Polityka przetwarzania Danych Osobowych
w fundacji OpenStax Poland

Spis treści

I. Definicje

Administrator – podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania Danych Osobowych, w tym Fundacja.

Dane Osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej w rozumieniu art. 4 pkt 1 RODO.

Odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się Dane Osobowe. Odbiorcą jest również Przetwarzający.

Organ Nadzorczy – niezależny organ publiczny, o którym mowa w art. 51 RODO, odpowiedzialny za monitorowanie stosowania RODO, w tym Prezes Urzędu Ochrony Danych Osobowych.

Naruszenie 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.

Podmiot Danych – osoba fizyczna, której Dane Osobowe dotyczą, osoby odwiedzające Fundację w jej siedzibie lub w miejscach, gdzie Fundacja realizuje swoje cele statutowe, osoby kontaktujące się z Administratorem, użytkownicy mediów społecznościowych, uczestnicy konkursów, pracownicy, wykonawcy, zleceniobiorcy, jak również przedsiębiorcy prowadzący jednoosobową działalność gospodarczą, których Dane Osobowe są przetwarzane.

Przepisy z zakresu ochrony Danych Osobowych – obowiązujące regulacje z zakresu ochrony danych osobowych, w tym RODO.

Przetwarzanie – operacja lub zestaw operacji wykonywanych na Danych Osobowych lub zestawach Danych Osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;

Przetwarzający – podmiot, który przetwarza Dane Osobowe w imieniu Administratora.

RODO – oznacza ogólne Rozporządzenie Parlamentu Europejskiego i Rady (UE) o ochronie danych osobowych nr 2016/679.

Fundacja – **Fundacja OpenStax Poland**, 00-132 Warszawa, ul. Grzybowska 5A, wpisana do rejestru przedsiębiorców prowadzonego przez Sąd Rejonowy dla m.st. Warszawy, XII Wydział Gospodarczy Krajowego Rejestru Sądowego do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji i publicznych zakładów opieki zdrowotnej pod numerem KRS 0000738271;

Wrażliwe Dane Osobowe / Dane wrażliwe – Dane Osobowe, które ujawniają pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, a także dane genetyczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia, seksualności lub orientacji seksualnej.

II. Cel, zakres, zakres odpowiedzialności

1. Cel

Celem niniejszej procedury jest zapewnienie zgodności procesów przetwarzania Danych Osobowych przez Fundację z Przepisami z zakresu ochrony danych osobowych. Procedura ta jest dostępna dla wszystkich pracowników (współpracowników) oraz wolontariuszy Fundacji, a jej znajomość jest obowiązkowa dla wszystkich pracowników (współpracowników) oraz wolontariuszy zaangażowanych w przetwarzanie Danych Osobowych.

2. Zakres

Niniejsza procedura stanowi zbiór podstawowych reguł i zasad z zakresu ochrony Danych Osobowych, które muszą być przestrzegane w procesie przetwarzania Danych Osobowych (w tym m. in. w trakcie zbierania i korzystania z tych danych) w ramach codziennej działalności wykonywanej w imieniu i na rzecz Fundacji.

3. Zakres odpowiedzialności

Szczegółowy zakres odpowiedzialności określono w Rozdziale III niniejszej procedury.

III. Wprowadzenie i zakres

1. W ramach codziennej działalności prowadzonej przez Fundację możemy mieć styczność ze zbieraniem i korzystaniem z Danych Osobowych pracowników i innych osób fizycznych.
2. Dane Osobowe oznaczają wszystko, co może zidentyfikować konkretną osobę i mogą oznaczać w szczególności: imię i nazwisko, numer telefonu, adres e-mail, adres korespondencyjny, numer PESEL, ale również nagrania, zdjęcia, jakiekolwiek dane identyfikujące Podmiot Danych lub umożliwiające jego identyfikację.
3. Naruszenie przestrzegania Przepisów z zakresu ochrony danych osobowych może prowadzić do poniesienia przez Fundację surowej odpowiedzialności i braku możliwości dalszego przetwarzania Danych Osobowych. Brak poszanowania praw Podmiotów Danych do prywatności i ochrony ich Danych Osobowych, może w konsekwencji prowadzić również do wystąpienia poważnej szkody wizerunkowej i strat w działalności (operacyjnej) Fundacji.
4. Reguły i zasady zawarte w niniejszej procedurze muszą być znane i przestrzegane przez wszystkich pracowników, współpracowników, wolontariuszy i kontrahentów Fundacji, którzy są zaangażowani w przetwarzanie Danych Osobowych.
5. Niniejsza procedura odnosi się do przetwarzania Danych Osobowych przez Fundację niezależnie od roli, w jakiej występuje, tj. jako Administrator danych, współadministrator czy Przetwarzający.

IV. Role i obowiązki

1. Pracownicy (współpracownicy) i wolontariusze

1.1. Każdy pracownik (współpracownik) i wolontariusz Fundacji może mieć przy okazji różnych sytuacji kontakt z Danymi Osobowymi. Może to nastąpić, gdy korzysta z systemów Fundacji, w których przetwarzane są Dane Osobowe, tj. np. z narzędzi zarządzania kontaktami z kontrahentami. Kontakt z danymi może być również wynikiem fizycznego dostępu do arkuszy danych lub dokumentów zawierających Dane Osobowe pracowników lub wolontariuszy itp.

