Fundacja EduMind by Smartt

Polityka bezpieczeństwa i ochrony danych

Spis Treści:

I. Zakres i cel dokumentu

1. Polityka bezpieczeństwa i ochrony danych osobowych **Fundacji EduMind by Smartt** z siedzibą w Warszawie („**Fundacja**"), zwana dalej „**Polityką**", określa zasady bezpieczeństwa w odniesieniu do danych osobowych, których Administratorem jest **Fundacja**, zgodnie z Rozporządzeniem 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 – zwane dalej **„RODO"**).

2. Polityka ma odpowiednie zastosowanie do przetwarzania przez **Fundację** Danych osobowych, których Administratorami są inne podmioty, chyba że postanowienia umów zawartych z tymi podmiotami stanowią inaczej.

3. Polityka ma zastosowanie we wszystkich procesach związanych z przetwarzaniem Danych osobowych, projektowanych i wdrażanych od 25 maja 2018 r., jak też wdrożonych przed tą datą i kontynuowanych po 25 maja 2018 r.

4. Celem Polityki jest zapewnienie poprawnego wykonania obowiązków nałożonych na **Fundację** przepisami RODO.

II. Kompetencje- odpowiedzialność

1. Za opracowanie, zatwierdzenie i wdrożenie do stosowania niniejszej Polityki odpowiedzialny jest Zarząd **Fundacji**.

2. Realizację zadań w zakresie ochrony Danych osobowych w **Fundacji** nadzoruje Zarząd.

3. Wszystkie funkcje i obowiązki zawarte w niniejszej Polityce wykonywane są przez Zarząd i osoby upoważnione przez Zarząd.

4. Za stosowanie niniejszej Polityki odpowiedzialni są wszyscy pracownicy i współpracownicy, którzy wykonując obowiązki służbowe uczestniczą w procesie przetwarzania Danych osobowych.

III. Definicje

1. **Administrator –** podmiot ustalający cele i sposoby przetwarzania Danych osobowych. **Fundacja** reprezentowana przez Zarząd jest Administratorem.

2. **Administrator Systemu Informatycznego –** osoba wyznaczona przez Zarząd zobowiązana do zarządzania systemami informatycznymi wykorzystywanymi do przetwarzania danych osobowych, odpowiedzialna za sprawność, konserwację oraz wdrażanie technicznych zabezpieczeń Systemu Informatycznego, na podstawie umowy z Administratorem.

3. **Bezpieczeństwo informacji** – zachowanie poufności, integralności, dostępności oraz rozliczalności informacji.

