Załącznik 1. Polityka bezpieczeństwa danych osobowych FDDS

Tekst jednolity 19 maja 2021 roku

Polityka bezpieczeństwa ochrony danych osobowych Fundacji Dajemy Dzieciom Siłę

Polityka bezpieczeństwa jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Fundację Dajemy Dzieciom Siłę w celu spełnienia wymagań rozporządzenia PE i RE 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych, zwanego dalej „RODO" oraz ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r., ustawy o ochronie danych osobowych z dnia 10 maja 2018 r., zwanymi dalej „ustawami".
Polityka stanowi jeden ze środków organizacyjnych, mających na celu wykazanie, że przetwarzanie danych osobowych odbywa się zgodnie z tym rozporządzeniem, a także usprawnienie i usystematyzowanie organizacji pracy Administratora.

Rozdział I
Postanowienia ogólne

§ 1

1. Fundacja Dajemy Dzieciom Siłę jest organizacją pozarządową o charakterze non-profit zajmującą się szeroko rozumianą pomocą dzieciom krzywdzonym, ich rodzinom i opiekunom. Pomoc tę realizuje się m. in. poprzez pomoc psychologiczną, prawną i medyczną indywidualnym klientom.
2. Fundacja Dajemy Dzieciom Siłę uznaje ochronę danych osobowych za istotne zagadnienie, wpisujące się w cele jej działania.

§ 2

1. Fundacja Dajemy Dzieciom Siłę jest administratorem danych osobowych (zwanym dalej „AD") - w rozumieniu ustawy o ochronie danych osobowych z dnia 29 sierpnia 1997 r., ustawy o ochronie danych osobowych z dnia 10 maja 2018 r. (zwanymi dalej „ustawami") oraz w zakresie Rozporządzenie Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (zwane dalej RODO).
2. Zarząd AD decyduje o celach i środkach przetwarzania danych osobowych będących w jego dyspozycji oraz o bezpieczeństwie tych danych.
3. Przez bezpieczeństwo danych osobowych rozumie się ochronę danych osobowych przetwarzanych przez AD przed nieuprawnionym ich przetwarzaniem, w szczególności przed dostępem osoby nieuprawnionej, zabraniem przez osobę nieuprawnioną, przetwarzaniem z naruszeniem przepisów oraz zmianą, utratą, uszkodzeniem lub zniszczeniem.
4. Bezpieczeństwo danych osobowych zapewniane jest z uwagi na obowiązujące przepisy, obowiązującą pracowników tajemnicę zawodową oraz z uwagi na przyjęte standardy pracy z klientem w AD.

5. W celu osiągnięcia i utrzymania wysokiego poziomu bezpieczeństwa danych osobowych w AD wprowadza się niniejszą Politykę bezpieczeństwa.
6. Polityka bezpieczeństwa ma zastosowanie do przetwarzania danych osobowych przez pracowników AD oraz osób świadczących mu usługi na podstawie umów cywilnoprawnych, w tym stażystów, wolontariuszy, praktykantów, o ile mają dostęp do tych danych.

§ 3

Ilekroć w niniejszym dokumencie jest mowa o:

1) Polityce bezpieczeństwa, dokumencie – należy przez to rozumieć „Politykę bezpieczeństwa danych osobowych w Fundacji Dajemy Dzieciom Siłę".

2) Fundacji – należy przez to rozumieć Fundację Dajemy Dzieciom Siłę.

3) Administratorze Danych (zwanym dalej „AD") - należy przez to rozumieć Fundację Dajemy Dzieciom Siłę.

4) Danych osobowych – należy przez to rozumieć informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej (zwanej dalej "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) Osobie możliwej do zidentyfikowania – należy przez to rozumieć osobę, której tożsamość można określić bezpośrednio lub pośrednio, w szczególności przez powołanie się na numer identyfikacyjny albo jeden lub kilka specyficznych czynników określających jej cechy fizyczne, fizjologiczne, umysłowe, ekonomiczne, kulturowe lub społeczne.

6) Zbiorze danych – należy przez to rozumieć uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

7) Pełnomocniku Zarządu ds. bezpieczeństwa danych (zwanego dalej „Pełnomocnikiem") – należy przez to rozumieć osobę wyznaczoną przez Zarząd AD do nadzorowania przestrzegania zasad ochrony danych osobowych.

8) Osobie upoważnionej – należy przez to rozumieć: pracownika, współpracownika, wolontariusza, praktykanta, stażystę AD posiadającego upoważnienie do przetwarzania danych osobowych nadane przez Pełnomocnika w imieniu AD.

9) Przetwarzaniu danych – oznacza operację 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.

10) Systemie informatycznym – należy przez to rozumieć zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych.

11) Zabezpieczeniu danych w systemie informatycznym – należy przez to rozumieć wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem.

12) Usuwaniu danych – należy przez to rozumieć zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą.
13) Anonimizacji danych – należy przez to rozumieć proces polegający na usunięciu wszystkich informacji, które w jakikolwiek sposób umożliwiają identyfikację określonej osoby, której dane dotyczą, przez administratora danych lub osobę trzecią. Zanonimizowane dane nie są już danymi osobowymi, ponieważ na ich podstawie nie jest możliwe zidentyfikowanie osoby, której dane zostały poddane temu procesowi.
14) Pseudoanonimizacji - należy przez to rozumieć przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
15) Zgodzie osoby, której dane dotyczą – należy przez to rozumieć dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
16) Zgodzie osoby powyżej 16 roku życia - należy przez to rozumieć oświadczenie woli, małoletniego, który ukończył 16 lat, którego treścią jest zgoda na przetwarzanie danych osobowych w zakresie płatnych usług społeczeństwa informacyjnego oferowanych bezpośrednio dziecku.
17) Odbiorcy danych - należy przez to rozumieć osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania.
18) Profilowaniu – należy przez to rozumieć dowolną formę zautomatyzowanego przetwarzania danych osobowych, która polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
19) Naruszeniu danych osobowych - należy przez to rozumieć każdy stwierdzony fakt nieuprawnionego ujawnienia danych, udostępnienia lub umożliwienia dostępu do nich osobom nieupoważnionym, zabrania danych przez osobę nieupoważnioną, uszkodzenia jakiegokolwiek elementu systemu informatycznego, a w szczególności:
- nieautoryzowany dostęp do danych,
- nieautoryzowane modyfikacje lub zniszczenie danych,
- udostępnienie danych nieautoryzowanym podmiotom,
- nielegalne ujawnienie danych,
- pozyskiwanie danych z nielegalnych źródeł.
20) Incydencie w zakresie danych osobowych – należy przez to rozumieć sytuację powodująca utratę poufności, integralności lub dostępności przetwarzanych danych.

Rozdział II
Struktura organizacyjna ochrony danych osobowych

§ 4

1. Administrator Danych jest odpowiedzialny za:

a. zapewnienie odpowiednich środków organizacyjnych i technicznych w celu zapewnienia i wykazania przetwarzania danych osobowych zgodnie z określonymi w RODO zasadami przetwarzania danych osobowych,
b. wdrożenie odpowiednich procedur ochrony danych osobowych,
c. jeśli uzna to za konieczne, stosowanie zatwierdzonych kodeksów postępowania lub zatwierdzonych mechanizmów certyfikacji, jako element dla stwierdzenia przestrzegania przez AD ciążących na nim obowiązków,
d. zapewnienie środków umożliwiających prawidłowa realizację praw osób, których dane dotyczą,
e. prowadzenie rejestru czynności przetwarzania danych osobowych,
f. prowadzenie rejestru kategorii przetwarzania dokonywanych w imieniu innego administratora,
g. współpracę z organem nadzorczym w ramach wykonywania przez niego swoich zadań,
h. wdrożenie odpowiednich środków organizacyjnych i technicznych, aby zapewnić stopień bezpieczeństwa odpowiadający istniejącemu ryzyku naruszenia praw lub wolności osób, których dane dotyczą,
i. zgłaszanie naruszenia ochrony danych osobowych właściwemu organowi nadzorczemu, a w przypadku, gdy zajdą ku temu odpowiednie przesłanki, również osobie, której dane dotyczą,
j. dokumentowanie wszelkich naruszeń ochrony danych osobowych, w tym okoliczności naruszenia, jego skutków oraz podjętych działań zaradczych,
k. zapewnienie odpowiednich środków w celu dokonania oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych w sytuacji, jeżeli dany rodzaj przetwarzania może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, w tym, jeżeli zajdą ku temu odpowiednie przesłanki, konsultację z organem nadzorczym,
l. nadawanie upoważnień do przetwarzania danych osobowych oraz prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych,
m. zapewnienie legalności przekazywania danych osobowych do podmiotów trzecich.

