Polityka Bezpieczeństwa Danych Osobowych w Fundacji „Światło-Życie” z siedzibą w Katowicach KRS 0000071891

obowiązująca od dnia 25 maja 2018 r.

Katowice 2018

SPIS TREŚCI

WYKAZ SKRÓTÓW

GIODO	-	Generalny Inspektor Ochrony Danych Osobowych
RODO	-	Rozporządzenie Ogólne o Ochronie Danych Osobowych
POLITYKA BEZPIECZEŃSTWA	-	dokumentacja określająca założenia ochrony danych osobowych w jednostce organizacyjnej (tutaj w Fundacji)
INSTRUKCJA ZARZĄDZANIA SYSTEMEM INFORMATYCZNYM	-	instrukcja związana z zarządzaniem wszelkim sprzętem informatycznym wykorzystywanym w celu zorganizowanej działalności przedsiębiorstwa
przetwarzanie danych	-	jakiekolwiek operacje wykonywane na danych osobowych, 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, a zwłaszcza te, które wykonuje się w systemach informatycznych
system informatyczny	-	zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych
integralność danych	-	właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany
rozliczalność	-	właściwość zapewniająca, że działania podmiotu mogą być przypisane w sposób jednoznaczny tylko temu podmiotowi
zabezpieczenie danych w systemie informatycznym	-	wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem
zgoda osoby której dane dotyczą	-	oświadczenie woli, którego treścią jest zgoda na przetwarzanie danych osobowych tego, kto składa oświadczenie; zgoda nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści, przy czym zgoda może obejmować przetwarzanie danych w przyszłości, o ile nie zmieni się jego cel
uwierzytelnianie	-	działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu
dane osobowe	-	wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej, jeżeli jej 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; informacji nie uważa się za umożliwiającą określenie tożsamości osoby, jeżeli wymagałoby to nadmiernych kosztów, czasu lub działań
dane wrażliwe	-	dane o pochodzeniu rasowym lub etnicznym, poglądach politycznych, przekonaniach religijnych lub filozoficznych, przynależności wyznaniowej, partyjnej lub związkowej, jak również danych o stanie zdrowia, kodzie genetycznym, nałogach lub życiu seksualnym oraz danych dotyczących skazań, orzeczeń o ukaraniu i mandatów karnych, a także innych orzeczeń wydanych w postępowaniu sądowym lub administracyjnym

zbiór danych - każdy posiadający strukturę zestaw danych o charakterze osobowym, dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest rozproszony lub podzielony funkcjonalnie

ADO - organ, jednostka organizacyjna, podmiot lub osoba, decydujące o celach i środkach przetwarzania danych osobowych (co do zasady jest to kierownictwo)

hasło - ciąg znaków literowych, cyfrowych lub innych, znany jedynie osobie uprawnionej do pracy w systemie informatycznym

obszar przetwarzania - wszelkiego rodzaju pomieszczenia wykorzystywane na cele zorganizowanej działalności:
- pomieszczenia biurowe, w których zlokalizowane są stacje robocze lub serwery służące do przetwarzania danych osobowych,
- pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego zawierające dane osobowe,
- pomieszczenia, w których przechowywane są sprawne i uszkodzone urządzenia, elektroniczne nośniki informacji oraz kopie zapasowe zawierające dane osobowe.

osoba upoważniona - osoba posiadająca formalne upoważnienie do przetwarzania danych osobowych

identyfikator użytkownika - ciąg znaków literowych, cyfrowych lub innych jednoznacznie identyfikujący osobę upoważnioną do przetwarzania danych osobowych w systemie informatycznym

poufność danych - właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom

odbiorca danych - za odbiorcę uznaje się osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, z wyjątkiem organów publicznych, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego

WSTĘP

Zarząd Fundacji „Światło-Życie" z siedzibą w Katowicach ul. Różyckiego 8, uznając wagę ochrony prawa do prywatności osób, których dane dotyczą, realizując zasady zgodności z prawem, ograniczenia celu, minimalizacji danych, prawidłowości i aktualności, ograniczenia przechowywania, integralności i poufności oraz rozliczalności, wyrażonych w Rozporządzeniu 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), dalej jako *RODO*, a także spełniając wymogi Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, przyjmuje niniejszą Politykę Bezpieczeństwa Danych Osobowych, zwaną dalej Polityką.