4. Dane osobowe (Dane) – wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej.
5. Dostęp do Danych osobowych – umożliwienie wglądu lub bezpośredniego wykonywania operacji na Danych osobowych.
6. Naruszenie ochrony Danych osobowych (Naruszenie) - 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. Na potrzeby niniejszej Polityki Naruszeniem jest również niedozwolone lub niezgodne z prawem Przetwarzanie Danych.
7. Nośniki Informacji / Nośniki - wszelkiego rodzaju nośniki służące do zapisu informacji w postaci cyfrowej, w szczególności dyski twarde, pamięci typu flash, płyty CD/DVD/Blu-ray, dyski magneto-optyczne, dyski SSD taśmy DLT/DDS, karty pamięci, karty chipowe, itd., które stanowią własność Fundacji, bądź stanowią własność innych osób fizycznych, prawnych lub jednostek organizacyjnych nie posiadających osobowości prawnej, ale są wykorzystywane do Przetwarzania Danych osobowych w Fundacji.
8. Odbiorca Danych osobowych (Odbiorca) – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się Dane osobowe. Organy publiczne, które mogą otrzymywać Dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są uznawane za Odbiorców.
9. Osoby przetwarzające Dane osobowe – osoby wykonujące jakiekolwiek operacje na Danych osobowych lub jedynie mające wgląd do Danych osobowych.
10. Państwo trzecie – państwo nienależące do Europejskiego Obszaru Gospodarczego.
11. PUODO – Prezes Urzędu Ochrony Danych Osobowych – organ nadzorczy właściwy w sprawach ochrony Danych osobowych.
12. Pracownik / współpracownik – osoba fizyczna zatrudniona w Fundacji na podstawie umowy o pracę, jak również na podstawie umowy cywilnoprawnej, w szczególności umowy zlecenia lub umowy o dzieło, w tym praktykanci i stażyści oraz wolontariusze. W każdym przypadku użycie pojęcia „pracownik" oznacza także współpracownika.
13. Powierzenie przetwarzania Danych osobowych (Powierzenie) – przekazanie zbioru danych, jego fragmentu, pojedynczych Danych osobowych lub przyznanie dostępu do Danych osobowych, na mocy umowy zawartej przez Fundację z innym podmiotem na podstawie art. 28 RODO, w celu ich przetwarzania przez ten podmiot w imieniu Fundacji; obejmuje to także dalsze powierzenie przetwarzania danych przetwarzanych przez Fundację w imieniu innych podmiotów.
14. Privacy by default (domyślna ochrona Danych) – zapewnienie, poprzez odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te Dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu Przetwarzania (dotyczy to ilości zbieranych Danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności). W szczególności środki te powinny zapewniać, by Dane osobowe nie były udostępniane bez interwencji (woli) danej osoby nieokreślonej liczbie osób fizycznych.
15. Privacy by design (ochrona Danych w fazie projektowania) – wdrożenie, na etapie projektowania, a następnie przetwarzania, odpowiednich środków technicznych i organizacyjnych w celu

skutecznej realizacji zasad ochrony Danych, w szczególności niezbędnego zabezpieczenia procesu przetwarzania Danych oraz ochrony praw osób, których Dane dotyczą.

16. Przetwarzanie Danych (przetwarzanie) – operacja lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, takie 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.
17. Rejestr – Rejestr czynności przetwarzania danych, o którym mowa w art. 30 RODO.
18. RODO - Rozporządzenie 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).
19. System Informatyczny – zespół współpracujących ze sobą środków technicznych i oprogramowania (infrastruktury i aplikacji) stanowiący integralną i logiczną całość wyodrębnioną ze względu na dostarczaną funkcjonalność przy założeniu, że głównym jego celem jest przetwarzanie informacji (w tym Danych osobowych).
20. Udostępnienie Danych – przekazanie uprawnionemu Odbiorcy Danych osobowych wybranych według określonych kryteriów, na podstawie pozytywnie rozpatrzonego wniosku lub umowy, w formie papierowej, na innym nośniku informacji lub poprzez umożliwienie dostępu do wyselekcjonowanych Danych w Systemie Informatycznym, do ich samodzielnego przetwarzania przez Odbiorcę jako odrębnego Administratora lub jako podmiot przetwarzający.
21. Urządzenie mobilne – przenośne urządzenie elektroniczne pozwalające na przetwarzanie informacji bez konieczności utrzymywania przewodowego połączenia z siecią, w szczególności telefon komórkowy, smartfon, palmtop, tablet, MDA (Mobile Digital Assistant), których typowym zastosowaniem może być odbieranie i wysyłanie poczty elektronicznej oraz przeglądanie stron sieci WWW za pomocą aplikacji mobilnych, z wyłączeniem komputerów przenośnych oraz elektronicznych nośników informacji.
22. Usunięcie Danych osobowych – zniszczenie Danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której Dane dotyczą (anonimizacja). Usunięcie Danych osobowych jest procesem trwałym i nieodwracalnym.