1.2. Dlatego, każdy pracownik (współpracownik) i wolontariusz musi znać podstawowe reguły i zasady ochrony Danych Osobowych oraz zasady opisane w niniejszej procedurze oraz w odpowiednich dodatkowych szczegółowych procedurach Fundacji dotyczących przetwarzania Danych Osobowych.

2. Osoby upoważnione

2.1. Każda osoba, która otrzymała upoważnienie do przetwarzania Danych Osobowych musi:

- przestrzegać Przepisów z zakresu ochrony danych osobowych, postanowień niniejszej procedury, procedur szczegółowych oraz zakresu udzielonego upoważnienia;
- zachować poufność wszelkich przetwarzanych Danych Osobowych oraz informacji o sposobach ich zabezpieczenia;
- uczestniczyć w szkoleniach w zakresie ochrony Danych Osobowych.

2.2. Użytkownicy systemów przetwarzających lub zawierających Dane Osobowe muszą przestrzegać wskazówek i instrukcji udzielanych przez Zarząd lub wskazane przez Zarząd osoby.

2.3. Każdy użytkownik systemów przetwarzających lub zawierających Dane Osobowe, uwzględniając charakter, zakres, kontekst i cele przetwarzania Danych Osobowych oraz ryzyko naruszenia praw lub wolności Podmiotów Danych, musi wdrażać i stosować wszystkie odpowiednie środki i procedury zapewniające zgodność z Przepisami z zakresu ochrony danych osobowych.

3. Zarząd

Do zadań Zarządu Fundacji należy:

- wdrożenie i monitorowanie w Fundacji przestrzegania standardów ochrony Danych Osobowych wynikających z Przepisów z zakresu ochrony Danych Osobowych;
- realizacja obowiązków wynikających z Przepisów z zakresu ochrony Danych Osobowych;
- zapewnienie przestrzegania w Fundacji zasad zawartych w niniejszej procedurze oraz w procedurach szczegółowych;
- przeprowadzanie audytów bezpieczeństwa przetwarzania Danych Osobowych w Fundacji;
- dbałość o kwalifikacje i szkolenia pracowników (współpracowników) i wolontariuszy z zakresu ochrony Danych Osobowych;
- współpraca z Organem Nadzorczym.

V. Zasady ochrony Danych Osobowych

Przetwarzając Dane Osobowe, należy przestrzegać poniższych zasad:

a) **Rzetelność**: możemy zbierać Dane Osobowe jedynie w taki sposób, aby nie miało to żadnych negatywnych konsekwencji dla Podmiotów Danych, w tym nie możemy stosować żadnych nieuczciwych praktyk w celu zdobycia informacji.

b) **Zgodność z prawem**: przetwarzanie, w tym zbieranie Danych Osobowych musi mieć uzasadnioną podstawę prawną, przewidzianą w Przepisach z zakresu ochrony danych osobowych.

c) **Przejrzystość**: musimy mieć pewność, że podmioty danych zdają sobie sprawę z faktu przetwarzania ich Danych Osobowych oraz wiedzą, dla jakich celów i w jaki sposób przetwarzamy ich Dane Osobowe. Stosujemy przejrzyste i łatwo dostępne klauzule informacyjne informujące o zasadach przetwarzania Danych Osobowych oraz o tym w jaki sposób podmioty danych mogą korzystać ze swoich praw. Kontaktujemy się z Podmiotami Danych w prosty i zrozumiały sposób, używając jasnego i prostego języka.

d) **Minimalizacja danych (adekwatność)**: ograniczamy zbieranie i korzystanie z Danych Osobowych do tych danych, które są bezpośrednio istotne i niezbędne do celów, dla których dane zostały zebrane.

e) **Ograniczenie celu**: przetwarzamy Dane Osobowe wyłącznie w określonych (szczegółowo) celach, wyraźnie przedstawionych Podmiotowi Danych oraz zgodnych z prawem (tj. w oparciu o stosowną podstawę prawną i w granicach uzasadnionych oczekiwaniami tej osoby); nie przetwarzamy Danych Osobowych w innych celach.

f) **Prawidłowość:** musimy dbać o to, żeby Dane Osobowe były dokładne i aktualne; nie powinniśmy przechowywać danych, które są niedokładne.

g) **Ograniczenie przechowywania**: nie możemy przechowywać Danych Osobowych dłużej, niż jest to konieczne dla osiągnięcia celu i zgodnie z okresem retencji, który został przez nas dla tego celu określony. W chwili, gdy Dane Osobowe nie są już potrzebne dla celów, dla których je zebrano, musimy je usunąć lub zanonimizować. Nie można przechowywać danych przez czas nieokreślony.