Zarząd zobowiązuje się do opracowywania, aktualizacji, przestrzegania i rozpowszechniania wśród współpracowników Fundacji zasad ochrony danych osobowych, szczególnie danych wrażliwych. Zarząd Fundacji „Światło-Życie" są świadomi zagrożeń społecznych i technologicznych, na jakie narażone są te dane. Realizując zatem przepisy prawa i najwyższe standardy etyczne, podejmują się za pomocą niniejszej polityki bezpieczeństwa i towarzyszących jej dokumentów chronić interesy osób, których dane mogłyby być zagrożone.

Rozdział 1
Przepisy ogólne

§ 1.

Niniejsza Polityka Fundacji „Światło-Życie" (zwana dalej Polityką), powstała w celu realizacji obowiązków wynikających z art. 36 ust. 2 Ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (dalej zwanej *Ustawą*) oraz Ogólnego rozporządzenia o ochronie danych.

§ 2.

Niniejsza polityka bezpieczeństwa określa zasady i tryb postępowania przy przetwarzaniu danych osobowych w Fundacji „Światło-Życie", w zakresie objętym postanowieniami aktów, o których mowa w § 1.

§ 3.

Celem niniejszej polityki bezpieczeństwa jest zapewnienie przestrzegania obowiązującego prawa, zobowiązań Fundacji „Światło-Życie" oraz poszanowanie i ochrona interesów, w szczególności prawa do prywatności, osób, których dane są przetwarzane.

§ 4

Zarząd Fundacji „Światło-Życie" jest administratorem danych w rozumieniu art. 7 pkt 4 Ustawy oraz RODO, zwanym w dalszej części również ADO.

§ 5 .

W imieniu ADO działa osoba wydelegowana przez Zarząd odrębnym dokumentem.

§ 6

Zarząd Fundacji „Światło-Życie" dokłada wszelkich starań, aby zbierane dane osobowe były przetwarzane zgodnie z prawem oraz uwzględnia interesy i rozsądne oczekiwania osób, których dane są przetwarzane, zachowując przy tym wszystkie obowiązki informacyjne względem nich.

§7.

Dane zbierane są i przetwarzane jedynie w konkretnych, wyraźnie wskazanych i uzasadnionych celach. Dalsze przetwarzanie danych przez ADO, po ich zebraniu następuje po uzyskaniu odrębnej zgody. Przetwarzane są tylko takie dane osobowe, bez których nie da się osiągnąć zamierzonego celu przetwarzania.

§8

Administrator dokłada szczególnej staranności w celu zbierania danych merytorycznie poprawnych, odpowiadających rzeczywistemu stanowi rzeczy oraz nie pozyskuje danych ze źródeł niewiadomego pochodzenia. Nieaktualne lub nieprawdziwe dane są niezwłocznie usuwane lub prostowane, w przypadku zaistnienia takich okoliczności.

§9.

Niezanonimizowane dane usuwane są po upływie okresu, w którym ich przetwarzanie było niezbędne do osiągnięcia celu przetwarzania.

§10.

ADO podejmuje wszelkie środki techniczne i organizacyjne, adekwatne do ryzyka naruszenia bezpieczeństwa danych, w tym ochronę przed niezgodnym z prawem przetwarzaniem, utratą, zniszczeniem i uszkodzeniem.

Rozdział 2
Podstawa przetwarzania danych

§ 1.