IV. Cele i zasady przetwarzania Danych osobowych

1. Fundacja przetwarza Dane w celach związanych z przedmiotem jej statutowej działalności, w szczególności dane osobowe pracowników, osób aplikujących o pracę lub wolontariat, uczestników wydarzeń (w tym kursów) organizowanych przez Fundację, a także w celu wykonywania obowiązków wynikających z powszechnie obowiązujących przepisów prawa oraz Dane powierzone przez inne podmioty będące ich administratorem.
2. Zasady określone w niniejszej Polityce obowiązują wszystkich pracowników Fundacji, jeżeli dla realizacji ich zadań konieczne jest przetwarzanie Danych osobowych, których Administratorem jest Fundacja lub powierzonych Fundacji na podstawie umowy zawartej z innym podmiotem, który jest ich administratorem.

3. Polityka ma zastosowanie do wszystkich Danych przetwarzanych w **Fundacji** za pośrednictwem Systemu Informatycznego, w formie papierowej, innych nośników informacji, jak i ustnie.
4. Udostępnianie jakichkolwiek Danych przetwarzanych przez **Fundację** na zewnątrz może następować wyłącznie w związku z realizacją celów statutowych **Fundacji.**
5. **Fundacja** przetwarza Dane osobowe zgodnie z następującymi zasadami wynikającymi z powszechnie obowiązujących przepisów prawa i dokumentów wewnętrznych **Fundacji** (w tym niniejszej Polityki):
   a. zgodności z prawem, rzetelności i przejrzystości (przetwarzanie Danych musi mieć legalną podstawę; odbywać się z poszanowaniem interesów i praw osób, których dane dotyczą; być transparentne dla osób, których dotyczą przetwarzane Dane);
   b. ograniczenia celu (cel Przetwarzania Danych musi być konkretny, wyraźny i prawnie uzasadniony; nie można przy tym Przetwarzać Danych niezgodnie z tym celem);
   c. minimalizacji Danych (Dane powinny być odpowiednie i niezbędne do celu Przetwarzania);
   d. prawidłowości Danych (Dane powinny być zgodne z prawdą, kompletne i aktualne);
   e. ograniczenia przechowywania (Dane muszą być Przetwarzane wyłącznie w okresie, w jakim konieczne jest to dla osiągnięcia zgodnego z prawem celu Przetwarzania);
   f. integralności, poufności i dostępności (Dane muszą być Przetwarzane w sposób zapewniający im bezpieczeństwo, w tym ochronę przed niedozwolonym lub niezgodnym z prawem Przetwarzaniem, przypadkową utratą, zniszczeniem lub uszkodzeniem);
   g. rozliczalności (przy Przetwarzaniu Danych wymagane jest przestrzeganie zasad wskazanych w pkt 1) – 6) powyżej i umiejętność wykazania ich przestrzegania).

V. Obowiązki osób posiadających dostęp do Danych osobowych

1. Wszyscy pracownicy, którzy wykonując swoje obowiązki służbowe mają Dostęp do Danych osobowych przetwarzanych w **Fundacji**, są obowiązani do:
   a. zapoznania się i ścisłego przestrzegania przepisów prawa oraz wewnętrznych procedur regulujących zasady ochrony Danych osobowych przyjętych w **Fundacji**;
   b. uczestniczenia w szkoleniach zapewnianych przez **Fundację**;
   c. uwzględniania we wszystkich planowanych i wdrożonych procesach, rozwiązaniach techniczno-organizacyjnych lub narzędziach, związanych z przetwarzaniem Danych:
      (i) zasady *Privacy by design* (ochrona Danych w fazie projektowania) oraz *Privacy by default* (domyślna ochrona Danych), a także
      (ii) wyników oceny PIA, jeżeli taka będzie wykonywana
   d. bezterminowego zachowania w tajemnicy przetwarzanych Danych osobowych oraz sposobów ich zabezpieczenia,

e. zgłaszania do Zarządu i wyjaśniania wszelkich wątpliwości dotyczących prawidłowości Przetwarzania Danych osobowych,

f. współpracy z Zarządem w przypadku przeprowadzanych w **Fundacji** Audytów (zarówno wewnętrznych, jak i zewnętrznych), jak też kontroli przeprowadzanej przez PUODO;