2. AD nadzoruje działania Pełnomocnika ds. bezpieczeństwa danych oraz Administratora Systemu Informatycznego oraz wydaje im zalecenia, co do sposobu wykonywania obowiązków wynikających z Polityki.
3. AD każdorazowo wyraża zgodę oraz ostateczną akceptację na kluczowe z perspektywy organizacji działania Pełnomocnika oraz AS, w które zaangażowane są podmioty trzecie. Do zaakceptowania tych działań, wystarczająca jest zgoda wyrażona w formie wiadomości e-mail.

§ 5

1. Zarząd AD wyznaczy pracownika do pełnienia funkcji Pełnomocnika Zarządu ds. bezpieczeństwa danych (zwanego dalej „Pełnomocnikiem"), wpisując mu w zakres obowiązków odpowiednie zadania.

2. Pełnomocnik jest wyznaczany przez AD na podstawie kwalifikacji zawodowych, w szczególności wiedzy fachowej na temat prawa i praktyki w dziedzinie ochrony danych oraz umiejętności wypełnienia swoich zadań.
3. Funkcję Pełnomocnika może sprawować inna osoba - wyznaczony przez Pełnomocnika i zatwierdzony przez AD zastępca. Liczba zastępców jest ustalana przez AD.

4. Zadaniami Pełnomocnika są:
n. reprezentowanie Zarządu w sprawach bezpieczeństwa danych osobowych w Fundacji,
o. informowanie o obowiązkach wynikających z RODO oraz innych właściwych przepisów Unii lub państw członkowskich o ochronie danych osobowych oraz doradzanie w tym zakresie,
p. sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych, przestrzegania procedur ochrony danych osobowych oraz opracowanie w tym zakresie sprawozdania dla AD
q. nadzorowanie opracowania i aktualizowania dokumentacji opisującej sposób przetwarzania danych oraz środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną, oraz przestrzegania zasad w niej określonych,
r. doradztwo w zakresie podziału obowiązków (np. między AD a podmiotem przetwarzającym lub pomiędzy pracownikami AD),
s. działania zwiększające świadomość pracowników AD w zakresie obowiązków wynikających z RODO lub przyjętych procedur, w tym szkolenia pracowników AD
t. prowadzenie rejestru zbiorów danych,
u. pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem danych,
v. pełnienie funkcji punktu kontaktowego dla osób, których dane dotyczą, we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

5. Swoje zadania Pełnomocnik wykonuje poprzez:
w. szkolenie pracowników ze stosowania zasad bezpieczeństwa danych osobowych,
x. stały monitoring stosowania zasad bezpieczeństwa danych osobowych poprzez nadzór nad pracownikami i współpracownikami oraz rozliczanie ich działań,
y. stały monitoring funkcjonowania środków organizacyjnych zapewniających bezpieczeństwo przetwarzanych danych osobowych,
z. przyjmowanie i reagowanie na sygnalizację problemów związanych ze stosowaniem Polityki bezpieczeństwa,
aa. dokonywanie stałej oceny zagrożeń dla bezpieczeństwa przetwarzanych danych i realizacja wniosków organizacyjnych i technicznych mających przeciwdziałać tym zagrożeniom,
bb. nadzór nad wykonywaniem zadań przez administratora systemu informatycznego.

6. Zadania wymienione w punkcie poprzedzającym Pełnomocnik realizuje we współpracy z Administratorem Systemu Informatycznego oraz z koordynatorami poszczególnych programów i działów AD.

§ 6

Administrator Systemu Informatycznego

1. Zarząd AD wyznaczy pracownika do pełnienia funkcji Administratora Systemu Informatycznego (zwanego dalej AS).
2. Zadaniem AS jest monitoring funkcjonowania środków technicznych dotyczących systemu informatycznego, służącego do przetwarzania danych osobowych w AD, w szczególności:

a. prowadzenie rejestru nadanych uprawnień do systemów informatycznych,
b. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,
c. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń,
d. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,
e. sprawowanie nadzoru nad kopiami zapasowymi,
f. inicjowanie i nadzór nad wdrażaniem nowych narzędzi, procedur organizacyjnych oraz sposobów zarządzania systemami informatycznymi, które mają doprowadzić do wzmocnienia bezpieczeństwa przy przetwarzaniu danych osobowych,
g. podejmowanie innych czynności w zakresie zabezpieczenia przetwarzania danych w systemach informatycznych,
h. dokonywanie cyklicznych przeglądów aktualności i stosowania procedur z zakresu przetwarzania danych w systemach informatycznych, na podstawie opracowanego planu przeglądów.
i. ścisła współpraca z Pełnomocnikiem w zakresie bezpieczeństwa i zasad przetwarzania danych osobowych w systemach informatycznych.

§ 7

Ocena skutków (analiza ryzyka)

1. Procedurę oceny skutków i przeprowadzenie analizy ryzyka wykonuje AS.
2. W celu dokonania analizy ryzyka wymagane jest zidentyfikowanie danych osobowych, które należy zabezpieczyć.
3. W ramach przeprowadzenia oceny skutków (analizy ryzyka) AS zobowiązany jest sprawdzić, czy AD spełnia wobec danych obowiązki prawne. Należy przede wszystkim zapewnić, że:

a. dane te są legalnie przetwarzane (na podstawie art. 6, 9 RODO),
b. dane te są adekwatne w stosunku do celów przetwarzania,
c. dane te są przetwarzane przez określony czas – zasada ograniczonego czasu,
d. wobec tych osób wykonano tzw. obowiązek informacyjny (art. 12, 13 i 14 RODO) wraz ze wskazaniem ich praw (np. prawa dostępu do danych, przenoszenia, sprostowania, usunięcia, ograniczenia przetwarzania, sprzeciwu, odwołania zgody),
e. opracowano klauzule informacyjne dla powyższych osób,
f. istnieją umowy powierzenia z podmiotami przetwarzającymi (art. 28 RODO).

§ 8

1. Procedura przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych jest adekwatna do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych. Analiza ryzyka powinna być dokonana na podstawie raportu oceny ryzyka.
2. Na podstawie analizy, AS tworzy plan postępowania z ryzykiem, w którym planuje obniżenie ryzyka, poprzez wyznaczenie listy zabezpieczeń do wdrożenia, terminu ich realizacji i osób odpowiedzialnych.
3. AD zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

Rozdział III
Środki organizacyjne i techniczne zapewniające ochronę danych osobowych

Dział 1.
Warunki i sposób przetwarzania danych osobowych

§ 9

1. AD dopuszcza do przetwarzania danych osobowych wyłącznie osoby posiadające imienne upoważnienie do przetwarzania danych osobowych. Fakt nadania upoważnienia podlega odnotowaniu w ewidencji.
2. Do wydawania upoważnień w imieniu AD uprawniony jest Pełnomocnik.
3. AD deleguje na Pełnomocnika prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych.
4. Wzór ewidencji określa załącznik nr 1.2 do niniejszej Polityki.
5. AD zapewnia, że każda osoba przed uzyskaniem upoważnienia do przetwarzania danych osobowych, zostanie przeszkolona z zakresu ochrony danych osobowych, na którym zapozna się m.in. z niniejszą Polityką. Szkolenie jest prowadzone w formie online.
6. AD zapewnia okresowe szkolenie (co najmniej raz w roku) i informowanie osób upoważnionych do przetwarzania danych osobowych o potencjalnych zagrożeniach oraz o formach i metodach zapewnienia bezpieczeństwa danych osobowych. Szkolenie może być prowadzone w formie stacjonarnej lub online.
7. Każda osoba, która uzyskała upoważnienie do przetwarzania danych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy oraz postanowieniami Polityki.
8. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia.
9. Naruszenie obowiązku ochrony danych osobowych, a w szczególności obowiązku zachowania danych osobowych w tajemnicy skutkuje poniesieniem odpowiedzialności karnej na podstawie przepisów Ustawy oraz stanowi ciężkie naruszenie obowiązków pracowniczych i może być podstawą rozwiązania stosunku pracy w trybie art. 52 Ustawy z dnia 26 czerwca 1974 r. Kodeks Pracy (t.j. Dz. U. z 2020 r. poz. 1320 z późn. zm.), bądź rozwiązania stosunku cywilnoprawnego.
10. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do przetwarzania danych osobowych wyłącznie w obszarze przetwarzania danych osobowych, z wyłączeniem Działu 4 niniejszej Polityki.

11. Przebywanie osób nieuprawnionych do przetwarzania danych w pomieszczeniu, w którym przetwarzane są dane osobowe jest dopuszczalne tylko w obecności osoby upoważnionej do ich przetwarzania, chyba, że dane te są w odpowiedni sposób zabezpieczone przed dostępem.
12. Pracownicy przechowujący dane osobowe zobowiązani są do zabezpieczenia materiałów zawierających dane w sposób uniemożliwiający dostęp do nich osobom nieuprawnionym.
13. Nie można udzielać informacji dotyczących danych osobowych innym podmiotom na podstawie prośby o takie dane skierowanej w formie zapytania telefonicznego.
14. Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych.
15. W czasie chwilowej nieobecności pracowników w pomieszczeniach, w godzinach pracy jak i po zakończeniu pracy, są oni zobowiązani do zamykania na klucz pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe.
16. Klucze do pomieszczeń, w których przetwarzane są dane osobowe nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia kluczy przed udostępnieniem ich osobom nieupoważnionym.
17. Przed wyjściem z pomieszczenia, w którym przechowywane są dane osobowe należy upewnić się, że zostało ono odpowiednio zabezpieczone (zamknięte okna, drzwi).