Przetwarzanie zebranych danych osobowych jest zgodne z prawem, gdy:

a) otrzymano zgodę na ich przetwarzanie od osoby, której dane dotyczą,
b) jest to niezbędne do wykonania umowy zawartej z osobą, której dane dotyczą,
c) jest to niezbędne do wykonania obowiązku prawnego, ciążącego na ADO
d) jest to niezbędne do ochrony żywotnych interesów osoby fizycznej,
e) ADO realizuje zadanie w interesie publicznym lub w ramach powierzonej mu władzy publicznej,
f) przetwarzanie wynika z prawnie uzasadnionych interesów ADO lub osoby trzeciej chyba, że jako nadrzędne należy uznać prawa i wolności osoby, której dane dotyczą, w szczególności w przypadku danych dziecka.

§2.

Zgoda na przetwarzanie danych osobowych jest zbierana, o ile to możliwe, pisemnie (w wersji papierowej, elektronicznej). Zgoda może zostać udzielona ustnie. Zgodę udziela się odrębnie dla każdego celu przetwarzania.

§3.

Zgodę na przetwarzanie, wyrażoną w formie pisemnej, ADO wyróżnia spośród pozostałej części tekstu, o ile jest ona częścią innego dokumentu. Zgoda formułowana jest w sposób maksymalnie przystępny, jasnym i zrozumiałym językiem.

§4.

ADO informuje o możliwości wycofania zgody w każdym momencie. Wycofanie zgody powinno być tak samo łatwe jak jej udzielenie.

§5.

W przypadku zbierania dodatkowych danych, ADO wyróżnia, które dane są niezbędne do realizacji umowy, a które mogą być podane dobrowolnie w innych celach przetwarzania.

§6.

W przypadku, w którym ADO będzie zbierał dane osobowe, w celu świadczenia usług drogą elektroniczną, odpłatnie (tzw. usługi społeczeństwa informacyjnego), oferowanych bezpośrednio dziecku, ADO dokłada wszelkich starań, aby za pomocą dostępnej technologii zweryfikować, czy osoba sprawująca opiekę nad dzieckiem poniżej 16 roku życia wyraziła zgodę na przetwarzanie danych osobowych.

§7.

Zgodę na przetwarzanie danych wrażliwych takich jak: pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby, ADO uzyskuje tylko w formie pisemnej, z jednoczesnym, wyraźnym wskazaniem celu przetwarzania. Wymóg ten nie dotyczy realizacji obowiązków wynikających z przepisów prawa pracy, ubezpieczeń społecznych i podatkowego i zabezpieczenia socjalnego.

Rozdział 3
Obowiązki informacyjne

§1.

ADO, zbierając dane osobowe, w maksymalnie zwięzły, zrozumiały i transparentny sposób, starając się, aby forma była łatwo dostępna, przekazuje informacje:

a) nazwa i dane kontaktowe Zarządu Fundacji lub Kierownika Ośrodka Fundacji
b) gdy ma to zastosowanie - dane kontaktowe osoby, odpowiedzialnej za procesy przetwarzania danych, z zaznaczeniem, że nie jest ona inspektorem ochrony danych,
c) cele przetwarzania danych osobowych oraz podstawę prawną,
d) opis prawnie uzasadnionych interesów ADO lub osoby trzeciej, dla których celów przetwarzanie jest niezbędne
e) odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją,
f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej wraz ze wzmianką o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych,
g) okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu,
h) o prawie do żądania od Zarządu Fundacji „Światło-Życie" (ADO) lub Kierownika Ośrodka Fundacji „Światło-Życie" dostępu do danych osobowych, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu, w szczególności wobec przetwarzania w celach marketingu bezpośredniego, a także o prawie do przenoszenia danych,
i) informacje o prawie do cofnięcia zgody w dowolnym momencie z zaznaczeniem, że wycofanie zgody nie powoduje, że dotychczasowe przetwarzanie było bezprawne,
j) o prawie wniesienia skargi do organu nadzorczego - Prezesa Urzędu Ochrony Danych Osobowych z podaniem adresu,

k) czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych,
l) gdy ma to zastosowanie - informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu oraz istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.
m) jeżeli Zarząd Fundacji „Światło-Życie" (ADO) lub Kierownik Ośrodka Fundacji „Światło-Życie" planuje przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu.