g. niezwłocznego przygotowywania i przesyłania na żądanie Zarządu informacji dotyczących Przetwarzania Danych osobowych (zgodnie z zakresem żądania);

h. prowadzenia i przestrzegania ewidencji osób upoważnionych do Przetwarzania Danych osobowych w ramach zadań realizowanych przez podległych pracowników,

i. nadzorowania podległych pracowników w zakresie wypełniania obowiązków opisanych w niniejszej Polityce,

j. zgłaszania każdej czynności, której elementem jest przetwarzanie Danych osobowych (z wyłączeniem Przetwarzania Danych wizytówkowych w celach komunikacyjnych) do Rejestru.

2. Ponadto pracownicy stosują wymagania bezpieczeństwa Systemu Informatycznego przyjętego w **Fundacji**.

VI. Realizacja praw osób, których Dane dotyczą

1. **Fundacja** realizuje prawa osób, których Dane dotyczą, tj.:
   a. prawo do informacji oraz uzyskania potwierdzenia Przetwarzania Danych przez Administratora, i dostępu do Danych,
   b. prawo do wycofania zgody;
   c. prawo do sprostowania/uzupełnienia Danych,
   d. prawo do Usunięcia Danych („prawo do bycia zapomnianym”),
   e. prawo do ograniczenia Przetwarzania,
   f. prawo do przenoszenia Danych,
   g. prawo do sprzeciwu wobec przetwarzania Danych osobowych,
   h. prawo do niepodlegania decyzjom podjętym w warunkach zautomatyzowanego przetwarzania Danych, w tym profilowania.
2. Realizację obsługi wniosków osób, których Dane dotyczą zapewnia Zarząd zgodnie z **Instrukcją postępowania w sprawie żądań podmiotów danych**.

VII. Rejestr

1. Zarząd prowadzi Rejestr.
2. Każdy Pracownik odpowiada za aktualizację informacji w Rejestrze, w tym o zaprzestaniu przetwarzania Danych osobowych, w szczególności:

1) niezwłoczne zgłasza fakt utworzenia nowego zbioru danych,

2) niezwłoczne zgłasza i aktualizuje informacje o procesie przetwarzania Danych osobowych, w tym o zaprzestaniu przetwarzania Danych osobowych.

3. Za sporządzenie i przekazanie do Zarządu poprawnego zgłoszenia do Rejestru lub jego aktualizacji w zakresie umów powierzenia albo udostępnienia Danych odpowiada pracownik odpowiedzialny merytorycznie za zawarcie umowy, zgodnie z pkt. VIII i IX Polityki.

VIII. Udostępnianie Danych

1. Decyzję w sprawie Udostępnienia Danych, w tym udostępniania Danych na wniosek uprawnionych organów państwa podejmuje Zarząd **Fundacji**.
2. Udostępnienie Danych osobowych, których Administratorem jest **Fundacja** jest odnotowywane w Rejestrze, po zgłoszeniu przez osobę odpowiedzialną merytorycznie za realizację Udostępnienia.
3. Udostępnienie Danych do Państwa trzeciego jest możliwe wyłącznie na zasadach określonych w obowiązujących przepisach prawa (Artykuł 44 i następne RODO).

