regulaminu sformułowania należy rozumieć:

- **bezpieczeństwo informacji** - rozumiane jako zachowanie jej poufności, integralności przy przesyłaniu i przetwarzaniu, dostępności;
- **dane osobowe** - wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania na ich podstawie, osoby fizycznej,
- **zbiór danych** - każdy posiadający strukturę zestaw danych osobowych dostępny wg określonych kryteriów, w którym dane te mogą być przetwarzane.
- **przetwarzanie danych** - wszelkie operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
- **powierzanie przetwarzania danych** zgodnie z art. 31 ustawy o ochronie danych osobowych, odnosi się do przekazywania innym podmiotom administrowanych danych.
- **system informatyczny** - zespół współpracujących ze sobą urządzeń, programów, procedur i narzędzi programowych zastosowanych w celu przetwarzania danych,
- **usuwanie danych** - zniszczenie danych osobowych, lub także ich modyfikacja, która nie pozwala na ustalenie tożsamości osoby, której dane dotyczą,
- **administrator danych osobowych** - administratorem danych osobowych jest stowarzyszenie Sieć Obywatelska Watchdog Polska.
- **administrator bezpieczeństwa informacji** - osoba odpowiedzialna za bezpieczeństwo danych osobowych w systemie informatycznych lub innym, zawężonym zbiorze danych osobowych, wyznaczona przez administratora danych osobowych,
- **identyfikator użytkownika (login)** - ciąg znaków literowych, cyfrowych lub innych, jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym,
- **hasło** - ciąg znaków literowych, cyfrowych lub innych, przypisany do identyfikatora użytkownika, znany jedynie osobie uprawnionej do pracy w systemie informatycznym,

- **uwierzytelnianie** - rozumie się przez to działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu,
- **integralność danych** - rozumie się przez to właściwość zapewniającą, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
- **poufności danych** - rozumie się przez to właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym podmiotom,
- **konto poczty służbowej** - elektroniczne konto pocztowe utworzone i utrzymywane przez stowarzyszenie Sieć Obywatelska Watchdog Polska w ramach usługi hostingowej świadczonej przez usługodawców.

§3 Odpowiedzialność za bezpieczeństwo informacji

1. Celem zabezpieczenia zbiorów danych osobowych darczyńców/czyń, odbiorców/czyń, członków/ień, wolontariuszy/ek, klientów/ek, pracowników/c oraz innych osób współpracujących, wprowadzono mechanizmy techniczne i organizacyjne **uniemożliwiające** dostęp do zbioru danych osobom nieuprawnionym, bądź zbieranie ich przez osoby nieuprawnione oraz zabezpieczenie danych przed ich uszkodzeniem lub zniszczeniem.
2. Administrator bezpieczeństwa informacji przeprowadza szkolenia, instruktaż na stanowisku pracy oraz stałe poradnictwo dla pracowników w zakresie realizowania wytycznych polityki bezpieczeństwa danych osobowych.
3. Stowarzyszenie może powierzyć przetwarzanie danych podmiotom, z którymi zostanie podpisana umowa powierzenia przetwarzania danych.

§4 Informacja o zbiorach danych

1. Stowarzyszenie jako administrator danych osobowych przetwarza informacje wymienione w Załączniku 6.
2. Zbiory danych osób wymienionych w punktach 1-4 Załącznika 6 nie podlegają zgłoszeniu do Generalnego Inspektora Danych Osobowych na podstawie art. 43 ust. 1 pkt. 4 ustawy o ochronie danych osobowych (uodo).
3. Zbiory wymienione w punktacj 5-11 Załącznika 6 podlegają zgłoszeniu do Generalnego Inspektora Danych Osobowych na podstawie artykułu 40 uodo.
4. Wzór zgłoszenia określa Rozporządzeniu Ministra Spraw Wewnętrznych i Administracji, a Generalny Inspektor Danych Osobowych udostępnia je na elektronicznej platformie: https://egiodo.giodo.gov.pl/index.dhtml.

