

Dokumentacja ochrony danych osobowych RODO  
Stowarzyszenie Przyjaciół „BATKO”

Stowarzyszenie Przyjaciół "Batko"  
41-500 Chorzów, ul. Powstańców 6a  
NIP: 6272755170 REGON: 369350553  
tel. (32) 2410 129

*Zakrzewski*  
*- prezydent*  
*Stowarzyszenia*  
*J. Zakrzewski*

## **1. Wprowadzenie**

Celem niniejszego dokumentu jest opisanie zasad ochrony danych osobowych oraz dostarczenie podstawowej wiedzy z zakresu ich przetwarzania. W dokumencie opisano podstawy prawne przetwarzania danych osobowych oraz prawa i wolności osób, których dane dotyczą.

## **2. Podstawy prawne**

### **Definicje:**

**RODO** – ROZPORZADZENIE PARLAMENTU EUROPEJSKIEGO I RADY UE w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych.

**Dane osobowe** – oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie.

**Przetwarzanie** – oznacza operację lub zestaw operacji wykonywanych na danych osobowych, takie jak: zbieranie, utrwalanie, porządkowanie, organizowanie, przechowywanie, adoptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie.

**Zbiór danych (art. 6 RODO)** – oznacza uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów.

**Administrator** – oznacza jednostkę lub inny podmiot, który ustala cele i sposoby przetwarzania danych osobowych.

**Zgoda osoby, której dane dotyczą** – oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą przyzwala na przetwarzanie dotyczących jej danych osobowych.

**Naruszenie ochrony danych osobowych** – oznacza 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

### **3. Prawa i wolności osób, których dane dotyczą.**

**Prawo do zwięzłej, przejrzystej i zrozumiałej informacji ze strony administratora** – osoba, której dane dotyczą ma prawo uzyskiwać od administratora wszelkie informacje dotyczące obowiązku informacyjnego oraz do komunikacji z administratorem w związku z realizacją swoich praw.

**Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą** – administrator jest zobowiązany podać osobie, od której zbiera dane następujące informacje:

- swoją tożsamość i dane kontaktowe;
- cel przetwarzania danych osobowych;
- okres przechowywania danych;
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawie do sprzeciwu wobec przetwarzania i ograniczenia przetwarzania;
- informacje o prawie do cofnięcia zgody;
- informacje o prawie do wniesienia skargi do organu nadzorczego

**Prawo dostępu przysługujące osobie, której dane dotyczą** – osoba, której dane dotyczą może na żądanie uzyskać od administratora potwierdzenie, że przetwarzane są jej dane osobowe, a wówczas do dostępu do nich.

**Prawo do sprostowania danych** – osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania swoich danych lub uzupełnienia niekompletnych danych.

**Prawo do usunięcia danych** – osoba, której dane dotyczą może zażądać od administratora usunięcia swoich danych osobowych. Administrator musi niezwłocznie wykonać to żądanie.

**Prawo do wniesienia skargi do organu nadzorczego** – każda osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego, [...] jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza rozporządzenie RODO.

**Prawo do skutecznego środka ochrony przed sądem przeciwko organowi nadzorcemu lub administratorowi** – każda osoba fizyczna lub prawna ma prawo do skutecznego środka

### **3. Prawa i wolności osób, których dane dotyczą.**

**Prawo do zwięzłej, przejrzystej i zrozumiałej informacji ze strony administratora** – osoba, której dane dotyczą ma prawo uzyskiwać od administratora wszelkie informacje dotyczące obowiązku informacyjnego oraz do komunikacji z administratorem w związku z realizacją swoich praw.

**Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą** – administrator jest zobowiązany podać osobie, od której zbiera dane następujące informacje:

- swoją tożsamość i dane kontaktowe;
- cel przetwarzania danych osobowych;
- okres przechowywania danych;
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawie do sprzeciwu wobec przetwarzania i ograniczenia przetwarzania;
- informacje o prawie do cofnięcia zgody;
- informacje o prawie do wniesienia skargi do organu nadzorczego

**Prawo dostępu przysługujące osobie, której dane dotyczą** – osoba, której dane dotyczą może na żądanie uzyskać od administratora potwierdzenie, że przetwarzane są jej dane osobowe, a wówczas do dostępu do nich.

**Prawo do sprostowania danych** – osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania swoich danych lub uzupełnienia niekompletnych danych.

**Prawo do usunięcia danych** – osoba, której dane dotyczą może zażądać od administratora usunięcia swoich danych osobowych. Administrator musi niezwłocznie wykonać to żądanie.

**Prawo do wniesienia skargi do organu nadzorczego** – każda osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego, [...] jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza rozporządzenie RODO.

**Prawo do skutecznego środka ochrony przed sądem przeciwko organowi nadzorcemu lub administratorowi** – każda osoba fizyczna lub prawna ma prawo do skutecznego środka

ochrony prawnej przed sadem przeciwko prawnie wiążącej decyzji organu nadzorczego lub przeciwko administratorowi, jeżeli uzna, że prawa jej przysługujące zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem rozporządzenia RODO.

**Prawo do odszkodowania** – każda osoba, która poniosła szkodę w wyniku naruszenia rozporządzenia RODO ma prawo uzyskać od administratora odszkodowanie za poniesioną szkodę.

#### **4. Podstawowe obowiązki administratora danych osobowych.**

##### **Wdrażanie odpowiednich środków technicznych.**

Na administratorze spoczywa obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO.

##### **Zestawienie środków technicznych i organizacyjnych:**

1. Przetwarzanie odbywa się wyłącznie w ramach działań statutowych Stowarzyszenia.
2. Do przetwarzania danych upoważniony administrator danych osobowych oraz członkowie założyciele Stowarzyszenia
3. Obszar przetwarzania zabezpiecza się przed dostępem osób nieuprawnionych.
4. Dane osobowe w formie papierowej przechowywane są w zamkniętej na klucz szafie, uniemożliwiającej dostęp do niej osobom nieupoważnionym.
5. Dane osobowe w postaci elektronicznego rejestru członków Stowarzyszenia w formie pliku \*.xls (lub \*.xlsx) przechowywane są na zewnętrznym nośniku.

#### **5. Proces przetwarzania danych osobowych:**

1. Zakres danych osobowych gromadzonych i przetwarzanych przez Stowarzyszenie:
  - imię i nazwisko;
  - miejsce urodzenia;
  - adres zamieszkania;
  - numer telefonu;
  - adres e-mail.
2. Cel gromadzenia i przetwarzania danych osobowych:
  - rekrutacja nowych członków;
  - działalność statutowa Stowarzyszenia.
3. Jedyne źródłem danych osobowych są kandydaci na członków Stowarzyszenia.
4. Stowarzyszenie nie gromadzi, nie przechowuje i nie przetwarza danych osobowych wrażliwych.

### **3. Prawa i wolności osób, których dane dotyczą.**

**Prawo do zwięzłej, przejrzystej i zrozumiałej informacji ze strony administratora** – osoba, której dane dotyczą ma prawo uzyskiwać od administratora wszelkie informacje dotyczące obowiązku informacyjnego oraz do komunikacji z administratorem w związku z realizacją swoich praw.

**Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą** – administrator jest zobowiązany podać osobie, od której zbiera dane następujące informacje:

- swoją tożsamość i dane kontaktowe;
- cel przetwarzania danych osobowych;
- okres przechowywania danych;
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawie do sprzeciwu wobec przetwarzania i ograniczenia przetwarzania;
- informacje o prawie do cofnięcia zgody;
- informacje o prawie do wniesienia skargi do organu nadzorczego

**Prawo dostępu przysługujące osobie, której dane dotyczą** – osoba, której dane dotyczą może na żądanie uzyskać od administratora potwierdzenie, że przetwarzane są jej dane osobowe, a wówczas do dostępu do nich.