IX. Powierzenie Danych

1. **Fundacja** jako Administrator może powierzyć innemu podmiotowi (podmiotowi przetwarzającemu) przetwarzanie Danych osobowych w imieniu **Fundacji** wyłącznie na podstawie pisemnej umowy zawartej z tym podmiotem, przy czym może nim być wyłącznie podmiot, który daje gwarancje prawidłowego i bezpiecznego Przetwarzania Danych osobowych.
2. **Fundacja** jako podmiot przetwarzający Dane może powierzyć dane innemu podmiotowi wyłącznie w celach i na zasadach określonych w umowie pomiędzy administratorem danych a **Fundacją** jako podmiotem przetwarzającym.
3. Umowa Powierzenia przetwarzania Danych osobowych, w której **Fundacja** występuje jako Administrator Danych lub jako podmiot przetwarzający, musi odpowiadać wymogom art. 28 RODO i podlega uprzedniej akceptacji Zarządu.
4. Powierzenie przetwarzania Danych osobowych, których Administratorem jest **Fundacja**, jest odnotowywane w Rejestrze, po zgłoszeniu przez osobę odpowiedzialną merytorycznie za zawarcie umowy.
5. W przypadku dostępu podmiotów zewnętrznych do Systemu Informatycznego, w celu wdrażania, napraw, przeglądów, konserwacji lub utrzymania tego Systemu, jeżeli podmiot zewnętrzny uzyskuje również Dostęp do Danych osobowych przetwarzanych w tym Systemie, należy zawrzeć umowę Powierzenia przetwarzania Danych osobowych, zgodnie z postanowieniami pkt 1 – 3 powyżej,
6. W przypadku zamiaru zawarcia umowy Powierzenia, w której **Fundacja** ma występować jako podmiot przetwarzający, osoba odpowiedzialna za jej zawarcie zobowiązana jest do jej zgłoszenia do Rejestru.
7. **Fundacja** jako Administrator może powierzać Dane do Państwa trzeciego na zasadach zgodnych z obowiązującymi przepisami prawa, przy czym decyzję w tym przedmiocie podejmuje Zarząd po przedstawieniu przez osobę odpowiedzialną merytorycznie za przedsięwzięcie związane z Powierzeniem Danych.

8. Powierzenie Danych, których Administratorem jest **Fundacja**, do Państwa trzeciego jest odnotowywane w Rejestrze po zgłoszeniu przez osobę odpowiedzialną merytorycznie za zawarcie umowy.

9. W przypadku, kiedy **Fundacja** wspólnie z innymi podmiotami ustala cele i sposoby Przetwarzania Danych osobowych (współadministrowanie danymi), należy zawrzeć umowę, która będzie regulowała zakresy odpowiedzialności każdego ze współadministratorów oraz relacje pomiędzy współadministratorami a podmiotami, których Dane dotyczą.

10. Zawarcie umowy o współadministrowanie Danymi jest odnotowywane w Rejestrze po zgłoszeniu przez osobę odpowiedzialną merytorycznie za jej zawarcie.

X. Zarządzanie Dostępem do Danych osobowych

1. Do Przetwarzania Danych mogą być dopuszczone jedynie osoby do tego upoważnione. Administrator upoważnia do Przetwarzania Danych każdą osobę Przetwarzającą Dane osobowe w związku z realizacją swoich obowiązków wobec Administratora, z zastrzeżeniem ust. 3 poniżej.
2. Upoważnienie do Przetwarzania Danych osobowych zawarte jest w umowie o pracę, kontrakcie managerskim, umowie zlecenia, innego rodzaju umowie o współpracy zawartej bezpośrednio między **Fundacją** a pracownikiem.
3. Warunki Dostępu do Danych osobowych, których Administratorem jest **Fundacja** przez podmiot przetwarzający określone mogą być w umowie Powierzenia przetwarzania Danych osobowych zawartej przez **Fundację** z podmiotem przetwarzającym.
4. Pracownicy upoważnieni do Przetwarzania Danych osobowych zobowiązani są:
   a. odbyć szkolenie z zasad ochrony Danych osobowych i podpisać, stanowiące element stosunku pracy, oświadczenie o zapoznaniu się z przepisami prawa w zakresie ochrony Danych osobowych oraz obowiązujących w **Fundacji** zasadach ochrony Danych osobowych,
   b. złożyć, stanowiące element stosunku pracy, zobowiązanie o bezterminowym zachowaniu w tajemnicy przetwarzanych Danych osobowych oraz sposobów ich zabezpieczenia,
   c. w przypadku zmiany zakresu zadań lub miejsca świadczenia pracy w **Fundacji**, skutkujących brakiem konieczności Przetwarzania Danych osobowych, lub rozwiązania umowy o pracę z pracownikiem jest on zobowiązany do zwrotu pracodawcy dokumentacji lub innych nośników zawierających Dane osobowe.
5. Ewidencja osób upoważnionych do przetwarzania Danych osobowych w Systemie Informatycznym prowadzona jest przez osobę wskazaną przez Zarząd, pod nadzorem Zarządu.
6. Dostęp do Danych osobowych przetwarzanych poza Systemem Informatycznym realizowany jest pod nadzorem Zarządu.