h) **Integralność i poufność**: musimy wdrażać odpowiednie środki techniczne i organizacyjne w celu zapewnienia odpowiedniego poziomu bezpieczeństwa Danych Osobowych. Środki muszą zapobiegać wszelkiemu nieuprawnionemu ujawnieniu lub nieuprawnionemu uzyskaniu dostępu, przypadkowemu lub niezgodnemu z prawem zniszczeniu lub przypadkowej utracie bądź zmianie oraz jakiejkolwiek innej nielegalnej formie działania wobec tych danych.

i) **Projektowanie ochrony Danych Osobowych**: uwzględniając szereg aspektów (stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania), myślimy o projektowaniu ochrony Danych Osobowych od samego początku, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania. Ochrona Danych Osobowych musi być wkomponowana w proces tworzenia nowego produktu, usługi, aplikacji, oferty, itd.

j) **Podejście oparte na ryzyku**: dbając o bezpieczeństwo, projektujemy ochronę danych uwzględniając prawdopodobieństwo i powagę ryzyka naruszenia praw lub wolności Podmiotu Danych.

k) **Rozliczalność**: Fundacja jest odpowiedzialne za przestrzeganie Przepisów z zakresu ochrony Danych Osobowych i musi być w stanie wykazać ich przestrzeganie w ramach prowadzonej działalności.

VI. Etapy przetwarzania Danych Osobowych

1. Planowanie/projektowanie procesu przetwarzania Danych Osobowych

W momencie rozpoczęcia nowego działania lub procesu, który obejmuje przetwarzanie Danych Osobowych, na samym początku musimy uwzględnić ochronę Danych Osobowych, w tym środki ochrony prywatności, już w założeniach takiej aktywności projektowej za pomocą planowania/projektowania związanego z nim przetwarzania Danych Osobowych w taki sposób, żeby przetwarzanie to było w szczególności ograniczone do tego, co jest ściśle niezbędne dla tej aktywności projektowej (zasada uwzględniania ochrony Danych Osobowych w fazie projektowania *„Privacy by Design"* oraz zasada domyślnej ochrony danych *„Privacy by Default"*).

2. Ocena skutków dla ochrony danych

2.1. W sytuacjach, gdzie prywatność Podmiotów Danych może być narażona na wysokie ryzyko, należy przeprowadzić szczegółową ocenę skutków dla ochrony danych, przed rozpoczęciem samego przetwarzania danych, w szczególności w przypadku przetwarzania danych wrażliwych na dużą skalę.

3. Przetwarzanie

3.1. Po rozpoczęciu przetwarzania Danych Osobowych, musimy zawsze przestrzegać niniejszej procedury i odpowiednich procedur szczegółowych Fundacji.

3.2. Czynności przetwarzania Danych Osobowych przez Fundację jako Administratora danych oraz kategorie czynności przetwarzania dokonywanych przez Fundację jako Przetwarzający należy rejestrować w Rejestrze czynności przetwarzania.

4. Zakończenie przetwarzania

4.1. Jeśli nie mamy aktualnego prawnego uzasadnienia dla kontynuowania przetwarzania Danych Osobowych, musimy je usunąć lub zanonimizować.

4.2. Schemat przechowywania i usunięcia Danych Osobowych jak również techniczne i organizacyjne środki to umożliwiające, muszą być ustalone i opisane w fazie planowania/projektowania działania lub procesu z uwzględnieniem zasad retencji Danych Osobowych obowiązujących w Fundacji.

VII. Podstawy prawne przetwarzania Danych Osobowych

Możemy przetwarzać Dane Osobowe, tylko jeśli mamy do tego ważne, określone prawem podstawy. Przed rozpoczęciem przetwarzania danych należy te podstawy legalizujące przetwarzanie zidentyfikować i wskazać.

W razie gdy przetwarzamy dane bez podstawy prawnej, takie przetwarzanie jest nielegalne, musi zostać natychmiast zakończone i wszystkie Dane Osobowe muszą zostać usunięte lub zanonimizowane.

Podstawy prawne umożliwiające zgodne z prawem przetwarzanie Danych Osobowych stanowią:

- zgoda podmiotu danych;
- wykonanie umowy zawartej z Podmiotem Danych lub podjęcia działań na żądanie Podmiotu Danych przed zawarciem umowy;
- prawnie uzasadniony interes realizowany przez Administratora danych;
- obowiązek prawny ciążący na Administratorze danych;
- sprawowanie władzy publicznej powierzonej Administratorowi danych (wykonanie zadania realizowanego w interesie publicznym);
- ochrona żywotnych interesów Podmiotu Danych / innej osoby fizycznej.

Trzy najważniejsze podstawy prawne zostały wyjaśnione poniżej.

