Procedura przetwarzania danych osobowych (RODO) w Stowarzyszenia Czas Przestrzeń Tożsamość

Administrator danych: Stowarzyszenia Czas Przestrzeń Tożsamość

email: sekretariat@cpt.org.pl www.cpt.org.pl

1. Cel i zakres

Procedura określa zasady przetwarzania i ochrony danych osobowych przez [nazwa organizacji]. Dotyczy pracowników, współpracowników, wolontariuszy oraz innych osób, które przetwarzają dane w imieniu organizacji.

Obejmuje dane m.in. członków, darczyńców, uczestników działań, beneficjentów, wolontariuszy, pracowników i kontrahentów.

2. Zasady przetwarzania

Organizacja przetwarza dane:

- zgodnie z prawem, rzetelnie i w sposób przejrzysty;
- wyłącznie w konkretnych, określonych celach;
- w zakresie niezbędnym do realizacji tych celów;
- przez okres nie dłuższy, niż jest to potrzebne lub wymagane przepisami;
- z zastosowaniem zabezpieczeń chroniących przed utratą, nieuprawnionym dostępem lub ujawnieniem.

Danych nie wykorzystuje się do innych celów bez ustalenia właściwej podstawy prawnej i, gdy jest to wymagane, poinformowania osoby.

3. Podstawy i cele przetwarzania

Przed rozpoczęciem przetwarzania organizacja ustala jego cel i podstawę prawną. Zależnie od sytuacji może to być m.in.:

- - zgoda osoby;
- - wykonanie umowy lub podjęcie działań przed jej zawarciem;
- - obowiązek prawny organizacji;
- - prawnie uzasadniony interes organizacji lub innej strony, po uprzednim rozważeniu praw i wolności osoby.

Podstawa prawna oraz cel są odnotowywane w ewidencji czynności przetwarzania lub innej dokumentacji organizacji.

4. Obowiązek informacyjny

Przy zbieraniu danych organizacja przekazuje osobie informacje wymagane przez RODO, w szczególności:

- - kto jest administratorem i jak się z nim skontaktować;
- - w jakim celu i na jakiej podstawie dane są przetwarzane;
- - komu dane mogą być ujawniane;
- - jak długo dane będą przechowywane;
- - jakie prawa przysługują osobie i jak z nich skorzystać;
- - czy podanie danych jest wymagane oraz jakie są skutki ich niepodania.

Informację przekazuje się w zrozumiałej formie, np. w formularzu, umowie, wiadomości e-mail lub na stronie internetowej.

5. Dostęp i poufność

1. Dostęp do danych otrzymują wyłącznie osoby, którym jest on potrzebny do wykonywania zadań.
2. Każda osoba upoważniona do przetwarzania danych zobowiązuje się do zachowania poufności.
3. Organizacja prowadzi wykaz osób upoważnionych i odbiera dostęp, gdy przestaje być potrzebny.
4. Dane nie mogą być przekazywane osobom nieuprawnionym ani omawiane w miejscach, gdzie mogą zostać usłyszane przez osoby postronne.

6. Zabezpieczenia

Organizacja stosuje zabezpieczenia odpowiednie do rodzaju danych i ryzyka, w szczególności:

- - silne, indywidualne hasła i — gdy dostępne — uwierzytelnianie wieloskładnikowe;
- - blokowanie urządzeń i ekranów podczas odejścia od stanowiska;
- - aktualizacje oprogramowania i ochronę urządzeń;
- - przechowywanie dokumentów papierowych w zamykanych szafach;
- - ograniczenie dostępu do poczty, dysków i systemów do osób upoważnionych;
- - bezpieczne niszczenie niepotrzebnych dokumentów i nośników.

Dane służbowe przechowuje się w zatwierdzonych przez organizację lokalizacjach, a nie na prywatnych kontach lub urządzeniach, chyba że organizacja wyraźnie na to zezwoli i określi zabezpieczenia.

7. Udostępnianie danych

1. Dane przekazuje się odbiorcom tylko wtedy, gdy jest to niezbędne i istnieje ku temu podstawa prawna.
2. Przed skorzystaniem z usługodawcy, który będzie przetwarzał dane w imieniu organizacji, sprawdza się jego wiarygodność i zawiera umowę powierzenia, jeśli jest wymagana.
3. Dane nie są przekazywane poza Europejski Obszar Gospodarczy bez uprzedniego sprawdzenia wymogów prawnych dotyczących takiego transferu.

8. Przechowywanie i usuwanie danych

1. Organizacja określa okresy przechowywania danych dla poszczególnych celów, uwzględniając przepisy, umowy i potrzeby dokumentacyjne.
2. Po upływie właściwego okresu dane usuwa się, niszczy lub anonimizuje, chyba że dalsze przechowywanie jest wymagane prawem albo ma inną podstawę.
3. Usuwanie obejmuje również kopie i miejsca przechowywania, nad którymi organizacja sprawuje kontrolę, z uwzględnieniem zasad tworzenia i nadpisywania kopii zapasowych.

9. Prawa osób

Osoba może złożyć wniosek dotyczący swoich danych, w tym o dostęp, sprostowanie, usunięcie, ograniczenie przetwarzania, przenoszenie danych lub sprzeciw — jeśli dane prawo ma zastosowanie w danej sytuacji. Może także wycofać zgodę, gdy przetwarzanie odbywa się na jej podstawie.

Wnioski należy kierować na adres: [e-mail lub adres korespondencyjny]. Organizacja weryfikuje tożsamość wnioskodawcy w zakresie niezbędnym do bezpiecznego rozpatrzenia wniosku i odpowiada w terminach przewidzianych przepisami.

10. Naruszenia ochrony danych

Każda osoba, która zauważy utratę danych, wysłanie ich niewłaściwemu odbiorcy, nieuprawniony dostęp lub inne możliwe naruszenie, niezwłocznie zgłasza je do [osoba/funkcja i dane kontaktowe].

Osoba odpowiedzialna:

- zabezpiecza dostępne informacje i ogranicza skutki zdarzenia;
- ustala, jakie dane i osoby mogą być objęte zdarzeniem;
- dokumentuje naruszenie oraz podjęte działania;
- ocenia ryzyko dla praw i wolności osób;
- w razie potrzeby dokonuje zgłoszenia do Prezesa Urzędu Ochrony Danych Osobowych w wymaganym terminie oraz informuje osoby, których dane dotyczą, gdy wymagają tego przepisy.

11. Szkolenia i odpowiedzialność

Osoby mające dostęp do danych zapoznają się z procedurą przed rozpoczęciem pracy z danymi. Organizacja przypomina zasady ochrony danych oraz aktualizuje procedurę, gdy zmieniają się procesy, systemy lub przepisy.

Za wdrożenie i aktualizację procedury odpowiada [funkcja/osoba]. Każdy pracownik, współpracownik i wolontariusz jest zobowiązany przestrzegać zasad oraz zgłaszać zauważone problemy.

12. Postanowienia końcowe

Procedura obowiązuje od [data]. Jest udostępniana osobom, których dotyczy. Organizacja prowadzi dokumentację potrzebną do wykazania zgodności z RODO, w tym — stosownie do skali i rodzaju działalności — ewidencję czynności przetwarzania, upoważnienia, umowy powierzenia i rejestr naruszeń.

1. Dokument należy dostosować do rzeczywistych działań organizacji, rodzajów przetwarzanych danych i stosowanych systemów.