XI. Miejsca Przetwarzania Danych osobowych

1. Miejsca przetwarzania Danych osobowych, tj. budynki, pomieszczenia lub części pomieszczeń tworzące obszar, w którym przetwarzane są Dane osobowe, podlegają ochronie poprzez zastosowanie środków ochrony fizycznej oraz przyjęcie odpowiednich rozwiązań organizacyjnych, chroniących przed nieuprawnionym dostępem do Danych. Miejscem przetwarzania danych jest wyłącznie siedziba Fundacji.
2. Osoby trzecie wchodzące do lokalu są przyjmowane przez upoważnionych pracowników sekretariatu, którzy zapewniają poufność Danych osobowych.
3. Z wyjątkiem miejsc dedykowanych do spotkań z osobami trzecimi, przebywanie osób nieuprawnionych w miejscach, o których mowa w ust. 1, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania Danych osobowych.
4. Miejsca, o których mowa w ust. 1, muszą być zabezpieczone na czas nieobecności w nich osób upoważnionych do przetwarzania Danych osobowych, w sposób uniemożliwiający dostęp fizyczny do nich osób nieuprawnionych.
5. Z wyjątkiem miejsc dedykowanych do spotkań z osobami trzecimi, zabrania się w miejscach, o których mowa w ust. 1, utrwalania obrazu lub dźwięku, jak również transmisji obrazu lub dźwięku poza te miejsca, z wyłączeniem sytuacji, gdy czynności te są podejmowane w ramach stosowanych środków ochrony fizycznej.
6. Osoby upoważnione do przetwarzania Danych osobowych zobowiązane są do kontrolowania, czy w miejscach, o których mowa w ust. 1, nie pozostały niezabezpieczone dokumenty lub materiały zawierające Dane osobowe (tj. przestrzegania zasady „czystego biurka").
7. Konserwacja, naprawa i obsługa awaryjna urządzeń i Systemu Informatycznego w miejscach, o których mowa w ust. 1, musi odbywać się po uzgodnieniu z Zarządem i w obecności osób upoważnionych do przetwarzania Danych osobowych.

XII. Przetwarzanie Danych osobowych w Systemie Informatycznym

1. Wszystkie urządzenia i System Informatyczny służący do przetwarzania Danych osobowych muszą:
   a. spełniać wymagania techniczne i organizacyjne adekwatne do ryzyka związanego z Przetwarzaniem Danych osobowych,
   b. uwzględniać zasadę *Privacy by default* (domyślna ochrona Danych) oraz *Privacy by design* (ochrona Danych w fazie projektowania), a także
2. System Informatyczny zapewnia poufność, integralność i rozliczalność przetwarzanych Danych osobowych.
3. Dane osobowe przetwarzane na mobilnych stacjach roboczych (komputerach przenośnych), muszą być szyfrowane.
4. Każdy dokument elektroniczny zawierający Dane osobowe, jeżeli jest to możliwe technologicznie, powinien być zabezpieczony przed nieuprawnionym dostępem (zaszyfrowany).
5. Bez wyraźnej zgody osoby, której Dane dotyczą zabrania się przesyłania Danych osobowych:
   1) na prywatne adresy poczty elektronicznej,

2) z wykorzystaniem komunikatorów społecznościowych (np. WhatsApp, Facebook Messenger, Snapchat, itp.).

6. Bez wyraźnej zgody osoby, której Dane dotyczą zabrania się udostępniania Danych osobowych na serwisach społecznościowych (np. Facebook, Twitter, Instagram).