§ 10

Podstawowe zasady zabezpieczeń danych osobowych

1. Obszar przetwarzania danych osobowych w Warszawie, przy ul. Walecznych 59:

a. Lokal znajduje się pod stałym monitoringiem ochrony.
b. Wejście znajduje się za ogrodzeniem, lokal znajduje się na ostatnim piętrze budynku. Do budynku klucze mają pracownicy FDDS oraz pracownicy Ośrodka Pomocy Społecznej, który zajmuje niższe piętra. Klucze do placówki mają jedynie pracownicy FDDS. Furtka zamykana jest na noc i otwierana o 7:00 w dni powszednie od poniedziałku do piątku.
c. Kod do alarmu zmieniany jest co kwartał i podawany zainteresowanym ustnie przez sekretariat.
d. Placówka podzielona jest na część pracowniczą i ogólnodostępną. Do części pracowniczej można dostać się przechodząc za recepcją.
e. Zamykany na klucz jest pokój programu „Standardy Ochrony Dzieci" oraz „Działu Szkoleń i Edukacji". Klucz do pokoju jest w sekretariacie. Pozostałe pokoje, w których mogą znajdować się dane osobowe, są w części służbowej, która jest oddzielna od części ogólnodostępnej, za sekretariatem, z tabliczką, że jest to część zamknięta do postronnych.
f. Do pomieszczeń części pracowniczej mają dostęp bez dozoru wyłącznie pracownicy etatowi, współpracownicy (dyżury nocne, ew. realizatorzy projektów, wolontariusze psycholodzy, wolontariusze prawnicy, sprzątaczka).
g. W sekretariacie jest kontener zamykany na klucz, w którym przechowywane są formularze na warsztaty i zgłoszenia telefoniczne klientów w formie papierowej.
h. W pokojach pracowników poradniczych (psychologów) znajdują się szafy zamykane na klucz, w których są przechowywane dane papierowe, dokumentacja klientów; klucze do szaf znajdują się w szufladach pracowników. Takie szafy znajdują się także w części służbowej na korytarzu. Klucze do nich są w kontenerach pracowników, także zamykanych na klucz.

i. Pracownicy pracują na komputerach osobistych z dostępem do internetu, każdy ma swoje konto dostępowe.
j. W pokojach poradniczych dane przetwarzane są tylko w trakcie udzielania pomocy klientowi, nie są nigdy w nich pozostawiane bez nadzoru upoważnionego pracownika.

2. Obszar przetwarzania danych osobowych w Warszawie, przy ul. Mazowieckiej 12/25:

a. Budynek znajduje się pod stałym monitoringiem ochrony.
b. Wejście dla klientów i pracowników jest z klatki schodowej budynku. Do biura klucze mają pracownicy FDDS oraz pani sprzątająca biuro. Klucze zapasowe są w sekretariacie. Wejście jest otwierane kluczem lub pilotem przez pracowników będących w środku, nie ma podglądu kto jest przed drzwiami.
c. Kod do alarmu nie jest zmieniany. Podawany pracownikom ustnie.
d. Pokoje 1, 2, 3 mają drzwi zamykane na klucz, który przechowywany jest w sekretariacie.
e. W sekretariacie – pokoju nr 11 w szafie znajdują się segregatory z pocztą przychodzącą i wychodzącą. Dziennik korespondencji jest elektroniczny znajduje się na SP Biuro FDDS. Stosowana jest elektroniczna książka korespondencji na SP Sekretariaty.
f. Dane osobowe w formie papierowej znajdują się z pokojach 1, 2, 3, 7, 8 oraz 11 w zamkniętych na klucz szafach, kontenerkach w pozostałych miejscach dane są zbierane w formie elektronicznej.
g. Pracownicy pracują na komputerach osobistych z dostępem do internetu, każdy ma swoje konto dostępowe.
h. Serwer plików jest na korytarzu przy sekretariacie w zamykanej szafie serwerowej, metalowej, zamykanej na klucz, z dostępem tylko dla administratorów - Dział IT.

3. **Obszar przetwarzania danych osobowych w Warszawie, przy ul. Przybyszewskiego 20/24:**

a. Wnętrze budynku znajduje się pod stałym monitoringiem ochrony.
b. W budynku na partnerze prowadzony jest stały monitoring wizyjny.
c. Wejście dla klientów jest z prawej strony budynku, od ulicy, za ogrodzeniem z furtką i bramą. Do budynku (tylnego wejścia, nieogrodzonego) klucze mają pracownicy FDDS oraz pracownicy Orange Polska S.A. (jedynie na parter budynku). Klucze do wejścia dla klientów ma tylko sekretariat, wejście to otwierane z klucza jest tylko od wewnątrz, następnie poprzez przycisk na domofonie.
d. Kod do alarmu zmieniany jest co kwartał i podawany zainteresowanym ustnie przez sekretariat.
e. Placówka podzielona jest na część pracowniczą i ogólnodostępną. Do części pracowniczej można dostać się także z tyłu budynku przy użyciu klucza, a następnie kodu do wewnętrznej klatki schodowej.
f. Do pomieszczeń części pracowniczej mają dostęp bez dozoru wyłącznie pracownicy etatowi, współpracownicy (stali zleceniobiorcy, realizatorzy projektów, wolontariusze psycholodzy, wolontariusze prawnicy, sprzątaczka).
g. Wszystkie pokoje są zamykane na klucz. Klucze do pokoi są zamykane w skrzynce w pokoju nr 9 – sekretariacie oraz w pokoju nr 20. Klucz do sekretariatu znajduje się w szufladzie w biurku sekretarki przy recepcji.
h. W sekretariacie – pokoju nr 9 znajdują się szafy zamykane na klucz i sejf, w których przechowywane są dane osobowe klientów w formie papierowej, m.in. zeszyt zapisów.
i. W pokojach pracowników poradniczych (psychologów, prawników, konsultantów telefonów zaufania) znajdują się szafy zamykane na klucz, w których są przechowywane dane papierowe; klucze do szaf znajdują się w szufladach pracowników.
j. Pracownicy pracują na komputerach osobistych z dostępem do internetu, każdy ma swoje konto dostępowe.
k. Dane w postaci nagrań przesłuchań znajdują się na komputerze w pokoju nr 6 – pokoju przesłuchań przez 24 h od momentu zakończenia czynności. Następnie są trwale skasowane.

l. Serwer plików jest w serwerowni pokoju nr 21, w zamykanej szafie serwerowej, metalowej, zamykanej na klucz, z dostępem tylko dla administratorów - Dział IT.
m. W pokojach poradniczych dane przetwarzane są tylko w trakcie udzielania pomocy klientowi, nie są nigdy w nich pozostawiane bez nadzoru upoważnionego pracownika.

4. Obszar przetwarzania danych osobowych w Gdańsku, przy ul. Jana Uphagena 18

a. Centrum Pomocy Dzieciom w Gdańsku otwarte jest w godzinach 8 – 20. Poza godzinami otwarcia CPD aktywowany jest alarm. Na sygnał alarmu lub na wezwanie przyjeżdża mobilny patrol ochrony.
b. Wejście do pomieszczeń znajduje się pod stałym nadzorem pracowników dyżurujących w sali recepcyjnej (poczekalni) – pokój nr 2.
c. Okna pomieszczeń na parterze są wyposażone w szyby wzmocnione I zabezpieczone zamkami;
d. Placówka podzielona jest na część pracowniczą oraz ogólnodostępną
e. Do pomieszczeń części pracowniczej mają dostęp bez dozoru wyłącznie pracownicy etatowi, współpracownicy (stali zleceniobiorcy, dyżury nocne, ew. realizatorzy projektów, wolontariusze psycholodzy, wolontariusze prawnicy, sprzątaczka) oraz superwizorzy;
f. W pokoju cichej pracy psychologów (pokój nr 4) znajdują się szafy zamykane na klucz, w których przechowywane są dane osobowe klientów w formie papierowej: raporty zgłoszeń, karty klientów, dokumentacja RODO.
g. W pokojach do pracy z klientami dokumentacja nie jest przechowywana.
h. Pracownicy pracują na 2 komputerach znajdujących się sali recepcyjnej (poczekalni) – pokój nr 2 oraz na 2 komputerach znajdujących się pokoju koordynatora (pokój nr 5), a także na 2 komputerach znajdujących się w pokoju cichej pracy psychologów (pokój nr 4). Wszystkie komputery mają dostęp do Internetu.
i. Klucze do pomieszczeń przechowywane są w pokoju koordynatora (pokój nr 5).
j. Archiwum CPD w Gdańsku przechowywane jest w pokoju terapii – pokój nr 7.
k. W pokojach poradniczych dane przetwarzane są tylko w trakcie udzielania pomocy klientowi, nie są nigdy w nich pozostawiane bez nadzoru upoważnionego pracownika.