§2.

Osoba, której dane dotyczą, może zwrócić się do ADO o potwierdzenie, czy dane są przetwarzane oraz na jakich zasadach.

§3.

ADO na żądanie dostarcza kopię danych osobowych. Za każdą kolejną kopię mogą być naliczone opłaty, odpowiadające kosztom administracyjnym ich wydania.

§4.

Na żądanie osoby, której dane dotyczą ADO usuwa je bez zbędnej zwłoki.

§5.

Obowiązek usunięcia aktualizuje się w przypadku, gdy:

- cofnięto zgodę na przetwarzanie,
- osiągnięto cel przetwarzania i nie są one już niezbędne,
- obowiązek usunięcia wynika z wniesienia sprzeciwu w zakresie przetwarzania w celu marketingu bezpośredniego lub w przypadku przetwarzania wynikającego z zadania realizowanego przez ADO w interesie publicznym lub w ramach sprawowania władzy (np. zadania zlecone przez Jednostkę Samorządu Terytorialnego) lub z uwagi na niezbędność przetwarzania z powodu prawnie uzasadnionych interesów.
- usunięcie wynika z obowiązku prawnego, któremu podlega ADO, gdy zgoda na przetwarzanie danych osobowych dziecka poniżej 16 roku życia, dotyczących usług społeczeństwa informacyjnego zostały zebrane bez zgody rodzica/opiekuna prawnego.

§6.

Na żądanie osoby, której dane dotyczą ADO przekazuje jej kopię przetwarzanych danych w formacie możliwym do odczytu maszynowego, które może przesłać innemu administratorowi. ADO, o ile jest to technicznie możliwe, na żądanie osoby fizycznej umożliwia przesłanie jej danych bezpośrednio innemu administratorowi. Obowiązek ten aktualizuje się w przypadku zautomatyzowanego przetwarzania danych, przekazanych na podstawie umowy lub zgody na przetwarzanie danych.

§7.

Ograniczenie przetwarzania danych oznacza, że ADO zobowiązany jest do przechowywania dotychczas zebranych danych, przy czym brak jest możliwości dokonywania na nich innych operacji niż przechowywanie, chyba że

- osoba wyrazi zgodę na inny rodzaj przetwarzanie lub
- przetwarzanie jest konieczne w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub
- z uwagi na ważne względy interesu publicznego

§8.

ADO ma obowiązek zrealizować żądanie ograniczenia przetwarzania danych, gdy:

- kwestionowana jest prawidłowość danych, do czasu sprawdzenia ich poprawności,
- ADO przetwarza dane niezgodnie z prawem, ale osoba uprawniona żąda w zamian ograniczenia,
- dane nie są potrzebne ADO do przetwarzania, ale są potrzebne uprawnionemu do ustalenia roszczeń, dochodzenia roszczeń, obrony roszczeń
- osoba uprawniona wniosła sprzeciw (do czasu ustalenia uprawnienia do przetwarzania).

§9.

ADO nie podejmuje decyzji w zakresie danych osobowych w sposób zautomatyzowany oraz nie dokonuje czynności profilowania. W przypadku zmiany sytuacji, ADO zawsze informuje o takim celu przetwarzania, dbając, aby przetwarzanie odbyło się na podstawowej świadomej zgody osoby, której dane dotyczą.

§10.

Prawo do wniesienia sprzeciwu przeciwko przetwarzaniu danych, przysługuje w dowolnym momencie osobie, której dane dotyczą, gdy przetwarzane są one na potrzeby marketingu bezpośredniego, w tym profilowania.

§11.

W innych przypadkach prawo do wniesienia sprzeciwu powstaje z przyczyn związanych ze szczególną sytuacją osoby, gdy ADO przetwarza dane osobowe, w tym dokonuje profilowania w związku z następującymi podstawami:

- z uwagi na niezbędność do zrealizowania zadania w interesie publicznym,
- w ramach sprawowania władzy publicznej powierzonej ADO,
- gdy przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez ADO lub przez stronę trzecią.