XIII. Przetwarzanie Danych osobowych na Urządzeniach mobilnych

1. Przetwarzanie Danych osobowych na Urządzeniach mobilnych musi być ograniczone tylko do niezbędnych przypadków i musi wynikać z realizacji zadań służbowych oraz uzyskać akceptację Zarządu.
2. Dane przetwarzane na Urządzeniu mobilnym muszą być zabezpieczone przed uzyskaniem dostępu do nich osób nieupoważnionych (urządzenie powinno być zabezpieczone kodem PIN, a dane jeśli będzie to technicznie możliwe zaszyfrowane).
3. Podczas transportu Urządzenia mobilnego jego użytkownik obowiązany jest zabezpieczyć je przed utratą, zabraniem przez osobę nieuprawnioną oraz przed dostępem osób nieupoważnionych do znajdujących się w nim Danych osobowych.
4. Użytkownik za każdym razem blokuje Urządzenie mobilne po zakończeniu pracy na nim. Dostęp do Danych osobowych na Urządzeniu mobilnym musi być poprzedzony wprowadzeniem PIN.
5. Zabrania się wyświetlania Danych na Urządzeniach mobilnych w bezpośredniej obecności osób nieupoważnionych, w szczególności w miejscach publicznych.
6. Zabrania się współdzielenia Urządzenia mobilnego z osobami nieupoważnionymi.

XIV. Przetwarzanie Danych osobowych poza Systemem Informatycznym

1. Dokumenty papierowe zawierające Dane osobowe, należy chronić przed uszkodzeniem, zniszczeniem lub udostępnieniem osobom nieupoważnionym.
2. Dokumenty powinny być fizycznie chronione przed utratą oraz dostępem osób nieupoważnionych. Zasada "czystego biurka" oznacza, że wszystkie dokumenty zawierające Dane osobowe, należy po zakończeniu dnia pracy przechowywać w miejscu gwarantującym brak dostępu osób nieuprawnionych (np.: meble biurowe zamykane na klucz).
3. Każdy dokument papierowy zawierający Dane osobowe, po ustaniu konieczności jego wykorzystania należy zniszczyć w bezpieczny sposób uniemożliwiający odczytanie treści tych dokumentów. Do chwili zniszczenia należy przechowywać w bezpiecznym miejscu, uniemożliwiającym dostęp osobom nieupoważnionym (np.: meble biurowe zamykane na klucz).
4. Zabrania się kopiowania jakichkolwiek Danych osobowych zawartych w dokumentach papierowych bez zgody bezpośredniego przełożonego.
5. Zasada „czystej drukarki” oznacza, że wydruki i kopie zawierające Dane osobowe są wykonywane wyłącznie przez pracownika, który jest zobowiązany do niezwłocznego zabrania ich z drukarki.
6. Dokumenty zawierające Dane osobowe przesyła się zapakowane w mocną, nieprzezroczystą kopertę, jako przesyłki polecone za potwierdzeniem odbioru, za pośrednictwem firm świadczących usługi pocztowe i kurierskie.

7. Elektroniczne Nośniki informacji z Danymi osobowymi należy chronić przed ich fizycznym uszkodzeniem lub zniszczeniem, co uniemożliwiłoby odczytanie lub odzyskanie informacji na nich zawartych.
8. Elektroniczne Nośniki informacji z Danymi osobowymi wykorzystywane przez użytkowników powinny być fizycznie zabezpieczone przed utratą oraz dostępem osób nieupoważnionych.
9. Opuszczając miejsce pracy, Nośniki informacji należy zabezpieczyć w sposób uniemożliwiający dostęp osób nieupoważnionych (np.: przechowywać w meblach biurowych zamykanych na klucz).
10. Zabrania się kopiowania jakichkolwiek Danych osobowych na Nośniki informacji w celach innych niż służbowe. Liczbę elektronicznych kopii dokumentów zawierających Dane osobowe należy ograniczyć do niezbędnego minimum.
11. Wykorzystanie Nośników informacji typu pendrive, dysk zewnętrzny itp. umożliwiających zapis danych, winien być limitowany i umożliwiony tylko w niezbędnych przypadkach za zgodą bezpośredniego przełożonego. Dostęp do Danych na tych nośnikach powinien być szyfrowany.