§ 5 Dostęp do danych osobowych przetwarzanych przez Stowarzyszenie

1. Dostęp do zbiorów danych osobowych mają członkowie/inie pracownicy/e, wolonatriusze/szki i osoby zatrudnione na umowy cywilno-prawne, które uzyskały pisemne upoważnienie wydane przez Zarząd Stowarzyszenia (wzór właściwej uchwały stanowi Załącznik 1) oraz po uprzednim złożeniu oświadczenia, o którym mowa w pkt 2.
2. Każda z osób, która uzyskała dostęp do zbiorów danych podpisuje oświadczenie o przestrzeganiu przepisów w zakresie zachowania poufności i inegralności danych, dbania o ich bezpieczeństwo oraz korzystania z nich wyłącznie w ramach udzielonego upoważnienia i na podstawie prawa (wzór oświadczenia stanowi Załącznik 2).
3. Oświadczenia przechowywane są w specjalnie wydzielonym segregatorze, wraz z uchwałami Zarządu udzielającymi upoważnień, a ich podpisywanie nadzorowane jest przez Zarząd Stowarzyszenia.

§6 Ochrona danych dostępnych w siedzibie Stowarzyszenia

1. Zbiory danych osobowych są przechowywane i przetwarzane w pomieszczeniach Stowarzyszenia.
2. Dostęp do biura Stowarzyszenia chroniony jest przez zamki i alarm.
3. Dane osobowe przetwarzane w siedzibie Stowarzyszenia są zabezpieczane w szafach metalowych, zamykanych na klucz.
4. Dostęp do szaf określa procedura stanowiąca Załącznik 3 do niniejszego Regulaminu.
5. Upoważnienia dostępu do szaf metalowych udzielane są przez Uchwałę Zarządu (Załącznik 4).
6. Bezpieczeństwo danych osobowych zapewniane jest przez Administratora Bezpieczeństwa Informacji i osoby, które uzyskały pisemne upoważnienie Zarządu oraz podpisały oświadczenie, o którym mowa w §5 pkt. 2.
7. Zbiory danych dostępne w formie papierowej mogą zostać przekazane na podstawie umowy powierzenia zewnętrznym podmiotom, w tym księgowości.

§ 7 Ochrona danych osobowych przetwarzanych w systemie informatycznym

1. System komputerowy Stowarzyszenia Sieć Obywatelska Watchdog Polska tworzą zestawy komputerowe mające połączenie z serwerem i dostęp do sieci publicznej Internet, służące do obsługi procesów organizacyjnych Stowarzyszenia;
2. Konserwację, modyfikację oraz uaktualnienie oprogramowania wykonuje Administrator Bezpieczenstwa Informacji lub osoby przez niego wyznaczone (Załącznik 5), a także przedstawiciele autora oprogramowań wdrożonych w Stowarzyszeniu, którzy na podstawie umowy wykonują wymagane operacje w obecności pracowników Stowarzyszenia.
3. Każdy z pracowników pracujący z wykorzystaniem danych osobowych posiada odrębny identyfikator i hasło pozwalające na zidentyfikowanie czasu i sposobu przetwarzania danych w zbiorach.
4. Zbiory danych archiwizowane są co najmniej raz na tydzień na zewnętrznym dysku do tego przeznaczonym i przechowywane w zamkniętej metalowej szafie; oraz wirtualnie u zewnętrznego usługodawcy zatwierdzonego uchwałą Zarządu. Za wykonanie archiwizacji lub ich zlecenie upoważnionym osobom odpowiada Administrator Bezpieczeństwa Informacji.
5. Zakazane jest dokonywanie kopii danych na nośniki informacji, które nie zostały zabezpieczone zgodnie z procedurą opisaną w punkcie 4.
6. Każda osoba posiadająca dostęp do danych zabezpiecza dostęp do katalogów zawierających dane osobowe oraz poczty e-mail za pomocą hasła.
7. Hasło do katalogów z danymi osobowymi zmieniane jest raz na miesiąc i na każde wezwanie Administratora Bezpieczeństwa Informacji.
8. Komputery służbowe chronione są za pomocą programu antywirusowego.
9. Zbiory danych dostępne wirualnie u zewnętrznego usługodawcy zabezpieczone są indywidalnym hasłem zmienianym raz w miesiącu.
10. Zakupowane oprogramowanie (chmura) pozwala na zidentyfikowanie od kiedy dane dostępne są w zbiorze, kiedy nastąpił dostęp do zbiorów konkretnego użytkownika i jakie zmiany zostały dokonane, a także kiedy były przetwarzane i udostępniane.
11. Formularze zgłoszeniowe użytkowane do rekrutacji uczestniców szkoleń przechowywane są na serwerach, które zapewniają bezpieczeństwo informacji.