5. Obszar przetwarzania danych osobowych w Starogardzie Gdańskim, przy ul. Hallera 19a:

a. Budynek jest monitorowany przez całą dobę przez agencję ochrony Hera. W godzinach 7.00-21.00 od poniedziałku do piątku w recepcji obiektu przebywa pracownik administratora budynku.
b. Klucz do siedziby jest w recepcji obiektu w gablocie z kluczami, rano odbiera klucz pracownik sekretariatu i otwiera inne pomieszczenia. Pracownik OSiRu może zabrać klucz i wejść do pomieszczeń CPD w godzinach od 19:00-8:00 od poniedziałku do piątku i przez całą dobę w soboty i niedziele w sytuacjach szczególnych (zalanie obiektu, otwarte okna w pomieszczeniu).
c. Placówka CPD znajduje się na I i II piętrze. Piętro II to część główna- sekretariat oraz wyodrębniona część pracownicza. (pokój nr 7) .Wejście do pomieszczeń I pietra (gabinety do spotkań indywidualnych i grupowych, poczekalnia) zabezpieczone są czytnikiem elektronicznym- dostęp do tych pomieszczeń mają tylko pracownicy CPD (czipy lub wejście na kod)
d. Wszystkie pomieszczenia w części ogólnodostępnej za wyjątkiem toalet są zamykane na klucz. Klucze od pokoi znajdują się w sekretariacie w szufladzie zamykanej na klucz, do którego dostęp ma pracownik sekretariatu, a w razie jego nieobecności – koordynator placówki.
e. Pokój techniczny przesłuchań jest zawsze zamknięty na klucz, dostęp do pokoju ma pracownik sądu, klucz jest zabezpieczony w sekretariacie.
f. Dane w postaci nagrań przesłuchań znajdują się na komputerze w pokoju przesłuchań przez 24 h od momentu zakończenia czynności. Następnie są trwale skasowane.
g. W sekretariacie są szafy zamykane na klucz oraz szafa metalowa zamykana na klucz do przechowywania dokumentów CPD.

h. Pracownicy pracują na komputerach stacjonarnych, każdy z nich ma hasło dostępu. Wszystkie komputery mają dostęp do internetu.
i. W części pracowniczej znajdują się metalowe szafy, zamykane na klucz, znajdują się w nich dokumenty klientów. Klucze od szaf przechowywane są w sekretariacie w sejfie.
j. W pokojach terapeutycznych i prawnych dane są przetwarzane tylko w trakcie udzielania pomocy klientowi, nie są nigdy w nich pozostawione bez nadzoru.
k. Książka korespondencji prowadzona jest w wersji papierowej. Książka jest zabezpieczona w sekretariacie w metalowej szafie zamykanej na klucz

§ 11

Zbiory danych osobowych

1. AD prowadzi następujące zbiory danych osobowych:

a. Baza klientów FDDS – prowadzona w formie elektronicznej i papierowej, obejmująca placówki Centrów Pomocy Dziecku w Warszawie, Gdańsku i Starogardzie Gdańskim oraz Centrum Dziecka i Rodziny w Warszawie,
b. Baza klientów programów 800 100 100 i 116 111 - prowadzona w formie elektronicznej i papierowej,
c. Baza pracowników FDDS i współpracowników FDDS – prowadzona w formie elektronicznej i papierowej,
d. Baza podwykonawców – prowadzona w formie elektronicznej i papierowej,
e. Baza stażystów, wolontariuszy i praktykantów – prowadzona w formie elektronicznej i papierowej,
f. Baza dziennikarzy do działań PR – prowadzona w formie elektronicznej,
g. Baza danych darczyńców FDDS – prowadzona w formie elektronicznej i papierowej,
h. Baza „Chronimy Dzieci" – prowadzona w formie elektronicznej i papierowej,
i. Baza „Dziecko w Sieci" – prowadzona w formie elektronicznej,
j. Baza „Stypendium im. H. Gumprichta" – prowadzona w formie elektronicznej i papierowej,
k. Baza Uczestników akcji „List od Mikołaja" – prowadzona w formie elektronicznej,
l. Baza osób nominowanych i wygranych nagrody im. Aliny Margolis Edelman – prowadzona w formie elektronicznej,
m. Baza odbiorców newslettera – prowadzona w formie elektronicznej,
n. Baza uczestników szkoleń i innych wydarzeń edukacyjnych – prowadzona w formie elektronicznej i papierowej,
o. Baza danych osób biorących udział w przesłuchaniu w trybie 185a kpk - w formie papierowej,
p. Baza utrwalonych przesłuchań w trybie 185 a kpk – prowadzone w formie elektronicznej,
q. Baza „Książka korespondencji" w poszczególnych placówkach.

2. Bazy danych z punktów a, b w rejestrze przetwarzania danych są wpisane wspólnie.

§ 12

Zbieranie i przetwarzanie danych osobowych

1. Przetwarzanie danych osobowych odbywa się zgodnie z ogólnymi zasadami przetwarzania danych osobowych określonymi w art. 5 RODO. Oznacza to, że dane osobowe przetwarza się:

a. zgodnie z prawem, w oparciu o co najmniej jedną przesłankę legalności przetwarzania danych osobowych wskazaną w art. 6 lub 9 RODO (zasada legalności),
b. w sposób rzetelny przy uwzględnieniu interesów i rozsądnych oczekiwań osób, których dane dotyczą (zasada rzetelności),

c. w sposób przejrzysty dla osób, których dane dotyczą (zasada przejrzystości),
d. w konkretnych, wyraźnych i prawnie uzasadnionych celach (zasada ograniczenia celu),
e. w zakresie adekwatnym, stosownym oraz niezbędnym dla celów, w których są przetwarzane (zasada minimalizacji danych),
f. przy uwzględnieniu ich prawidłowości i ewentualnego uaktualniania (zasada prawidłowości),
g. przez okres nie dłuższy, niż jest to niezbędne dla celów, w których są przetwarzane (zasada ograniczenia przechowywania),
h. w sposób zapewniający odpowiednie bezpieczeństwo (integralność i poufność).

2. AD gwarantuje, że określone decyzje odnoszące się do procesów przetwarzania danych osobowych zostały przeanalizowane z punktu widzenia zgodności z ogólnymi zasadami przetwarzania danych, a przede wszystkim, że są z nimi zgodne.

§ 13

1. Dane osobowe są przetwarzane na różnych podstawach prawnych:
a. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
b. przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
c. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
d. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
e. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
f. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Dane klientów bezpośrednich AD i darczyńców są zbierane i przetwarzane na podstawie dobrowolnie wyrażonej zgody klienta, w tym zgody wyrażonej przez przystąpienie do programu pomocowego.
3. Inną podstawą prawną może być przetwarzanie danych niezbędne do wykonania wiążącej klienta z AD umowy lub do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora.
4. Dysponentem danych osobowych jest osoba, której dotyczą dane osobowe lub która ma prawo udzielać zgody na przetwarzanie danych osobowych osoby niepełnoletniej (rodzic/opiekun prawny dziecka).
5. Przy pierwszym kontakcie osoby z AD pracownik uzyskuje zgodę na przetwarzanie danych osobowych od dysponenta danych osobowych oraz zbiera dane, które są potrzebne do udzielenia pomocy/dalszego kontaktu.
6. Brak zgody dysponenta uniemożliwia udzielenie pomocy, chyba, że istnieje inna podstawa prawna do przetwarzania jej danych osobowych.
7. AD może podjąć decyzje o udzielaniu pomocy klientom bez przetwarzania ich danych osobowych (anonimowo). W wyjątkowych przypadkach możliwe jest udzielenie klientowi pomocy jednorazowej mimo braku zgody i innych podstaw prawnych do przetwarzania jego danych osobowych. W takim przypadku sporządzana jest notatka z konsultacji, która nie zawiera danych osobowych klienta.
8. U AD obowiązuje formularz zgody klienta na przetwarzanie danych osobowych, stanowiący załącznik nr 1.2 do Polityki.