**Prawo do sprostowania danych** – osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania swoich danych lub uzupełnienia niekompletnych danych.

**Prawo do usunięcia danych** – osoba, której dane dotyczą może zażądać od administratora usunięcia swoich danych osobowych. Administrator musi niezwłocznie wykonać to żądanie.

**Prawo do wniesienia skargi do organu nadzorczego** – każda osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego, [...] jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza rozporządzenie RODO.

**Prawo do skutecznego środka ochrony przed sądem przeciwko organowi nadzorcemu lub administratorowi** – każda osoba fizyczna lub prawna ma prawo do skutecznego środka

ochrony prawnej przed sadem przeciwko prawnie wiążącej decyzji organu nadzorczego lub przeciwko administratorowi, jeżeli uzna, że prawa jej przysługujące zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem rozporządzenia RODO.

**Prawo do odszkodowania** – każda osoba, która poniosła szkodę w wyniku naruszenia rozporządzenia RODO ma prawo uzyskać od administratora odszkodowanie za poniesioną szkodę.

#### **4. Podstawowe obowiązki administratora danych osobowych.**

##### **Wdrażanie odpowiednich środków technicznych.**

Na administratorze spoczywa obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO.

##### **Zestawienie środków technicznych i organizacyjnych:**

1. Przetwarzanie odbywa się wyłącznie w ramach działań statutowych Stowarzyszenia.
2. Do przetwarzania danych upoważniony administrator danych osobowych oraz członkowie założyciele Stowarzyszenia
3. Obszar przetwarzania zabezpiecza się przed dostępem osób nieuprawnionych.
4. Dane osobowe w formie papierowej przechowywane są w zamkniętej na klucz szafie, uniemożliwiającej dostęp do niej osobom nieupoważnionym.
5. Dane osobowe w postaci elektronicznego rejestru członków Stowarzyszenia w formie pliku \*.xls (lub \*.xlsx) przechowywane są na zewnętrznym nośniku.

#### **5. Proces przetwarzania danych osobowych:**

1. Zakres danych osobowych gromadzonych i przetwarzanych przez Stowarzyszenie:
  - imię i nazwisko;
  - miejsce urodzenia;
  - adres zamieszkania;
  - numer telefonu;
  - adres e-mail.
2. Cel gromadzenia i przetwarzania danych osobowych:
  - rekrutacja nowych członków;
  - działalność statutowa Stowarzyszenia.
3. Jedyne źródłem danych osobowych są kandydaci na członków Stowarzyszenia.
4. Stowarzyszenie nie gromadzi, nie przechowuje i nie przetwarza danych osobowych wrażliwych.

## Analiza ryzyka

Lp.	Nazwa czynności	Cel przetwarzania	Kategorie osób
1	Zarządzanie dokumentami księgowymi.	Wystawianie rachunków i odbieranie faktur.	Wystawcy faktur lub odbiorcy rachunków.
2	Obsługa kontrahentów.	Współpraca z kontrahentami.	Kontrahenci.
3	Prowadzenie korespondencji.	Realizacja obowiązków prawnych.	Osoby korespondujące.
4	Obsługa umów.	Realizacja obowiązków prawnych.	Osoby, z którymi zawarto umowy.
5	Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.	Realizacja ustawowego obowiązku.	Osoby upoważnione do przetwarzania danych osobowych.
6	Prowadzenie strony internetowej.	Publikacja informacji o instytucji.	Osoby, których dane publikowane są na stronie internetowej.
7	Rekrutacja członków.	Przeprowadzenie naboru członków stowarzyszenia.	Osoby kandydujące.
<b>Mechanizmy kontrolne</b>			
Źródła i jakość danych		Dane pozyskiwane bezpośrednio od osób, których dotyczą; Dane są prawidłowe.	
<b>Aktywa</b>			
Lp.	Nazwa	Rodzaj	Ryzyko
1	Faktury	Dokumentacja papierowa.	Niskie
2	Rejestr przychodów i wydatków	Oprogramowanie	Niskie
3	Poczta elektroniczna	Oprogramowanie	Średnie
4	Nośniki mobilne	Sprzęt	Średnie
<b>Zabezpieczenia</b>			
1	Drzwi zamykane na klucz.	Siedziba	Niskie
2	Program antywirusowy.	Oprogramowanie	Niskie
3	Wykonywanie kopii bezpieczeństwa.	Oprogramowanie	Niske
4	Szafa niemetalowa zamykana na klucz.	Siedziba	Niskie
5	Właściwe utrzymanie i postępowanie ze sprzętem.	Sprzęt	Średnie
6	Polityka czystego biurka.	Organizacja	Wysokie