§12.

W przypadku zgłoszenia przez osobę, której dane dotyczą, żądań określonych w rozdziale 3 §1 punkt h ADO podejmuje niezwłoczne działania w celu ustalenia zasadności żądania oraz jego zrealizowania. O swojej decyzji lub podjętych działaniach informuje niezwłocznie w sposób jasny i zrozumiały.

§13.

Żądanie może być wyrażone w każdej formie. Na stronie internetowej ADO zamieszcza się krótką informację o danych kontaktowych osoby odpowiedzialnej za przetwarzanie danych osobowych (o ile zostanie wyznaczona) albo ogólne dane kontaktowe, dzięki którym mogą być realizowane powyższe uprawnienia osób, których dane dotyczą.

Rozdział 4
Pozostałe obowiązki ADO

§1.

ADO uwzględnia charakter, zakres, kontekst i cele przetwarzania oraz bierze pod uwagę ryzyko naruszenia praw i wolności osób fizycznych. W tym celu wdraża odpowiednie środki techniczne i organizacyjne.

§2.

W przypadku powierzenia przetwarzania innym podmiotom, w szczególności w zakresie usług IT, chmury obliczeniowej, działalności statutowej ADO w internecie, przesyłania danych osobowych,

ADO korzysta z usług podmiotów, które gwarantują poziom zabezpieczeń zgodny z wymogami UE i prawa krajowego.

§3.

ADO w miarę możliwości, szczególnie w przypadku zwiększania zakresu i kategorii przetwarzania danych oraz wprowadzania nowych narzędzi technologicznych, dokonuje przeglądu istniejących procedur ochrony danych oraz zastosowanych środków technicznych i organizacyjnych, nie rzadziej niż raz na rok.

§4.

Ocenę ryzyka i aktualizację dokumentacji bezpieczeństwa informacji przeprowadza się także w przypadku pojawienia się nowego urządzenia technicznego, nowego sposobu przetwarzania informacji, nowej kategorii przetwarzanych danych lub nowego procesu przetwarzania.

Rozdział 5
Realizacja zasad

§1.

Wprowadzając nowe narzędzia, związane z prowadzonymi działaniami statutowymi, albo planując kolejne działania, w tym projektując i wprowadzając nowe rozwiązania technologiczne, ADO przeprowadza analizę obejmującą odpowiedzi na następujące pytania:

- czy projektowane rozwiązanie będzie wymagało przetwarzania danych osobowych lub jest wprowadzane w celu ich przetwarzania?
- jakie środki techniczne i organizacyjne są konieczne do zapewnienia bezpieczeństwa?
- czy możliwa jest pseudonimizacja danych, szyfrowanie?
- w jaki sposób ograniczyć prawdopodobieństwo udostępnienia danych osobom nieupoważnionym?

§2.

Analiza, o której mowa w niniejszym paragrafie, powinna zostać przeprowadzona przed rozpoczęciem przetwarzania danych osobowych. Wnioski z analizy powinny zostać utrwalone.

§3.

Po dokonaniu identyfikacji czy istnieje ryzyko naruszenia praw osób, których dane dotyczą, ADO podejmuje działanie w celu jego minimalizacji, co może obejmować:

1) uniknięcie ryzyka poprzez powstrzymanie się od wykonywania określonej czynności obarczonej ryzykiem,
2) usunięcie źródeł ryzyka,
3) podjęcie działań pozwalających zmniejszyć prawdopodobieństwo wystąpienia ryzyka,
4) podjęcie działań umożliwiających uniknięcie następstw wystąpienia ryzyka.

§4.

W przypadku stosowania rozwiązań technologicznych, ADO zapewnia, aby domyślne przetwarzanie danych dotyczyło jedynie danych niezbędnych do realizacji zadania. Żadne dodatkowe informacje nie powinny być udostępniane bez interwencji osoby, której dane zebrano nieokreślonej liczbie osób fizycznych.