§ 8 Administrator Bezpieczeństwa Informacji

1. Funkcję administratora bezpieczeństwa informacji w Stowarzyszeniu pełni pracownik/ca lub współpracownik/ca wyznaczony/a przez Zarząd, w drodze uchwały.

2. Administrator bezpieczeństwa informacji nadzoruje przestrzeganie zasad ochrony danych osobowych, o których mowa w art. 36 ust. 1 ustawy o ochronie danych osobowych, będąc odpowiedzialnym za:
   - bezpieczeństwo danych osobowych gromadzonych w systemie informatycznym przy zastosowaniu środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
   - zabezpieczenie danych przed ich udostępnieniem osobom nieupoważnionym, przetwarzaniem z naruszeniem ustawy o ochronie danych osobowych oraz zmianą, utratą, uszkodzeniem lub zniszczeniem;
   - podejmowanie odpowiednich działań – opisanych w punkcie 4 - w przypadku wykrycia naruszeń w systemie zabezpieczeń,
   - przeszkolenie pracowników, prowadzenie instruktażu stanowiskowego oraz stałego poradnictwa w zakresie realizacji polityki bezpieczeństwa danych osobowych w Stowarzyszenia.
3. Osoba przetwarzająca dane w systemie informatycznym obowiązana jest niezwłocznie powiadomić administratora bezpieczeństwa informacji, gdy:
   - stwierdzi naruszenie zabezpieczeń informatycznych,
   - stan urządzeń, zawartość zbioru danych osobowych, ujawnione metody pracy, sposób działania programu lub jakości komunikacji w sieci telekomunikacyjnej mogą wskazywać na naruszenie zabezpieczeń tych danych.
4. Administrator bezpieczeństwa informacji po potwierdzeniu naruszenia systemu informatycznego ma obowiązek:
   - zabezpieczyć ślady pozwalające na określenie przyczyn naruszenia systemu informatycznego,
   - przeanalizować i określić skutki naruszenia informatycznego;
   - określić czynniki, które spowodowały naruszenie systemu informatycznego,
   - dokonać niezbędnych korekt w systemie informatycznym polegających na zabezpieczeniu systemu przed ponownym jego naruszeniem,
   - powiadomić organy ścigania, jeżeli skutki noszą znamiona przestępstwa oraz gdy sposób naruszenia i skutki mogą być powtórzone w innym miejscu lub w przyszłości.
5. System informatyczny powinien zapewnić odnotowanie:
   - daty wprowadzenia i modyfikacji danych osobowych,
   - identyfikatora użytkownika systemu wprowadzającego dane,
   - informację, kiedy i w jakim zakresie dane zostały wygenerowane przez system.

§9 Ochrona danych osobowych - kryteria dostępu

1. Osoba, której dane przetwarzane są przez Stowarzyszenie ma prawo do informacji o:
   - sposobie i zakresie przetwarzania danych osobowych,
   - treści danych,
   - sposobie udostępniania danych oraz odbiorcach lub kategorii odbiorców danych.

oraz żądania uzupełnienia, uaktualnienia i sprostowania danych osobowych.