### **3. Prawa i wolności osób, których dane dotyczą.**

**Prawo do zwięzłej, przejrzystej i zrozumiałej informacji ze strony administratora** – osoba, której dane dotyczą ma prawo uzyskiwać od administratora wszelkie informacje dotyczące obowiązku informacyjnego oraz do komunikacji z administratorem w związku z realizacją swoich praw.

**Prawo do bycia poinformowanym w przypadku zbierania danych od osoby, której dane dotyczą** – administrator jest zobowiązany podać osobie, od której zbiera dane następujące informacje:

- swoją tożsamość i dane kontaktowe;
- cel przetwarzania danych osobowych;
- okres przechowywania danych;
- informacje o prawach do: dostępu do danych osobowych osoby, której dane dotyczą, ich sprostowania, usunięcia i przenoszenia oraz o prawie do sprzeciwu wobec przetwarzania i ograniczenia przetwarzania;
- informacje o prawie do cofnięcia zgody;
- informacje o prawie do wniesienia skargi do organu nadzorczego

**Prawo dostępu przysługujące osobie, której dane dotyczą** – osoba, której dane dotyczą może na żądanie uzyskać od administratora potwierdzenie, że przetwarzane są jej dane osobowe, a wówczas do dostępu do nich.

**Prawo do sprostowania danych** – osoba, której dane dotyczą może żądać od administratora niezwłocznego sprostowania swoich danych lub uzupełnienia niekompletnych danych.

**Prawo do usunięcia danych** – osoba, której dane dotyczą może zażądać od administratora usunięcia swoich danych osobowych. Administrator musi niezwłocznie wykonać to żądanie.

**Prawo do wniesienia skargi do organu nadzorczego** – każda osoba, której dane dotyczą ma prawo wnieść skargę do organu nadzorczego, [...] jeżeli sądzi, że przetwarzanie danych osobowych jej dotyczących narusza rozporządzenie RODO.

**Prawo do skutecznego środka ochrony przed sądem przeciwko organowi nadzorcemu lub administratorowi** – każda osoba fizyczna lub prawna ma prawo do skutecznego środka

ochrony prawnej przed sadem przeciwko prawnie wiążącej decyzji organu nadzorczego lub przeciwko administratorowi, jeżeli uzna, że prawa jej przysługujące zostały naruszone w wyniku przetwarzania jej danych osobowych z naruszeniem rozporządzenia RODO.

**Prawo do odszkodowania** – każda osoba, która poniosła szkodę w wyniku naruszenia rozporządzenia RODO ma prawo uzyskać od administratora odszkodowanie za poniesioną szkodę.

#### **4. Podstawowe obowiązki administratora danych osobowych.**

##### **Wdrażanie odpowiednich środków technicznych.**

Na administratorze spoczywa obowiązek wdrażania odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO.