§5.

ADO uwzględnia stan wiedzy technicznej dotyczącej możliwych do zastosowania środków oraz koszt wdrożenia tych środków.

Rozdział 6
Zarządzanie ryzykiem

§1.

ADO przeprowadza szczegółową analizę prowadzonych procesów przetwarzania danych i dokonuje samodzielnej oceny ryzyka naruszenia ochrony przetwarzanych danych w konkretnym przypadku.

§2.

Oceny ryzyka bezpieczeństwa informacji dokonuje w imieniu i na rzecz Fundacji „Światło-Życie" - Zarząd, członek Zarządu, Kierownik Ośrodka, któremu delegowano realizację obowiązków z zakresu ochrony danych osobowych,

§3.

Istnieje możliwość zlecenia dokonania oceny ryzyka podmiotowi zewnętrznemu lub osobie odpowiedzialnej za określony proces przetwarzania danych.

§4.

Ryzyko jest szacowane na podstawie obiektywnej i rzeczowej analizy, której celem jest określenie stopnia ryzyka, wiążącego się z operacjami przetwarzania danych (wysokie lub niskie).

§5.

Ocenę ryzyka przeprowadza się przed przystąpieniem do przetwarzania danych, uwzględniając zasadę ochrony danych osobowych w fazie projektowania rozwiązań, nie rzadziej niż raz na rok.

§6.

Ocenę ryzyka o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, wynikające z przetwarzania danych, przeprowadza się uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych.

§7.

Ocena ryzyka dokonywana jest w miarę możliwości w sposób ilościowy i jakościowy. W przypadku niemożliwości lub zbytniej trudności dokonania oceny ilościowej dopuszczalne jest ograniczenie się do jakościowej oceny ryzyka.

§8.

Ocenę ryzyka i aktualizację dokumentacji bezpieczeństwa informacji można przeprowadzić w każdym innym czasie, o ile jest to celowe, zwłaszcza po wystąpieniu naruszenia lub jego realnej możliwości.

Rozdział 7
Wdrażanie zasad

§1

ADO instruuje pracowników i wolontariuszy oraz osoby, które współpracują z Fundacją „Światło-Życie" na podstawie umów cywilnoprawnych o obowiązkach, wynikających z powszechnie obowiązujących przepisów o ochronie danych osobowych oraz niniejszej polityki i innych dokumentów wewnętrznych.

§2.

Podmioty wymienione w ustępie poprzednim, współpracujące z Fundacją „Światło-Życie", potwierdzają na piśmie zapoznanie się z dokumentacją dotyczącą ochrony danych osobowych.

§3.

Zarząd nadaje upoważnienia osobom dopuszczonym do przetwarzania danych osobowych. Upoważnienia mogą być nadawane w formie pisemnej lub elektronicznie. W razie konieczności ADO prowadzi rejestr upoważnień w formie elektronicznej.

§4.

Umowy, zawierane przez Fundację „Światło-Życie", zawierają klauzulę zobowiązującą podmioty wymienione w poprzednim paragrafie do zachowania w tajemnicy danych osobowych przetwarzanych przez Fundację „Światło-Życie" i przestrzegania ww. obowiązków, o ile tylko przewiduje się, że podmiot będzie mieć dostęp do tych danych.

§5.

Umowy wskazane w poprzednim ustępie, będą przewidywać odpowiedzialność ww. podmiotów w przypadku naruszenia przez nie obowiązków w zakresie ochrony danych osobowych.

§7.