1. Zgoda osoby

1.1. Jeśli wybieramy zgodę jako podstawę do przetwarzania danych Podmiotu Danych, zgoda ta zawsze musi spełniać poniższe wymogi, tj.:

- **dobrowolna** – nie należy zmuszać do udzielenia zgody, np. poprzez uzależnianie wykonania usługi od udzielenia zgody; jeśli przetwarzanie Danych Osobowych jest niezbędne do wykonania zleconej usługi, w takim wypadku podstawą do przetwarzania danych nie jest „zgoda", ale przesłanka „wykonania umowy";
- **konkretna** – zgoda musi być na tyle konkretna, żeby było jasne, jakie dane są przetwarzane i w jakich celach;
- **świadoma** – Podmioty Danych muszą być w pełni poinformowane o konsekwencjach udzielonej zgody w odniesieniu do swojej prywatności i powiązanych z nią praw, jakie dane podlegają zbieraniu, jak długo będą wykorzystywane, kto ma dostęp do tych danych, itd.;
- **jednoznaczna** – osoba udzielająca zgody musi mieć jasność, co do tego na co wyraża zgodę; wykorzystanie przez nas danych nie powinno przekraczać oczekiwań tej osoby, co do zakresu udzielonej zgody.

1.2. Jeśli zgoda jest udzielana w formie pisemnej deklaracji, która również obejmuje inne kwestie (tj. rejestrację na stronie internetowej, potwierdzenie regulaminu, podpisanie zamówienia na produkt lub usługę, akceptację ogólnych warunków umownych), należy zapewnić, że zgoda jest:

- jednoznacznie odróżniona od innych kwestii,
- łatwo dostępna w każdym czasie,
- wyrażona jasnym i prostym językiem.

1.3. W celu uzyskania zgody podmiotu danych na przetwarzanie jego Danych Osobowych, Fundacja stosuje wzór formularza zgody. Konkretny formularz zgody, musi być każdorazowo dostosowany do szczególnych celów, zakresu Danych Osobowych i zakresu przetwarzania.

1.4. Musimy również zapewnić, żeby Podmiot Danych mógł **wycofać swoją zgodę** w każdym czasie. Wycofanie zgody powinno być równie łatwe jak jej udzielenie. W momencie uzyskania zgody musimy poinformować o możliwości jej wycofania.

1.5. W związku z tym, że Podmiot Danych ma prawo wycofania swojej zgody, to zanim wybierzemy zgodę jako podstawę przetwarzania danych, musimy zawsze ostrożnie ocenić wykonalność i przydatność innych podstaw prawnych w odniesieniu do przetwarzania danych.

2. Wykonanie umowy

2.1. Jeśli przetwarzanie danych opiera się na umowie, musi to być umowa, której stroną jest dany Podmiot Danych. Wykonanie umowy może stanowić uzasadnioną podstawę prawną dla procesów przetwarzania Danych Osobowych w zakresie, w jakim stanowią one realizację celu zawartej umowy.

2.2. Podstawa ta uzasadnia również podjęcie działań na żądanie Podmiotu Danych przed zawarciem umowy.

3. Uzasadniony interes

Jeśli przetwarzanie danych opiera się na podstawie przesłanki prawnie uzasadnionego interesu Administratora danych, musimy:

3.1. jasno określić, co stanowi ten interes i dlaczego jest on prawnie uzasadniony; przy czym za prawnie uzasadniony interes Administratora uznaje się przetwarzanie danych do celów marketingu bezpośredniego;

3.2. wyważyć, czy nad naszym uzasadnionym interesem nie przeważa interes i prawa podstawowe Podmiotu Danych; przy czym taki prawnie uzasadniony interes może istnieć na przykład w przypadkach, gdy zachodzi istotny i odpowiedni rodzaj powiązania między Podmiotem Danych a Administratorem, na przykład gdy Podmiotem Danych jest osoba działająca na rzecz Administratora.

VIII. Prawa Podmiotów Danych

Celem Przepisów z zakresu ochrony danych osobowych jest zapewnienie ochrony prywatności Podmiotów Danych.

1. Informowanie Podmiotów Danych

1.1. Musimy zapewnić, że Podmiot Danych, którego Dane Osobowe Fundacja przetwarza, zostanie poinformowany w szczególności o:

- nazwie i danych kontaktowych Fundacji występującej w roli Administratora danych;
- poszczególnych celach, dla których dane będą przetwarzane;
- podstawach prawnych przetwarzania Danych Osobowych;
- odbiorcach danych (ich kategoriach), którym dane będą udostępniane (ze szczególnym uwzględnieniem zasad przekazywania danych do podmiotów spoza Unii Europejskiej);
- przewidzianym okresie przechowywania Danych Osobowych;
- niestosowaniu zautomatyzowanego podejmowania decyzji, w tym profilowania;
- prawie do dostępu do Danych Osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania, cofnięcia udzielonej zgody, wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia Danych Osobowych;
- prawie wniesienia skargi do Organu Nadzorczego.

1.2. Informacja dotycząca prywatności musi być uzupełniona o szczegółowe informacje dotyczące specyfiki przetwarzania danych, w odniesieniu do konkretnego procesu przetwarzania. Niezbędne jest poinformowanie podmiotu danych, czy podanie jego Danych Osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy Podmiot Danych jest zobowiązany do ich podania i jakie są ewentualne konsekwencje niepodania danych.

1.3. W celu przekazania Podmiotom Danych informacji dotyczących przetwarzania danych, Fundacja stosuje wzór klauzuli informacyjnej. Konkretna klauzula informacyjna musi być każdorazowo dostosowana do szczególnych celów, zakresu Danych Osobowych, zakresu przetwarzania i podstawy prawnej przetwarzania.