2. Informacji, o których mowa w ust. 1 Zarząd Stowarzyszenia jest zobowiązany udzielić w terminie 30 dni od otrzymania wniosku.

Załącznik 1

Uchwała Zarządu

stowarzyszenia **Sieć Obywatelska Watchdog Polska**

nr …… z dnia ……..

w sprawie **upoważnienia wybranych osób do przetwarzania danych osobowych**

Zarząd Stowarzyszenia Sieć Obywatelska Watchdog Polska działając w oparciu o § 24 ust. 1 Statutu oraz o § 5 ust. 2 Regulaminu Ochrony Danych Osobowych, ustala co następuje:

§ 1

Zezwala się następującym osobom:
…….
…….
na przetwarzanie danych osoby w następujących zbiorach:
…….
…….

§ 2

Uchwała wchodzi w życie z dniem podjęcia.

Głosowanie:

za	osoby ….
przeciw	osób ……
wstrzymało się	osób ….

Uchwała została przyjęta stosunkiem …./…. oddanych głosów.

Załącznik 2

DATA i MIEJSCOWOŚĆ

Jako osoba, która uzyskał dostęp do następujących zbiorów danych:

…….
…….
…….

Ja niżej podpisana/y oświadczam, że:

- będę przestrzegać przepisów w zakresie zachowania inegralności danych;
- dbać o bezpieczeństwo danych w zbiorach;
- zachowam poufność danych;
- będę przetwarzać dane wyłącznie w ramach udzielonego upoważnienia Zarządu, zgodnie z przepisami prawa, Regulaminu Ochrony Danych Osobowych stowarzyszenia Sieć Obywatelska Watchdog Polska i na podstawie udzielonej zgody na przetwarzanie danych.

.....

Załącznik 3

Procedura zamykania szaf z dokumentami zawierającymi dane osobowe

Wszystkie dokumenty, które zawierają dane osobowe muszą być przechowywane w szafach zamykanych na klucz. Szafy otwierane są wtedy, gdy ktoś chce mieć dostęp do dokumentów i zamykane po zakończeniu korzystania z dokumentów (najpóźniej na koniec każdego dnia pracy). Wszystkie klucze do szaf są przechowywane w skrzynce na klucze, również zamykanej na klucz. Klucz do skrzynki mają pracownicy/pracownice Sieci obywatelskiej upoważnieni przez Zarząd oraz członkowie Zarządu. Jeżeli szafę chce otworzyć osoba nieposiadająca klucza (np. wolontariusz), to pracownik otwiera szafę i odpowiada za zamknięcie jej.

Spis osób posiadających klucz do skrzynki aktalizowany jest kolejnymi uchwałami Zarządu dostępnymi na panelu wewnętrznym Stowarzyszenia.

Załącznik 4

Uchwała Zarządu

stowarzyszenia **Sieć Obywatelska Watchdog Polska**

nr …… z dnia ……..

w sprawie **upoważnienia wybranych osób do posiadania kluczy do szaf zamykanych**

Zarząd Stowarzyszenia Sieć Obywatelska Watchdog Polska działając w oparciu o § 24 ust. 1 Statutu oraz o § 5 ust. 2 Regulaminu Ochrony Danych Osobowych, ustala co następuje:

§ 1

Zezwala się następującym osobom:
…….
…….
na posiadanie klucza do szaf metalowych.

§ 2

Osoby te muszą podpisać „Procedurę zamykania szaf z dokumentami zawierającymi dane osobowe“ zawartą w Regulaminie Ochrony Danych Osobowych i przekazać do Administratora Bezpieczeństwa Informacji.

§ 3

Uchwała wchodzi w życie z dniem podjęcia.

Głosowanie:

za	osoby ….
przeciw	osób ……
wstrzymało się	osób ….

Uchwała została przyjęta stosunkiem …./…. oddanych głosów.

Załącznik 5

Warszawa, ...