ADO prowadzi rejestr czynności przetwarzania, który zawiera:

a. imię i nazwisko lub nazwę oraz dane kontaktowe administratora oraz wszelkich współadministratorów,
b. cele przetwarzania,
c. opis kategorii osób, których dane dotyczą, oraz kategorii danych osobowych,
d. kategorie odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w tym odbiorców w państwach trzecich lub w organizacjach międzynarodowych,
e. przekazanie danych osobowych do państwa trzeciego lub organizacji międzynarodowej, wraz z informacją o wprowadzeniu odpowiednich zabezpieczeń,
f. planowane terminy usunięcia poszczególnych kategorii danych,
g. ogólny opis technicznych i organizacyjnych środków bezpieczeństwa.

§8.

ADO wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający określonemu ryzyku, w tym w zależności od potrzeb i celów przetwarzania:

a. pseudonimizację i szyfrowanie danych osobowych,
b. zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania,
c. zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego,
d. regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

Rozdział 8
Naruszenia bezpieczeństwa

§1.

Podejrzenie naruszenia bezpieczeństwa danych lub jego realną możliwość zgłasza się niezwłocznie Zarządowi lub właściwemu Kierownikowi Ośrodka Fundacji. Zgłoszenia dokonuje podmiot, który ww. naruszenie lub jego realną możliwość odkrył lub podejrzewa.

§2.

ADO sprawdza czy nastąpiło naruszenie lub jego realna możliwość, a jeśli tak - w jakiej skali i jakich danych dotyczy.

§3.

W przypadku naruszenia bezpieczeństwa informacji lub realnej możliwości jego wystąpienia, ADO podejmuje wszelkie niezbędne kroki dla powstrzymania naruszenia lub jego możliwości, a także zminimalizowania ich skutków.

§4.

ADO bez zbędnej zwłoki - w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia - zgłasza je Prezesowi Urzędu Ochrony Danych Osobowych (PUODO). Do zgłoszenia przekazanego *GIODO* po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

§5.

ADO dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Jego treść zawiera szczegółowe dane o naruszeniu lub możliwości jego wystąpienia, takie jak metoda naruszenia, zaangażowane podmioty, zagrożone dane. Zarząd opisuje także podjęte środki techniczne i instytucjonalne, służące powstrzymaniu naruszenia i zabezpieczające przed wystąpieniem naruszenia w przyszłości. Sprawozdanie może także sugerować dalsze kroki do podjęcia przez ADO, w tym zwłaszcza ponowną ocenę ryzyka.

§6.

Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki powiadamia osoby, których dane dotyczą, o takim naruszeniu.

§7.

Zawiadomienie sporządza się jasnym i prostym językiem. Zawiadomienie opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej następujące informacje i środki:

a. imię i nazwisko oraz dane kontaktowe osoby, której dotyczy naruszenie;
b. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
c. opisywać środki zastosowane lub proponowane w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

§8.

Zawiadomienie, o którym mowa w §1 i §2, nie jest wymagane, gdy:

a. wdrożono 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. zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą,
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.

§9.

W przypadku naruszenia bezpieczeństwa danych przez pracowników, wolontariuszy lub osoby pozostające z Fundacją „Światło-Życie" w stosunku cywilnoprawnym, Fundacją „Światło-Życie" może wyciągnąć wobec nich konsekwencje przewidziane odpowiednimi umowami.

§10.

Jeśli jest to celowe, Zarząd po wystąpieniu naruszenia lub jego realnej możliwości, instruuje odpowiednich współpracowników o wprowadzonych zmianach i sposobach przetwarzania danych i ich ochrony.

§11.

W przypadku naruszeń dokonanych przez pracowników, Fundacją „Światło-Życie" stosuje środki przewidziane Kodeksem pracy.

Rozdział 9
Ocena skutków

§1.

W przypadku przetwarzania danych osobowych na dużą skalę lub w sposób zautomatyzowany, w tym profilowania dokonywanych za pomocą chmury obliczeniowej. ADO dokonuje oceny skutków dla ochrony danych w związku z ww. sposobem przetwarzania.

§2.

Ocena skutków zawiera, co najmniej:

- systematyczny opis planowanych operacji przetwarzania i celów przetwarzania,
- ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
- ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą, o którym mowa w ust. 1;
- środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

Rozdział 10
Środki techniczne i organizacyjne

§1.