§ 14

Zbieranie i przetwarzanie danych osobowych uczestników wydarzeń edukacyjnych

1. Dane uczestnika szkolenia/warsztatu organizowanego i prowadzonego przez AD (imię, nazwisko, telefon, e-mail, instytucja) zbierane są w trakcie szkolenia w formie listy obecności.
2. Obowiązuje jeden wzór listy obecności na szkoleniu/warsztacie.
3. We wzorze listy organizator/prowadzący szkolenia/warsztatu wypełnia nazwę szkolenia i datę jego przeprowadzenia.
4. W razie wątpliwości co do określenia celu przetwarzania danych, określonego w punkcie poprzedzającym, zalecana jest konsultacja z Pełnomocnikiem.
5. Listy gromadzone są w teczkach/segregatorach związanych z projektem, w ramach którego prowadzone jest szkolenie/warsztat, a następnie przekazywane koordynatorowi projektu, który przetwarza dane w nich zawarte w zakresie niezbędnym do realizacji i rozliczenia projektu, z zachowaniem zasad określonych w niniejszej polityce.

§ 15

Zbieranie danych osobowych za pomocą stron internetowych oraz korespondencji elektronicznej

1. Przez zbieranie danych osobowych za pomocą strony internetowej rozumie się każde zbieranie danych za pomocą strony internetowej poprzez umieszczone na niej formularze.
2. Przez zbieranie danych osobowych za pomocą korespondencji elektronicznej rozumie się także każde zbieranie danych poprzez odbiór od klienta korespondencji elektronicznej zawierającej te dane.
3. Zgody na przetwarzanie danych osobowych w celu korzystania z płatnych usług społeczeństwa informacyjnego mogą udzielać samodzielnie osoby, które ukończyły 16 rok życia.
4. Jeśli podstawą zbierania danych jest wyrażenie zgody, następuje ono przez aktywne zaznaczenie przez dysponenta danych opcji wyrażenia zgody na przetwarzanie danych osobowych umieszczonej pod formularzem z danymi. Opcja wyrażenia zgody na przetwarzanie danych nie może być na stronie automatycznie zaznaczona.
5. Przesłanie korespondencji elektronicznej do AD jest uznane za wyrażenie zgody na przetwarzanie danych osobowych klienta zawartych w treści tej korespondencji.

§ 16

Zbieranie danych osobowych
podczas udzielania konsultacji lub informacji telefonicznej

1. Pracownicy AD dokładają wszelkich starań, żeby podczas udzielania konsultacji lub informacji w kontakcie telefonicznym nie zbierać danych osobowych klienta.
2. W przypadku zbierania danych osobowych wymagana jest ustna zgoda klienta na przetwarzanie jego danych osobowych.
3. Na okoliczność uzyskania zgody w formie ustnej pracownik AD powinien sporządzić notatkę służbową.

4. W przypadku, gdy rozmówcą jest osoba niepełnoletnia, dane osobowe nie mogą być zbierane, za wyjątkiem pomocy psychologicznej świadczonej w ramach programu 116 111. W przypadku tego programu dane zbierane są w ograniczonym zakresie, umożliwiającym odnotowanie konsultacji i jej przebiegu na potrzeby przyszłego kontaktu z dzieckiem (adres email, historia konwersacji), celem ochrony lub sprawdzenia jego psychofizycznego dobrostanu. Powyższe zasady, w tym ograniczenie zakresu przetwarzania danych nie dotyczą sytuacji określonych w § 18.

§ 17

Zbieranie danych podczas zapisów klientów na konsultacje

1. W przypadku zapisu klienta na pierwszą konsultacje pracownik sekretariatu AD zapisuje podane w kontakcie telefonicznym dane osobowe klienta w Karcie Klienta.
2. W zapisie na kolejne konsultacje podawane są dane osobowe w postaci imienia, nazwiska i numeru telefonu pełnoletniego opiekuna/rodzica dziecka lub dziecka.
3. Zapisu dokonuje się poprzez wpis do bazy danych klientów FDDS, prowadzonej w formie papierowej lub w formie elektronicznej.

§ 18

Wyłączenie konieczności uzyskania zgody

1. W przypadku, gdy istnieje podejrzenie zagrożenia dobra osoby niepełnoletniej (dziecka) lub podejrzenie popełnienia przestępstwa, dane osobowe klienta, w tym osoby niepełnoletniej, mogą być zbierane – w celu i w zakresie umożliwiającym podjęcie interwencji. W takim wypadku nie jest wymagane wyrażenie przez klienta zgody na przetwarzanie danych osobowych, gdyż przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej (art. 6 ust. 1 pkt. d RODO).
2. Brak zgody lub sprzeciw wobec przetwarzania danych dziecka w przypadku konfliktu między przedstawicielami ustawowymi/opiekunami prawnymi osoby niepełnoletniej nie tamuje działań w celu udzielenia niezbędnej pomocy. W takim wypadku dane dziecka są zanonimizowane.
3. Zapis niniejszego paragrafu ma zastosowanie do zbierania danych osobowych w każdy sposób, w tym – w kontakcie bezpośrednim i telefonicznym.

Dział 2.
Środki ochrony i prowadzenia zbiorów danych osobowych w formie papierowej

§ 19

1. Wszystkie dane osobowe oraz inne informacje dotyczące klienta AD, przetwarzane w formie papierowej (w tym dokumenty, opinie) znajdują się w jego dokumentacji.
2. W dokumentacji przechowuje się także zgodę klienta na przetwarzanie danych osobowych. Jeżeli zgoda przechowywana jest w dokumentacji klienta prowadzonej przez innego pracownika AD, należy w dokumentacji powołać się na tę zgodę.
3. W dokumentacji klienta umieszcza się wyłącznie kserokopie przedstawianych przez niego dokumentów. Oryginały dokumentów oddawane są klientowi. Decyzja o umieszczeniu w dokumentacji wytworów dziecka należy do terapeuty AD.

§ 20

1. Dane osobowe i informacje dotyczące klienta przechowywane są w tekturowych teczkach lub segregatorach.
2. Wszystkie teczki i segregatory przechowywane są w zamykanych na klucz szafach, które znajdują się wyłącznie w obszarach chronionych.
3. Klucze do ww. szaf oraz obszarów chronionych w czasie godzin pracy AD pozostają w dyspozycji pracowników upoważnionych do przetwarzania danych osobowych. Po godzinach pracy klucze deponowane są w szafce/kasetce na klucze.
4. Kopie zapasowe, jeśli istnieją oraz archiwalne zbiorów danych osobowych przechowywane są w zamkniętych niemetalowych szafach lub pomieszczeniach archiwum niedostępnych dla osób postronnych.
5. Pomieszczenia, w których przetwarzane są zbiory danych osobowych zabezpieczone jest przed skutkami pożaru za pomocą systemu przeciwpożarowego lub wolnostojącej gaśnicy.
6. Dokumenty zawierające dane osobowe po ustaniu przydatności oraz brudnopisy, błędne lub zbędne kopie materiałów są niszczone w sposób mechaniczny, za pomocą niszczarek dokumentów. Zniszczenie powinno nastąpić w sposób, który uniemożliwia odczytanie danych osobowych z tych dokumentów.
7. W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. *czystego biurka*, która oznacza niepozostawianie materiałów zawierających dane osobowe w miejscu umożliwiającym fizyczny dostęp do nich osobom nieuprawnionym. Za realizację powyższej zasady odpowiedzialny jest na swym stanowisku każdy z pracowników. Nie należy pozostawiać danych osobowych w miejscach ogólnodostępnych takich jak np. biurka, blaty, parapety, drukarki.

Dział 3.
Środki ochrony i prowadzenia zbiorów danych osobowych w formie elektronicznej

§ 21

1. Dostęp do zbiorów danych osobowych w formie elektronicznej możliwy jest ze stacji roboczych (komputerów) umieszczonych w obszarze przetwarzania danych, za wyjątkiem określonym w pkt 8 niniejszego paragrafu oraz na zasadach opisanych w §23 i §24 Polityki.
2. Dostęp do wymienionych w punkcie poprzedzającym stacji roboczych mają wyłącznie osoby posiadające upoważnienie do przetwarzania danych osobowych. Dostęp do stacji roboczych możliwy jest wyłącznie po wprowadzeniu identyfikatora i hasła.
3. Monitory stacji roboczych z dostępem do zbiorów danych osobowych są ustawione w taki sposób, by uniemożliwić wgląd w dane osobom nieuprawnionym.
4. Nikomu nie należy udostępniać indywidualnych haseł i identyfikatorów do systemów informatycznych.