2. Żądania Podmiotów Danych

2.1. Podmioty Danych posiadają określone prawa związane z ochroną prywatności i w celu wykonania tych praw mogą się kontaktować z Fundacją. Prawa te obejmują:

- prawo dostępu do ich Danych Osobowych;
- prawo wniesienia sprzeciwu wobec przetwarzania Danych Osobowych w pewnych przypadkach (np. w odniesieniu do marketingu bezpośredniego);
- prawo do cofnięcia udzielonej zgody na przetwarzania Danych Osobowych;

- prawo do usunięcia Danych Osobowych (zwane również *„prawem do bycia zapomnianym”*), np. gdy Danych Osobowych nie są już potrzebne do celów, w których zostały zebrane, lub w razie wycofania zgody na ich przetwarzanie;
- prawo do ograniczenia przetwarzania Danych Osobowych;
- prawo do sprostowania Danych Osobowych, które są nieprawidłowe;
- prawo do przenoszenia Danych Osobowych (tylko w sytuacji, gdy przetwarzanie oparte jest na przesłance zgody lub wykonania umowy z daną osobą), tj. prawo do otrzymania swoich Danych Osobowych lub do przekazania ich innemu Administratorowi danych.

2.2. Każdy z nas musi przestrzegać powyższych praw związanych z ochroną prywatności, w każdym czasie. Każdy, z którego działaniami wiąże się przetwarzanie danych, odpowiada za faktyczne stosowanie odpowiednich środków ochrony oraz musi zapewnić, że rozwiązania umożliwiające wykonanie praw Podmiotów Danych są skutecznie wdrożone.

2.3. Szczegółowe zasady zapewnienia Podmiotom Danych realizacji ich praw określa procedura obsługi praw Podmiotów Danych. Określa ona również terminy odpowiedzi na żądania Podmiotów Danych.

IX. Powierzenie przetwarzania Danych Osobowych

Zawsze, kiedy przekazujemy Dane Osobowe jakimkolwiek osobom lub podmiotom trzecim, to przekazanie lub dostęp do Danych Osobowych lub wykorzystanie Danych Osobowych musi być zgodne z prawem. Włączając podmioty trzecie w proces przetwarzania Danych Osobowych, musimy przestrzegać określonych reguł, w szczególności zadbać o istnienie podstawy prawnej udostępnienia danych zarówno od strony Podmiotu Danych, jak i pomiędzy stronami transferu (np. zawarta umowa, wiążące reguły korporacyjne). Przekazywanie Danych Osobowych do państw trzecich tj. poza Unią Europejską wymaga zapewnienia należytej ochrony tych danych.
W odniesieniu do opisanych powyżej sytuacji pojęcie „osoby trzecie” obejmuje nie tylko zewnętrznych dostawców, sprzedawców, partnerów biznesowych, itd.

1. Dostawcy usług

1.1. Możemy korzystać z pomocy zewnętrznych dostawców usług w procesie przetwarzania danych.

1.2. Kiedy przekazujemy dane dostawcom zewnętrznym wyłącznie w celu Przetwarzania tych Danych Osobowych na polecenie i w imieniu Fundacji, te podmioty mogą przetwarzać Dane Osobowe wyłącznie w taki sposób, w jaki zostały przez nas poinstruowane, oraz w celach i w zakresie przez nas zdefiniowanych. Podmioty te są odpowiedzialne za przetwarzanie Danych Osobowych przy użyciu określonych środków ochrony i nie mogą przetwarzać tych danych w swoich własnych celach.

1.3. Kiedy włączamy dostawców zewnętrznych w nasze procesy przetwarzania danych, Fundacja zawsze będzie ostatecznie odpowiedzialna względem Podmiotów Danych oraz Organów Nadzorczych, w razie naruszenia ochrony Danych Osobowych, niezależnie czy dojdzie do tego po stronie Fundacji, czy tych podmiotów trzecich. Dlatego niezwykle istotne jest dokonanie ostrożnego ich wyboru oraz monitorowanie zewnętrznych dostawców, z którymi współpracujemy, pod kątem sposobu przetwarzania przez nich Danych Osobowych.

1.4. Te same zasady obowiązują również w drugą stronę, kiedy to Fundacja przetwarza Dane Osobowe na polecenie lub w imieniu osób lub podmiotów trzecich.

2. Przekazywanie danych osobom trzecim

2.1. Możemy przekazywać Dane Osobowe osobom trzecim dla ich celów projektowych, niezależnych od naszych celów.

2.2. Możemy to robić wyłącznie, gdy mamy do tego odpowiednie prawne podstawy (np. zgodę klienta).

2.3. To samo stosuje się do sytuacji, gdy otrzymujemy Dane Osobowe od podmiotów trzecich. Przed rozpoczęciem przetwarzania takich danych musimy sprawdzić, czy istnieją prawne podstawy do otrzymania przez nas tych danych w celach, w jakich mamy zamiar je wykorzystywać (np. dowód uzyskania zgody klienta przez podmiot trzeci, który nam te dane przekazuje).