Niniejszym zlecam .....(jaka czynność) .....(komu)

Administrator Bezpieczeństwa Informacji

Załącznik 6

Zbiory danych

Nr	Zbiór danych	Zakres danych	Forma przechowywania	Powiązania
1	Dane kadrowe oraz płacowe	• imię i nazwisko • adres stacjonarny • płeć • wykształcenie • imiona rodziców • PESEL • Data urodzenia • Miejsce urodzenia • numer dowodu • numer konta bankowego • przebieg kariery zawodowej	papierowa, dane przechowywane przez księgowość Stowarzyszenia na podstawie umowy powierzenia	Brak
2	Dane o współpracownikach/cach na umowy cywilno-prawne	• imię i nazwisko • adres stacjonarny • płeć • imiona rodziców • PESEL • data urodzenia • miejsce urodzenia; • numer konta bankowego	papierowa, dane przechowywane przez księgowość Stowarzyszenia na podstawie umowy powierzenia	Brak
3	Dane członkiń i członków	• imię i nazwisko; • adres stacjonarny; • adres e-mail; • telefon; • płeć.	papierowa w segregatorze Zarządu elektroniczna – na panelu członkowskim* w CMSie**	Z bazą darczyńców; odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób szkolonych; osób rekrutowanych;

				osób korzystających z list dyskusyjnych
4	Dane członkiń i członków wspierających	• imię i nazwisko • adres stacjonarny • adres e-mail telefon • płeć	papierowa w segregatorze Zarządu; elektroniczna – na panelu członkowskim; w CMSie.	Z bazą darczyńców; odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób szkolonych; osób rekrutowanych; osób korzystających z list dyskusyjnych
5	Dane wolontariuszy/ek	• imię i nazwisko • adres stacjonarny • adres e-mail telefon • numer dokumentu tożsamości • płeć	papierowa w segregatorze wolontariuszy; elektroniczna – na panelu członkowskim; w CMSie.	Z bazą darczyńców; odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób szkolonych; osób rekrutowanych; osób korzystających z list dyskusyjnych
6	Dane osób rekrutowanych na szkolenia	• imię i nazwisko • afiliacja organizacyjna • adres e-mail • telefon • płeć	Elektroniczna – formularze zgłoszeniowe LimeSurvey**** w chmurze**** i w CMS	Z bazą darczyńców; odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób szkolonych; osób korzystających z list dyskusyjnych
7	Dane osób szkolonych	• imię i nazwisko • afiliacja organizacyjna • adres e-mail • telefon • płeć	Elektroniczna – w CMS	Z bazą darczyńców; odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji

				prawnych; osób rekrutowanych; osób korzystających z list dyskusyjnych
8	Dane odbiorców newslettera	• adres e-mail	Elektroniczna – w CMSach stron internetowych	Z bazą darczyńców; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób rekrutowanych szkolonych; osób korzystających z list dyskusyjnych
9	Osoby korzystające z list dyskusyjnych	• imię i nazwisko • adres e-mail • płeć	Elektroniczna – w CMS	Z bazą darczyńców; bazą odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób rekrutowanych szkolonych.
10	Dane darczyńców	• imię i nazwisko • adres e-mail • data urodzenia • telefon • płeć • numer konta bankowego	Elektroniczna – w CMS, Zgoda na przetwarzanie danych w papierze.	Z bazą odbiorców newslettera; osób zachęcanych do działania; osób korzystających z konsultacji prawnych; osób rekrutowanych i szkolonych; osób korzystających z list dyskusyjnych
11	Dane osób zachęcanych do działania	• imię i nazwisko • adres e-mail • płeć • miejscowość	Elektroniczna – w CMS	Z bazą darczyńców; bazą odbiorców newslettera; osób korzystających z konsultacji prawnych; osób rekrutowanych szkolonych; osób korzystających z list dyskusyjnych

*Panel członkowski – autorskie oprogramowanie zawierające dane, które mogły być publicznie dostępne
**CRM
*** Elektroniczne formularze zgłoszeniowe
**** Chmura