5. Po zakończeniu pracy w systemie informatycznym, w którym przechowywane są dane osobowe, należy wylogować się z systemu.
6. Wysyłanie seryjnych wiadomości e-mail (do więcej niż jednego adresata) do więcej niż jednego adresata wymaga zastosowania opcji *kopia ukryta*.
7. Dane osobowe wrażliwe przesyłane elektronicznie powinny być zabezpieczone hasłem. Hasło to powinno być wysyłane oddzielnym kanałem telekomunikacyjnym.
8. Komputery przenośne (laptopy) z dostępem do zbiorów danych mogą być przenoszone poza obszary chronione wyłącznie przez osoby posiadające upoważnienie do przetwarzania danych osobowych w sposób zabezpieczający je przed nieuprawnionym dostępem, w szczególności poprzez unikanie pozostawiania komputera przenośnego bez nadzoru osoby upoważnionej. Wobec danych osobowych przetwarzanych na komputerach przenośnych przenoszonych poza obszary chronione stosuje się środki ochrony kryptograficznej (szyfrowanie). Osoba użytkująca komputer przenośny zawierający dane osobowe zobowiązana jest do zachowania szczególnej ostrożności podczas jego transportu, przechowywania i użytkowania poza obszarem, w którym przetwarzane są dane osobowe.
9. Osoba upoważniona do przetwarzania danych w przypadku zakończenia pracy/współpracy u AD obowiązana jest do niezwłocznego zwrotu posiadanego sprzętu (komputery przenośne/nośniki danych), nie później niż ostatniego dnia pracy/współpracy. Także dniem zakończenia pracy/współpracy (nie później niż do godziny 16) Administrator Systemu Informatycznego blokuje tej osobie dostęp do systemów informatycznych AD.

§ 22

1. Do obsługi zbiorów danych w formie elektronicznej używane są programy wchodzące w skład pakietu biurowego oraz aplikacja do obsługi klientów indywidualnych, przyjęta w danej placówce.
2. Stacje robocze z dostępem do zbiorów danych osobowych połączone są z siecią publiczną.
3. Przepływ danych między serwerem a stacjami roboczymi ma charakter dwukierunkowy. Dane osobowe przesyłane są z serwera na stacje robocze przy użyciu kryptograficznych środków ochrony (szyfrowania).

Dział 4.
Praca zdalna z danymi osobowymi

§ 23

1. W przypadkach uzasadnionych organizacją pracy przyjętą przez AD osoba upoważniona do przetwarzania danych osobowych może pracować zdalnie na danych osobowych.
2. Miejscem przetwarzania danych osobowych może być miejsce zamieszkania osoby upoważnionej do przetwarzania danych osobowych lub inne miejsce, z którego łączy się jego prywatny komputer lub urządzenie mobilne.
3. Na osobie upoważnionej do przetwarzania danych osobowych, pracującej zdalnie spoczywa obowiązek odpowiedniego zabezpieczenia danych tak, aby osoby trzecie nie miały dostępu do danych osobowych.
4. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do zabezpieczenia danych przed nieuprawnionym dostępem, w szczególności poprzez stosowanie się do Podstawowych

zasad bezpieczeństwa IT i w razie wątpliwości lub braku wiedzy zgłaszanie się do działu IT, celem otrzymania technicznego wsparcia.

5. Osoba upoważniona do przetwarzania danych jest zobowiązana do zapoznania się z zasadami bezpiecznego przetwarzania danych przy użyciu urządzeń teleinformatycznych oraz sieci Internet. W przypadku wątpliwości lub braku wiedzy, co do sposobu zabezpieczenia danych przed nieuprawnionym dostępem osoba upoważniona do przetwarzania danych zobowiązana jest do kontaktu z AS celem wyjaśnienia wątpliwości i uzupełnienia potrzebnej wiedzy.
6. Praca zdalna z danymi osobowymi odbywa się wyłącznie za pomocą oprogramowania zapewniającego zdalny dostęp (dane w chmurze). Niedopuszczalnym jest wynoszenie danych osobowych zapisanych na nośnikach danych (pendrive, płyta CD i podobne).
7. Niedopuszczalnym jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

§ 24

1. Korzystanie z prywatnych urządzeń wymaga posiadania w nich oddzielnego konta użytkownika, zabezpieczonego hasłem, niedostępnym dla osób nieupoważnionych.
2. Dane osobowe przetwarzane elektronicznie muszą być jedynie poprzez kanały służbowe: e-mail służbowy, platformę służbową do kontaktów wewnętrznych, bazy danych.
3. Osoba upoważniona do przetwarzania danych osobowych jest zobowiązana do stosowania wszelkich zabezpieczeń sprzętu prywatnego, na którym dane są przetwarzane, rekomendowanych przez ASI.

§ 25

W przypadku zdarzenia zagrażającego lub naruszającego ochronę danych osobowych, pracownik obowiązany jest zastosować procedury zawarte w Rozdziale VI.

Rozdział IV
Udostępnianie danych osobowych

§ 26

1. Dane udostępnia się wyłącznie osobom, których dane dotyczą oraz uprawnionym na podstawie przepisów ustawy organom i instytucjom, w szczególności sądom i prokuraturom.
2. Udostępnienie danych organom i instytucjom następuje tylko w oparciu o co najmniej jedną przesłankę spośród wskazanych w art. 6 RODO lub art. 9 RODO.
3. Udostępnienie danych osobie, której dane dotyczą następuje na wniosek tej osoby. Wniosek nie wymaga uzasadnienia.
4. Udostępnienie danych osobie, której dane dotyczą następuje w sposób uniemożliwiający zapoznanie się tej osoby z danymi innych osób. W szczególności udostępnienie może nastąpić w formie doręczenia wydruku danych dotyczących tej osoby z bazy danych klientów FDDS.
5. Osoba, której dane dotyczą, po udostępnieniu jej danych, ma prawo zażądać poprawienia danych przetwarzanych przez AD.

6. Fakt udostępnienia danych podmiotom wymienionym w ustępie 1 niniejszego paragrafu jest odnotowywany we właściwym zbiorze danych – w dokumentacji osoby, której dane dotyczą.
7. Przekazywanie danych, których administratorem jest Administrator Danych do państw trzecich i organizacji międzynarodowych, może się odbywać wyłącznie po spełnieniu warunków przewidzianych w Rozdziale V RODO.

§ 27

AD uwzględnia procedury i zasady ułatwiające osobie, której dane dotyczą, wykonywanie praw przysługujących jej na mocy przepisów RODO, w szczególności:

a. prawo do wycofania wyrażonej zgody (art. 7 ust. 3 RODO),
b. prawo dostępu przysługujące osobie, której dane dotyczą (art. 15 RODO),
c. prawo do sprostowania danych (art. 16 RODO),
d. prawo do usunięcia danych (*prawo do bycia zapomnianym*) (art. 17 RODO),
e. prawo do ograniczenia przetwarzania (art. 18 RODO),
f. prawo do przenoszenia danych (art. 20 RODO),
g. prawo sprzeciwu (art. 21 RODO),
h. prawo do niepodlegania decyzjom opartym na zautomatyzowanym przetwarzaniu (art. 22 RODO).

§ 28

1. Dane osobowe klientów Fundacji są przetwarzane przez okres zgodny z celem ich przetwarzania - nie dłużej jednak niż przez okres 5 lat od ostatniego kontaktu z klientem. W szczególnych wypadkach, gdy wymaga tego grantodawca lub przepisy prawa, dane osobowe mogą być przetwarzane dłużej. Dane w bazie elektronicznej przechowywane są przez okres wymagany przez grantodawcę dla celów rozliczeniowych, nie dłużej niż 5 lat po tym okresie.
2. Dane osobowe pracowników Fundacji oraz osób świadczących usługi na podstawie umów cywilnoprawnych, w tym wolontariuszy, przetwarzane są przez okres określony w odrębnych przepisach, w szczególności prawa pracy, prawa cywilnego.
3. Po upływie okresu, o którym mowa w punktach poprzedzających, dane osobowe są usuwane lub zanonimizowane. Zachowaniu podlegają dokumenty zgody na przetwarzanie danych osobowych.
4. Osobą odpowiedzialną za przygotowanie i selekcję dokumentów/nośników/rekordów, zawierających dane osobowe przeznaczone do usunięcia jest koordynator działu we współpracy z Pełnomocnikiem.
5. Selekcji dokonuje się w pierwszym kwartale roku następnego po roku, w którym wygasa okres ich przechowywania.
6. Usunięcia danych wyselekcjonowanych zgodnie z procedurą opisaną w punktach poprzedzających dokonuje komisja składająca się z co najmniej dwóch osób wskazanych przez Zarząd Fundacji. W przypadku usunięcia rekordu w elektronicznym zbiorze danych, usunięcia danych dokonuje Administrator Systemu Informatycznego, w porozumieniu z osobą prowadzącą sprawę danego klienta.
7. Z usunięcia danych sporządza się protokół, którego wzór stanowi załącznik nr 1.3 do Polityki.
8. Usunięcia danych może dokonać firma zewnętrzna wybrana przez Zarząd Fundacji.