3. Umowy z Przetwarzającymi

3.1. Jeśli dostawcy zewnętrzni przetwarzają dane wyłącznie na polecenie Fundacji (np. dostawca usług IT ma dostęp do naszej bazy danych), musimy się upewnić, że te podmioty udzielają Fundacji wystarczających gwarancji w zakresie stosowania środków organizacyjnych i technicznych w celu ochrony Danych Osobowych. W szczególności, musimy dysponować pisemną umową z tym dostawcą, zawierającą szczególne postanowienia dotyczące ochrony Danych Osobowych.

3.2. W razie, gdy przekazujemy Dane Osobowe osobie trzeciej, która nie przetwarza Danych Osobowych w naszym imieniu, ale we własnych celach, musimy również zawrzeć pisemną umowę z tą osobą trzecią zapewniającą, że będzie ona przetwarzać dane w zgodzie z odpowiednimi Przepisami z zakresu ochrony danych osobowych.

3.3. Musimy również przestrzegać powyższych zasad, gdy to Fundacja otrzymuje Dane Osobowe od podmiotów trzecich, niezależnie od tego, czy przetwarzamy te dane dla własnych celów projektowych, czy jako wsparcie dla podmiotów trzecich.

3.4. Powyższe zasady odnoszą się również do współpracowników Fundacji. Z nimi również muszą wiązać nas odpowiednie postanowienia umowne, jeśli są zaangażowani w przetwarzanie danych na polecenie lub w imieniu Fundacji.

3.5. Pracownicy i wolontariusze Fundacji zajmują się przetwarzaniem Danych Osobowych na podstawie i w zakresie udzielonych im upoważnień.

4. Przekazywanie Danych Osobowych do krajów spoza Unii Europejskiej (UE)

4.1. Eksport Danych Osobowych z kraju członkowskiego UE **do kraju spoza UE** jest dozwolony wyłącznie, jeśli podmiot otrzymujący te Dane Osobowe w swoim kraju zapewnia **adekwatny poziom ochrony** do obowiązującego w UE. Pewne kraje są uznane przez Komisję Europejską jako *„bezpieczne”*. Odbiorcy z tych krajów uznani są za zapewniający ochronę na adekwatnym poziomie.

4.2. Należy unikać przekazywania przez Fundację Danych Osobowych do podmiotów trzecich z siedzibą w państwach spoza UE, które nie są wymienione na liście jako kraje *„bezpieczne”*. Przekazanie danych do państw spoza UE, które nie znajdują się na liście krajów *„bezpiecznych”* podlega szczegółowym zasadom, w szczególności niezbędne jest zastosowanie w umowach z Odbiorcami odpowiednich standardowych klauzul umownych przyjętych przez Komisję Europejską oraz skontrolowanie zgodności ze standardami RODO Odbiorcy znajdującego się poza UE.

X. Dane wrażliwe

1. Wrażliwe Dane Osobowe to w szczególności (ale nie wyłącznie) dane, które ujawniają pochodzenie rasowe lub etniczne, dane biometryczne przetwarzane w celu jednoznacznego zidentyfikowania osoby fizycznej oraz dane dotyczące zdrowia.
2. Przetwarzanie danych wrażliwych jest co do zasady zabronione i jest przedmiotem specjalnych restrykcyjnych zasad. Przepisy z zakresu ochrony Danych Osobowych określają odrębny katalog podstaw prawnych uprawniających Administratora danych do przetwarzania danych wrażliwych.
3. Fundacja w ramach swojej działalności statutowej z zasady przetwarza dane wrażliwe. Dlatego niezwykle ważne jest, abyśmy zawsze byli w stanie zweryfikować, na jakiej podstawie dane wrażliwe będą podlegały przetwarzaniu. W każdym takim wypadku niezbędne jest ustalenie w porozumieniu z Zarządem – szczegółowych zasad takiego przetwarzania przed jego rozpoczęciem i zastosowanych środków bezpieczeństwa.

XI. Środki fizyczne i techniczne związane z przetwarzaniem Danych Osobowych

Do elementów zabezpieczenia Danych Osobowych w Fundacji zalicza się:

- stosowane metody ochrony pomieszczeń, w których przetwarzane są Dane Osobowe (zabezpieczenia fizyczne siedziby),
- inne zabezpieczenia Danych Osobowych, w szczególności dokumentów papierowych.

1. Zabezpieczenia fizyczne siedziby

1.1. Budynek (w którym znajduje się siedziba Fundacji), wchodzący w skład obszaru przetwarzania Danych Osobowych, jest chroniony przez firmę ochroniarską przez całą dobę.

1.2. Pomieszczenie, w którym przetwarzany jest zbiór Danych Osobowych, jest zabezpieczone drzwiami o podwyższonej odporności ogniowej, wyposażone w system alarmowy przeciwwłamaniowy, w system przeciwpożarowy i wolnostojącą gaśnicę.

1.3. Dostęp do pomieszczeń, wchodzących w skład obszaru przetwarzania danych osobowych, jest limitowany dwustopniowo:

1.3.1. na recepcji budynku,

1.3.2. na recepcji przestrzeni biurowej, w której znajduje się siedziba Fundacji.