XV. Postępowanie w sytuacjach Naruszenia ochrony Danych osobowych

1. Każdy, kto uzyskał informację o podejrzeniu Naruszenia ochrony Danych osobowych Przetwarzanych w Systemie Informatycznym i poza Systemem, a także o przypadku przełamania lub próby przełamania zastosowanych środków ochrony fizycznej oraz przyjętego systemu ochrony miejsc, w których Przetwarza się Dane osobowe, obowiązany jest do niezwłocznego, po uzyskaniu takiej informacji, zgłoszenia Naruszenia do Zarządu.
2. Zgłoszone Naruszenia analizowane są zgodnie z postanowieniami wewnętrznych procedur i przekazywane do Zarządu.
3. Zgodnie z obowiązującymi przepisami prawa, po potwierdzeniu, że doszło do Naruszenia:
   1) Zarząd zgłasza Naruszenie PUODO;
   2) osoba, której Danych dotyczy Naruszenie, jest o nim zawiadamiana

zgodnie z postanowieniami ‘Instrukcji postępowania w sytuacji naruszenia ochrony danych osobowych’.

XVI. Audyty

1. Audyt zgodności Przetwarzania Danych osobowych w **Fundacji** z przepisami o ochronie Danych osobowych obejmuje wszystkie stanowiska pracy w **Fundacji**, w których Przetwarzane są Dane osobowe, oraz podmioty przetwarzające, którym **Fundacja** powierzyła Dane osobowe do przetwarzania.
2. Audyt zgodności Przetwarzania Danych osobowych z przepisami o ochronie Danych osobowych odbywa się w trybie:
   1) Audytu planowego – zgodnego z zatwierdzonym przez Zarząd planem audytów,
   2) Audytu doraźnego - prowadzonego w przypadkach Naruszenia ochrony Danych osobowych lub uzasadnionego podejrzenia wystąpienia takiego Naruszenia.
3. Audyt planowy jest prowadzony przez wskazanych przez Zarząd pracowników.

4. Audyt doraźny prowadzony jest przez wskazanych przez Zarząd pracowników. Osoby prowadzące audyt doraźny lub uczestniczące w nim w charakterze ekspertów, przekazują Zarządowi raport z Audytu niezwłocznie po jego zakończeniu.
5. Po zakończeniu Audytu przygotowywany jest raport. Raport sporządzany jest w postaci elektronicznej lub papierowej i przedstawiany Zarządowi.

XVII. Kontrole PUODO

1. Na zasadach przewidzianych w obowiązujących przepisach prawa PUODO może przeprowadzać w Fundacji kontrole zgodności Przetwarzania Danych z przepisami o ochronie Danych osobowych.
2. Każdy, kto uzyskał informację o kontroli PUODO obowiązany jest do niezwłocznego poinformowania o niej Zarząd lub bezpośredniego przełożonego, który z kolei zawiadamia o niej Zarząd. Upoważniony przez Zarząd pracownik Fundacji, odpowiedzialny za kontrolowany przez PUODO obszar, uczestniczy w czynnościach kontrolnych podejmowanych przez PUODO osobiście albo poprzez wyznaczonych pracowników.
3. O wynikach kontroli przeprowadzonej przez PUODO, pracownik, o którym mowa w ust. 2 informuje Administratora.

XVIII. Postanowienia końcowe

1. W sprawach nieuregulowanych postanowieniami Polityki mają zastosowanie powszechnie obowiązujące przepisy prawa.
2. Nieprzestrzeganie postanowień Polityki przez pracowników Fundacji skutkować będzie podjęciem działań dyscyplinujących wynikających z przepisów Kodeksu Pracy.