Rozdział V
Powierzenie danych osobowych

§ 29

1. AD dopuszcza, by dane osobowe, których jest administratorem były przetwarzane poza własnymi strukturami organizacyjnymi. Może się to odbywać wyłącznie na drodze powierzenia danych, w określonym celu i zakresie, podmiotowi przetwarzającemu na mocy umowy powierzenia przetwarzania danych osobowych lub innego instrumentu prawnego.
2. Podstawowym warunkiem dopuszczalności powierzenia przetwarzania danych w imieniu administratora jest poddanie planowanego outsourcingu analizie, która powinna zapewnić, że wybór podmiotu przetwarzającego został uzależniony od zapewnienia wystarczających gwarancji ochrony danych.
3. Zawierana przez AD umowa powierzenia przetwarzania danych osobowych musi być zgodna z postanowieniami art. 28 RODO, tj. w szczególności określać:

a. przedmiot powierzenia,
b. czas trwania powierzenia,
c. charakter i cel przetwarzania,
d. rodzaj powierzanych danych osobowych,
e. kategorie osób, których dane dotyczą,
f. warunki podpowierzenia przetwarzania danych
g. obowiązki i prawa Administratora Danych,
h. obowiązki podmiotu przetwarzającego.

4. Umowa powierzenia może zostać zawarta w formie pisemnej, w tym elektronicznej.
5. W przypadku, gdy elementy powierzenia przetwarzania danych wskazane w ustępie 3 znajdują się już w zawartej z danym podmiotem umowie, nie ma konieczności sporządzania dodatkowej umowy powierzenia przetwarzania danych osobowych.
6. Za zawieranie umów powierzenia przetwarzania danych osobowych odpowiadają koordynatorzy działań.
7. Koordynatorzy przed planowanym rozpoczęciem współpracy z podmiotem przetwarzającym, są zobowiązani poinformować o tym Pełnomocnika oraz skonsultować z nim postanowienia zawieranej umowy w zakresie powierzenia przetwarzania danych osobowych. Powierzenie przetwarzania danych może odbyć się wyłącznie na podstawie postanowień zaakceptowanych przez Pełnomocnika.
8. Umowa powierzenia przetwarzania danych osobowych podpisywana jest zgodnie z zasadami reprezentacji AD lub udzielonymi pełnomocnictwami.
9. AD ma prawo kontroli podmiotów przetwarzających, którym powierzył przetwarzanie danych osobowych.
10. AD w zakresie prowadzonej przez siebie działalności może przetwarzać również dane osobowe powierzone przez podmioty, na rzecz których świadczy usługi. Przyjęcie danych w powierzenie przez AD musi zostać obligatoryjnie odnotowane w rejestrze kategorii czynności przetwarzania danych osobowych.

Rozdział VI

Postępowanie w sytuacji zagrożenia lub naruszenia ochrony danych osobowych

§ 30
Zagrożenie naruszenia danych osobowych – procedura

1. Zagrożeniem bezpieczeństwa informacji jest sytuacja, w której występuje zagrożenie zaistnienia naruszenia danych osobowych. Zagrożeniem są m.in.:

a. nieprzestrzeganie Polityki przez osoby przetwarzające dane, np. niezamykanie pomieszczeń, szaf, biurek, brak stosowania zasad ochrony haseł,
b. niewłaściwe zabezpieczenie fizyczne dokumentów, urządzeń lub pomieszczeń,
c. niewłaściwe zabezpieczenie oprogramowania lub sprzętu IT przed wyciekiem, kradzieżą lub utratą danych osobowych.

2. W przypadku stwierdzenia wystąpienia zagrożenia każdy pracownik jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu oraz powstrzymać się od pracy lub innych działań mogących zatrzeć dowody naruszenia. W razie konieczności zobowiązany jest także podjąć, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych.
3. Przełożony zgłasza to Pełnomocnikowi Zarządu, który we współpracy z AS:

a. ustala zakres i przyczyny zagrożenia oraz jego ewentualnych skutków,
b. w miarę możliwości przywrócenie stanu zgodnego z zasadami ochrony danych osobowych,
c. w razie konieczności zainicjowanie działań dyscyplinarnych,
d. zarekomendowanie działań zapobiegawczych w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
e. udokumentowanie prowadzonego postępowania w rejestrze naruszeń bezpieczeństwa.

§ 31
Incydent – procedura

1. Incydentem jest sytuacja naruszenia bezpieczeństwa informacji ze względu na dostępność, integralność i poufność. Incydenty powinny być wykrywane, rejestrowane i monitorowane w celu zapobieżenia ich ponownemu wystąpieniu. Incydentem są m.in.:

a. losowe zdarzenie wewnętrzne, np. awaria komputera, serwera, twardego dysku, błąd użytkownika, informatyka, zgubienie danych,
b. losowe zdarzenie zewnętrzne, np. klęski żywiołowe, zalanie, awaria zasilania, pożar,
c. incydent umyślny, np. wyciek informacji, ujawnienie danych nieupoważnionym osobom, świadome zniszczenie danych, działanie wirusów komputerowych, włamanie do pomieszczeń lub systemu informatycznego (wewnętrzne i zewnętrzne).

2. W przypadku stwierdzenia wystąpienia incydentu każdy pracownik jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu oraz powstrzymać się od pracy lub innych działań mogących zatrzeć dowody incydentu. W razie konieczności zobowiązany jest także podjąć, stosownie do zaistniałej sytuacji, wszelkie niezbędne działania celem zapobieżenia dalszym zagrożeniom, które mogą skutkować utratą danych osobowych..
3. Przełożony zgłasza to Pełnomocnikowi Zarządu, który we współpracy z AS:

a. ustala czas zdarzenia będącego incydentem,
b. ustala zakres incydentu,
c. określa przyczyny, skutki oraz szacuje zaistniałe szkody,
d. zabezpiecza dowody,
e. ustala osoby odpowiedzialne za naruszenie,
f. usuwa skutki incydentu,
g. ogranicza szkody wywołane incydentem,
h. inicjuje działania dyscyplinarne,
i. rekomenduje działania zapobiegawcze w kierunku wyeliminowania podobnych zagrożeń w przyszłości,
j. dokumentuje prowadzenie postępowania w rejestrze naruszeń.

§ 32

Naruszenie danych osobowych – procedura

1. Każdy pracownik, który stwierdzi lub podejrzewa fakt naruszenia danych osobowych, jest zobowiązany niezwłocznie zgłosić to swojemu bezpośredniemu przełożonemu. Przełożony zgłasza to Pełnomocnikowi Zarządu.
2. Typowe sytuacje, gdy użytkownik powinien powiadomić przełożonego:
a. ślady na drzwiach, oknach i szafach wskazują na próbę włamania;
b. dokumentacja jest niszczona bez użycia niszczarki;
c. fizyczna obecność w budynku lub pomieszczeniach osób zachowujących się podejrzanie;
d. otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe, stwierdzone nieprawidłowości w zakresie zabezpieczenia miejsc przechowywania informacji (otwarte szafy, biurka, regały, urządzenia archiwalne i inne) na nośnikach tradycyjnych tj. na papierze (wydrukach), kliszy, folii, zdjęciach, płytach CD w formie niezabezpieczonej itp.;
e. nie wylogowanie się przed opuszczeniem stanowiska pracy, pozostawienie danych w drukarce, na ksero, nie zamknięcie pomieszczenia z komputerem, nie wykonanie w określonym terminie kopii bezpieczeństwa, prace na informacjach służbowych w celach prywatnych;
f. ustawienie monitorów pozwala na wgląd osób postronnych w dane osobowe;
g. wynoszenie danych osobowych w wersji papierowej lub elektronicznej na zewnątrz firmy bez upoważnienia;
h. udostępnienie danych osobowych osobom nieupoważnionym w formie papierowej, elektronicznej lub ustnej;
i. stwierdzono próbę lub modyfikację danych lub zmianę w strukturze danych bez odpowiedniego upoważnienia (autoryzacji);
j. telefoniczne próby wyłudzenia danych osobowych;
k. kradzież komputerów lub twardych dysków z danymi osobowymi;
l. utrata kontroli nad kopią danych osobowych;
m. maile zachęcające do ujawnienia identyfikatora i/lub hasła;
n. pojawienie się wirusa komputerowego lub niestandardowe zachowanie komputerów;
o. istnienie nieautoryzowanych kont dostępu do danych lub tzw. "bocznej furtki";
p. hasła do systemów przechowywane są w pobliżu komputera.

§ 33

Każdy pracownik, który stwierdzi fakt naruszenia danych osobowych ma obowiązek podjąć czynności niezbędne do powstrzymania skutków naruszenia ochrony oraz zabezpieczyć dowody umożliwiające ustalenie przyczyn oraz skutków naruszenia.

§ 34

W przypadku stwierdzenia naruszenia bezpieczeństwa danych należy zaniechać wszelkich działań mogących utrudnić analizę wystąpienia naruszenia i udokumentowanie zdarzenia oraz nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Pełnomocnika Zarządu lub innej osoby upoważnionej przez AD.

§ 35

AS jest zobowiązany do informowania Pełnomocnika o wszelkich anomaliach w pracy administrowanych przez siebie urządzeń, mogących być przyczyną lub skutkiem incydentu w zakresie danych osobowych.