2. Inne zabezpieczenia Danych Osobowych

2.1. Dokumenty papierowe zawierające Dane Osobowe i informacje poufne są przechowywane w zamykanych szafach bądź kasetkach.

2.2. Dostęp do kluczy do szaf i kasetek mają wyłącznie osoby upoważnione przez Zarząd.

2.3. Dokumenty archiwalne, gdy ustanie ich przydatność są niszczone w taki sposób, aby uniemożliwić z nich odczyt Danych Osobowych. Dokumentacja w formie papierowej powinna zostać zniszczona za pomocą niszczarki.

XII. Zabezpieczenia informatyczne

Do elementów zabezpieczenia Danych Osobowych w formie informatycznej w Fundacja zalicza się:

1. Obowiązek uwierzytelniania użytkownika i zasady korzystania z haseł

1.1. Każdorazowe uwierzytelnienie użytkownika w systemie informatycznym następuje po podaniu loginu i hasła. Login jest nadawany przez Zarząd wraz z nadaniem upoważnień do przetwarzania Danych Osobowych przez Fundację.

1.2. W Fundacji obowiązują następujące zasady korzystania z haseł:

1.2.1. Hasło użytkownika składa się z co najmniej 16 znaków,

1.2.2. Hasło zostało zweryfikowane jako „silne” np. przez algorytm Google i nie zawiera publicznie dostępnych informacji o użytkowniku (np. data urodzenia, imiona, itp.),
1.2.3. W przypadku zmiany hasła, hasła dotychczas wykorzystane przez użytkownika do logowania nie mogą być wykorzystane ponownie.

2. Procedury rozpoczęcia, zawieszenia i zakończenia pracy

2.1. Przed przystąpieniem do pracy w systemie informatycznym użytkownik zobowiązany jest sprawdzić urządzenie komputerowe i stanowisko pracy ze zwróceniem uwagi, czy nie zaszły okoliczności wskazujące na naruszenie ochrony Danych Osobowych.
2.2. Niedopuszczalne jest logowanie się na identyfikator i hasło innego użytkownika.
2.3. W przypadku opuszczenia stanowiska pracy (zawieszenie pracy) użytkownik zobowiązany jest wylogować się lub zaktywować wygaszacz ekranu z opcją ponownego logowania się do systemu z podaniem identyfikatora i hasła.
2.4. Zakończenie przez użytkownika pracy w systemie informatycznym następuje po wylogowaniu się z systemu. Po zakończeniu pracy użytkownik zabezpiecza swoje stanowisko pracy, w szczególności informatyczne nośniki Danych Osobowych, dokumenty i wydruki zawierające Dane Osobowe przed dostępem osób nieupoważnionych.

3. Sposób zabezpieczenia systemu informatycznego przed obecnością oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego

3.1. Sprawdzanie obecności oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu, w tym obecności wirusów komputerowych, dokonywane jest poprzez zainstalowanie oprogramowania, które skanuje wszystkie pliki automatycznie, tj. bez udziału użytkownika, na obecność wirusów. Program jest zainstalowany na serwerze i stacjach roboczych.
3.2. Informatyczne nośniki Danych Osobowych pochodzenia zewnętrznego (płyty CD, DVD, pendrive’y, dyski zewnętrzne) przed rozpoczęciem korzystania z nich podlegają sprawdzeniu przez aktywne zabezpieczenia antywirusowe obecne w systemie operacyjnym lub przez aktualizowany na bieżąco program antywirusowy.
3.3. Na bieżąco sprawdzane są wszystkie używane podczas pracy pliki z automatycznym usuwaniem wykrytych wirusów.
3.4. Regularnie są instalowane poprawki systemowe dotyczące bezpieczeństwa systemu informatycznego.

4. Sposób przechowywania, tworzenia oraz niszczenia (likwidacji) nośników informacji, w tym kopii informatycznych oraz wydruków

4.1. Informatyczne nośniki Danych Osobowych przechowywane są wyłącznie w zamykanych szafach bądź kasetkach zamykanych na klucz.
4.2. Wykorzystywane informatyczne nośniki Danych Osobowych muszą być zaszyfrowane.
4.3. System jest zabezpieczony przed utratą Danych Osobowych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej.
4.4. Kopie zapasowe zbiorów danych oraz programów służących do przetwarzania Danych Osobowych:
4.4.1. wykonywane są codziennie,
4.4.2. przechowywane są przez tydzień.
4.5. Kopie zmian zbiorów Danych Osobowych oraz programów służących do przetwarzania danych:
4.5.1. wykonywane są codziennie,
4.5.2. przechowywane są przez rok.

4.6. Fizycznej likwidacji zniszczonych lub niepotrzebnych informatycznych nośników danych z Danymi Osobowymi należy dokonywać w sposób uniemożliwiający odczyt Danych Osobowych.

5. Zasady postępowania z komputerami przenośnymi

5.1. Osoba użytkująca komputer przenośny zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania, w tym stosuje środki ochrony kryptograficznej wobec przetwarzanych Danych Osobowych.