##### **Zestawienie środków technicznych i organizacyjnych:**

1. Przetwarzanie odbywa się wyłącznie w ramach działań statutowych Stowarzyszenia.
2. Do przetwarzania danych upoważniony administrator danych osobowych oraz członkowie założyciele Stowarzyszenia
3. Obszar przetwarzania zabezpiecza się przed dostępem osób nieuprawnionych.
4. Dane osobowe w formie papierowej przechowywane są w zamkniętej na klucz szafie, uniemożliwiającej dostęp do niej osobom nieupoważnionym.
5. Dane osobowe w postaci elektronicznego rejestru członków Stowarzyszenia w formie pliku \*.xls (lub \*.xlsx) przechowywane są na zewnętrznym nośniku.

#### **5. Proces przetwarzania danych osobowych:**

1. Zakres danych osobowych gromadzonych i przetwarzanych przez Stowarzyszenie:
  - imię i nazwisko;
  - miejsce urodzenia;
  - adres zamieszkania;
  - numer telefonu;
  - adres e-mail.
2. Cel gromadzenia i przetwarzania danych osobowych:
  - rekrutacja nowych członków;
  - działalność statutowa Stowarzyszenia.
3. Jedyne źródłem danych osobowych są kandydaci na członków Stowarzyszenia.
4. Stowarzyszenie nie gromadzi, nie przechowuje i nie przetwarza danych osobowych wrażliwych.

## Analiza ryzyka

Lp.	Nazwa czynności	Cel przetwarzania	Kategorie osób
1	Zarządzanie dokumentami księgowymi.	Wystawianie rachunków i odbieranie faktur.	Wystawcy faktur lub odbiorcy rachunków.
2	Obsługa kontrahentów.	Współpraca z kontrahentami.	Kontrahenci.
3	Prowadzenie korespondencji.	Realizacja obowiązków prawnych.	Osoby korespondujące.
4	Obsługa umów.	Realizacja obowiązków prawnych.	Osoby, z którymi zawarto umowy.
5	Prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.	Realizacja ustawowego obowiązku.	Osoby upoważnione do przetwarzania danych osobowych.
6	Prowadzenie strony internetowej.	Publikacja informacji o instytucji.	Osoby, których dane publikowane są na stronie internetowej.
7	Rekrutacja członków.	Przeprowadzenie naboru członków stowarzyszenia.	Osoby kandydujące.
<b>Mechanizmy kontrolne</b>			
Źródła i jakość danych		Dane pozyskiwane bezpośrednio od osób, których dotyczą; Dane są prawidłowe.	
<b>Aktywa</b>			
Lp.	Nazwa	Rodzaj	Ryzyko
1	Faktury	Dokumentacja papierowa.	Niskie
2	Rejestr przychodów i wydatków	Oprogramowanie	Niskie
3	Poczta elektroniczna	Oprogramowanie	Średnie
4	Nośniki mobilne	Sprzęt	Średnie
<b>Zabezpieczenia</b>			
1	Drzwi zamykane na klucz.	Siedziba	Niskie
2	Program antywirusowy.	Oprogramowanie	Niskie
3	Wykonywanie kopii bezpieczeństwa.	Oprogramowanie	Niske
4	Szafa niemetalowa zamykana na klucz.	Siedziba	Niskie
5	Właściwe utrzymanie i postępowanie ze sprzętem.	Sprzęt	Średnie
6	Polityka czystego biurka.	Organizacja	Wysokie

Scenariusze zdarzeń				
Lp.	Zdarzenie	Przyczyna	Skutek	Ryzyko
1	Awaria urządzenia.	Brak właściwego utrzymania i postępowania ze sprzętem. Brak kopii zapasowych	Strata finansowa, utrata danych.	Średnie
2	Pożar lub inna forma zniszczenia.	Brak fizycznej ochrony p-poż. Nieobecność personelu. Brak świadomości w zakresie bezpieczeństwa.	Strata finansowa. Utrata danych.	Niskie
3	Ujawnienie, utrata lub kradzież danych.	Brak fizycznej ochrony budynku. Brak kopii zapasowych. Niewystarczająca polityka czystego biurka.	Strata finansowa. Utrata danych.	Średnie