§ 36

1. Pełnomocnik Zarządu podejmuje następujące kroki:

a. zapoznaje się z zaistniałą sytuacją i wybiera sposób dalszego postępowania uwzględniając zagrożenie w prawidłowości i ciągłości pracy,
b. odbiera dokładną relację z zaistniałego naruszenia bezpieczeństwa danych od osoby powiadamiającej, jak również od każdej innej osoby, która może posiadać informacje w związku z zaistniałym naruszeniem,
c. nawiązuje kontakt ze specjalistami zewnętrznymi (jeśli zachodzi taka potrzeba).

2. Pełnomocnik Zarządu dokumentuje zaistniały przypadek naruszenia bezpieczeństwa danych sporządzając raport - załącznik nr 4.5 do Polityki i przedstawia go Zarządowi. Raporty są przechowywane przez Pełnomocnika Zarządu przez okres 5 lat.
3. Pełnomocnik Zarządu zasięga potrzebnych mu opinii i proponuje działania naprawcze (w tym także ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń oraz terminu wznowienia przetwarzania danych osobowych) - załącznik nr 4.6 do Polityki - rejestr incydentów i działań korygujących i zapobiegawczych.

§ 37

Naruszenie danych osobowych – odpowiedzialność

1. Wobec osoby, która w przypadku naruszenia danych osobowych nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami wszczyna się postępowanie dyscyplinarne lub porządkowe.
2. Przypadki nieuzasadnionego zaniechania obowiązków wynikających z niniejszego dokumentu mogą być potraktowane jako ciężkie naruszenie obowiązków pracowniczych. Kara dyscyplinarna, wobec osoby uchylającej się od powiadomienia o naruszeniu danych osobowych nie wyklucza odpowiedzialności karnej tej osoby zgodnie z aktualnie obowiązującym przepisami oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.

§ 38

Zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu

1. W przypadku naruszenia ochrony danych osobowych, administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Urzędowi ochrony danych, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia. Wzór zgłoszenia – załącznik nr 4.7 do Polityki
2. Zgłoszenie, o którym mowa w ust. 1, musi co najmniej:

a. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
b. zawierać imię i nazwisko oraz dane kontaktowe inspektora Pełnomocnika lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
c. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
d. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

3. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.
4. Administrator dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić organowi nadzorczemu weryfikowanie przestrzegania niniejszego artykułu.

§ 39

Zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu.
2. Zawiadomienie, o którym mowa w ust. 1 niniejszego artykułu, jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w paragrafie poprzedzającym, ust. 2 lit. b, c i d.
3. Zawiadomienie, o którym mowa w ust. 1, nie jest wymagane, w następujących przypadkach:

a. administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
b. administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą, o którym mowa w ust. 1;

c. wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

Rozdział VII
Postanowienia końcowe
§ 40

1. Polityka wchodzi w życie z dniem ogłoszenia.
2. Ogłoszenie następuje w sposób dostępny dla pracowników AD oraz osób świadczących mu usługi na podstawie umów cywilnoprawnych, w tym stażystów, wolontariuszy, praktykantów, w szczególności poprzez przesłanie jej tekstu drogą elektroniczną.
3. Załączniki do Polityki stanowią jej integralną część.
4. Za wdrożenie Polityki odpowiedzialny jest zarząd Fundacji.
5. Polityka jest dokumentem wewnętrznym i jest objęta obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona.
6. Do spraw nieuregulowanych w Polityce stosuje się przepisy prawa powszechnie obowiązującego, w szczególności RODO oraz ustaw.

§ 41

1. Zarząd dokonuje okresowego, nie rzadziej niż raz do roku, przeglądu Polityki bezpieczeństwa i w razie konieczności dokonuje niezbędnych zmian w polityce.
2. Przegląd powinien obejmować, w szczególności ocenę adekwatności Polityki do:
a. procesów funkcjonujących w strukturach AD,
b. obowiązujących przepisów prawa odnoszących się do ochrony danych osobowych, którym podlega AD.

3. W każdym przypadku, gdy zmianie ulegają przepisy prawa będące źródłem wskazanych w Polityce obowiązków lub zaistnieją istotne zmiany faktyczne w ramach struktury AD, przegląd Polityki wykonywany jest niezwłocznie.
4. Jeżeli w wyniku przeglądu Polityki stwierdzona zostanie konieczność aktualizacji jej zapisów, Zarząd dokonuje aktualizacji Polityki w wymaganym zakresie.
5. Zmiany ogłaszane są w sposób określony w § 40 pkt 2.

Załączniki:

1.1. Wzór ewidencji upoważnień
1.2. Wzór ogólny zgody klienta na przetwarzanie danych osobowych
1.2 Wzór protokołu zniszczenia akt
1.3 Wzór raportu z naruszenia ochrony danych
1.4 Wzór rejestru incydentów bezpieczeństwa i działań korygujących i zapobiegawczych
1.5 Wzór zgłoszenia naruszenia ochrony danych osobowych organowi nadzorczemu

Załącznik 1.1 Wzór ewidencji osób upoważnionych do przetwarzania danych

Ewidencja osób upoważnionych do przetwarzania danych osobowych

w Fundacji Dajemy Dzieciom Siłę

Lp	Imię i nazwisko	Data nadania upoważnienia	Data ustania upoważnienia	Zakres upoważnienia			Login / Identyfikator	Uwagi
				Stanowisko służbowe	Dostęp do oprogramowania (nazwy systemów / zbiorów, do których użytkownik ma dostęp)	Dostęp do zbiorów danych		
1.								
2.								
3.								
4.								
5.								
6.								

Załącznik 1.2 Wzór ogólny zgody na przetwarzanie danych osobowych klienta

Warszawa, dnia……

Ja……wyrażam zgodę na przetwarzanie moich danych osobowych oraz jako przedstawiciel ustawowy małoletniej/go ……wyrażam zgodę na przetwarzanie danych osobowych mojego dziecka przez Fundację Dajemy Dzieciom Siłę, z siedzibą przy ul. Walecznych 59, 03-926 Warszawa w celu udzielenia pomocy interdyscyplinarnej (psychologicznej, prawnej, medycznej, socjalnej) oraz interwencji w Centrum Pomocy Dzieciom FDDS/Centrum Dziecka i Rodziny FDDS.

……

podpis

Załącznik 1.3 Wzór protokołu zniszczenia akt

Wzór protokołu:

Protokół zniszczenia akt		
ID klienta/opis danych	Data zakończenia sprawy	Data zniszczenia

Podpisy komisji

.....

Data sporządzenia protokołu

.....

Załącznik nr 1.4 Wzór raportu z naruszenia ochrony danych

Raport z naruszenia ochrony danych

Data …… Godzina ……

1. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe,):
……

2. Lokalizacja zdarzenia (nr. pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
……

3. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu:
……

4. Podjęte działania:
……

5. Wstępna ocena przyczyn wystąpienia naruszenia:
……

6. Postępowanie wyjaśniające i naprawcze:
……

…… ……

(podpis pracownika) (data i podpis Pełnomocnika Zarządu)

Załącznik nr 1.5 Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych

Rejestr incydentów bezpieczeństwa i działań korygujących i zapobiegawczych								
Zadanie / problem / incydent	**Źródło zgłoszenia**	**Data rozpoczęcia**	**Data zakończenia**	**Czy koniec?**	**Odpowiedzialny za realizację**	**Przyczyna niezgodności**	**Działanie korygujące / zapobiegawcze**	**Ocena skuteczności**
podać opis incydentu	podać źródło zgłoszenia np. zawiadomienie, kontrola, itd.			czy incydent się zakończył Tak/Nie	podać dane osoby lub funkcje osoby odpowiedzialnej	podać przyczynę powstania incydentu	opisać działania jekie podjęto w celu przywrócenia bezpieczeństwa	opisać jakie skutki przyniosło działanie korygujące

Załącznik nr 1.6 Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Zgłoszenie naruszenia ochrony danych osobowych organowi nadzorczemu

Data …… Godzina ……(naruszenia)

1. Osoba powiadamiająca o naruszeniu oraz inne osoby zaangażowane lub odpytane w związku z naruszeniem (imię, nazwisko, stanowisko służbowe):
……..

2. Lokalizacja zdarzenia (nr pokoju, nazwa pomieszczenia, określenie komputerowego stanowiska roboczego, nazwa programu lub aplikacji itp.):
……

3. Rodzaj naruszenia i określenie okoliczności towarzyszących naruszeniu (*opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie);*
……

4. Podjęte działania:
……

5. Wstępna ocena przyczyn wystąpienia naruszenia (*opisywać możliwe konsekwencje naruszenia ochrony danych osobowych);*
……

6. Postępowanie wyjaśniające i naprawcze (*opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków);*
……

7. Imię i nazwisko oraz dane kontaktowe punktu kontaktowego, od którego można uzyskać więcej informacji:
……

……
(data i podpis administratora)