5.2. W szczególności należy:

5.2.1. Używać dodatkowego zabezpieczenia dostępu do komputera.

5.2.2. Nie zezwalać na używanie komputera osobom nieupoważnionym.

5.2.3. Pliki z Danymi Osobowymi znajdujące się na komputerze należy dodatkowo chronić hasłem.

6. Zasady postępowania z telefonami

6.1. Osoba użytkująca telefon, za pośrednictwem którego przetwarza Dane Osobowe, zachowuje szczególną ostrożność podczas jego transportu, przechowywania i użytkowania.

6.2. W szczególności należy:

6.2.1. Używać hasła do zabezpieczenia dostępu do telefonu.

6.2.2. Nie zezwalać na używanie telefonu osobom nieupoważnionym.

XIII. Postępowanie w razie wystąpienia naruszenia ochrony Danych Osobowych

1. Każdy pracownik (współpracownik) i wolontariusz Fundacji ma obowiązek dbałości o ochronę danych przed niechcianym, nieautoryzowanym i bezprawnym użyciem lub dostępem oraz obowiązek przestrzegania zasad ustalonych przez Zarząd lub osobę przez niego wskazaną, np. praw dostępu i poufności oraz informowania natychmiast Zarządu w razie wystąpienia naruszenia ochrony Danych Osobowych.
2. W przypadku, gdy Fundacja jest Przetwarzającym Dane Osobowe, niezbędne jest dokonanie powiadomienia o naruszeniu samego Administratora danych.
3. W razie wystąpienia naruszenia ochrony Danych Osobowych, należy stosować się do Polityki postępowania z naruszeniami dotyczącymi Danych Osobowych.

XIV. Zapewnianie zgodności z Przepisami z zakresu ochrony danych osobowych

1. Szkolenia

1.1. Każdy pracownik (współpracownik) i wolontariusz musi na bieżąco uczestniczyć w wewnętrznych szkoleniach z zakresu ochrony Danych Osobowych organizowanych przez Fundację, w celu poprawy oraz aktualizacji wiedzy odnośnie reguł i zasad ochrony Danych Osobowych.

1.2. Wszyscy pracownicy i wolontariusze Fundacji zostaną zapoznani z niniejszą procedurą, procedurami szczególnymi oraz zasadami ochrony Danych Osobowych obowiązującymi w Fundacji.

1.3. Znajomość zasad przetwarzania Danych Osobowych obowiązujących w Fundacji będzie weryfikowana i monitorowana przez Fundację.

2. Monitoring

2.1. Fundacja dba o zapewnienie zgodności z Przepisami z zakresu ochrony Danych Osobowych, zapewniając regularny monitoring zgodności tj. czynności mające na celu zweryfikowanie

zgodności przetwarzania Danych Osobowych z Przepisami z zakresu ochrony Danych Osobowych, niniejszą procedurą oraz szczegółowymi procedurami.

3. Audyty

3.1. Niezależnie od monitoringu, weryfikacja i potwierdzenie zgodności z Przepisami z zakresu ochrony Danych Osobowych może dodatkowo przeprowadzać wewnętrzny lub zewnętrzny audytor. Audyty przeprowadzane są na zlecenie Zarządu.

3.2. Audytorzy dokumentują przeprowadzenie czynności kontrolnych oraz po zakończeniu audytu przygotowują sprawozdanie, które przekazują do Zarządu; w szczególności w przypadku dostrzeżenia istotnych nieprawidłowości przekazuje informacje na ich temat niezwłocznie Zarządowi.

XV. Kontakt z władzami

1. W razie otrzymania żądania od przedstawiciele jakichkolwiek władz, tj. Organów Nadzorczych (np. Prezesa Urzędu Ochrony Danych Osobowych), policji, sądu (np. biegłego sądowego), organów podatkowych, ZUS itd., dotyczących dostępu do Danych Osobowych przetwarzanych przez Fundację lub z pytaniami dotyczącymi czynności przetwarzania dokonywanych przez Fundację, należy treść żądania niezwłocznie przekazać do Zarządu.
2. W każdym wypadku wszelkie kontakty z władzami (zarówno z inicjatywy Fundacji, jak i w odpowiedzi na żądanie władz) dokonywane na rzecz lub w imieniu Fundacji, w odniesieniu do jakichkolwiek kwestii związanych z czynnościami przetwarzania Danych Osobowych, muszą się odbywać za pośrednictwem lub co najmniej z udziałem Zarządu.
3. Kontrolę przestrzegania Przepisów z zakresu ochrony Danych Osobowych przeprowadzają pracownicy Urzędu Ochrony Danych Osobowych (ewentualnie organu nadzorczego innego państwa członkowskiego UE w przypadku prowadzenia wspólnych operacji z polskim urzędem) po okazaniu imiennego upoważnienia oraz legitymacji służbowej.

Załączniki

1. Procedura obsługi praw Podmiotów Danych
2. Procedura retencji Danych Osobowych
3. Polityka postępowania z naruszeniami dotyczącymi Danych Osobowych
4. Formularz zgody
5. Klauzula informacyjna
6. Upoważnienie do przetwarzania
7. Umowa powierzenia przetwarzania
8. Rejestr czynności przetwarzania