Fundacja przetwarza dane osobowe w siedzibie Zarządu Fundacji, jak również w siedzibie poszczególnych Ośrodków Fundacji.

§2.

Dane przetwarzane w sposób tradycyjny znajdują się w pomieszczeniach, z których korzysta Fundacja. Dane znajdują się w szafach zamkniętych na klucz, do których dostęp mają tylko upoważnione osoby. Po zakończonej pracy klucze do szaf chowane są do zamykanej szuflady.

§3.

Dane przetwarzane elektronicznie są przetwarzane za pomocą programów:

- pakiet biurowy Office
- programu księgowego

§4.

Ww. dane są przetwarzane na komputerach przenośnych i stacjonarnych, należących do Fundacji jak też komputerach przenośnych prywatnych.

§5.

Dostęp do jednostek roboczych należących do Fundacji zabezpieczony jest bezpiecznym hasłem, zmienianym raz na 6 miesięcy. Hasło składa się z minimum 8 znaków, w tym wielkiej litery, cyfry i znaku specjalnego.

§6.

ADO zobowiązuje swoich współpracowników, by zabezpieczali jednostki robocze, na których dokonują przetwarzania informacji, za pomocą hasła spełniającego te kryteria.

§7.

Każdy współpracownik ma własny login/identyfikator, który umożliwia powiązanie dokonywanych przez niego czynności na danych osobowych w systemie teleinformatycznym (e-mail).

§8.

Niektóre dane przetwarzane w sposób tradycyjny, są również przetwarzane elektronicznie. ADO ogranicza do minimum przetwarzanie danych osobowych w formie elektronicznej.

§9.

Po wyczerpaniu celów przetwarzania dane osobowe w formie tradycyjnej są niszczone za pomocą niszczarki znajdującej się w biurze. Nośniki elektroniczne danych są czyszczone z zawartości, a jeśli nie jest to możliwe - uszkadzane w sposób uniemożliwiający odczyt. Nośniki elektroniczne danych nie są przekazywane innym podmiotom ani nie służą innym celom niż przetwarzanie danych.

§10.

Dostęp do komputera zabezpieczony jest nazwą użytkownika i hasłem 8-znakowym, w którym występują litery wielkie i małe i cyfry lub znaki specjalne. Komputer jest zabezpieczony przed nieuprawnionym dostępem z zewnątrz za pomocą oprogramowania antywirusowego i systemowej "zapory ogniowej" (*firewall*) o parametrach ustalonych przez producenta systemu.

§11.

Oprogramowanie jest aktualizowane na bieżąco za pomocą wbudowanego mechanizmu aktualizacji. System operacyjny jest aktualizowany na bieżąco za pomocą wbudowanego mechanizmu aktualizacji.

§12.

Tworzone są kopie zapasowe danych elektronicznych, na dyskach zewnętrznych, przechowywanych w biurze Zarządu i Ośrodków Fundacji.

§13.

Zarząd Fundacji i Kierownik Ośrodka zobowiązuje osoby współpracujące i pracowników do stosowania zasad bezpieczeństwa, w szczególności zmiany haseł, a także nie przetwarzania danych osobowych na prywatnych komputerach.

§14.

Przetwarzanie przez współpracowników danych osobowych na prywatnym komputerze powinno odbywać się za wyraźną zgodą Zarządu lub Kierownika Ośrodka po upewnieniu się, że pracownik (wolontariusz) stosuje wszystkie konieczne zasady bezpieczeństwa.

§15.

Zabronione jest przetwarzanie danych osobowych na prywatnych smartfonach oraz przesyłanie danych osobowych, przetwarzanych przez Fundację poprzez prywatne konta pocztowe takie jak @gmail.com, publiczne, darmowe chmury obliczeniowe takie jak google drive, na portalach społecznościowych takich jak Facebook, czy whatssap, messenger.

§16.

Strona www. fundacja.oaza.pl posiada certyfikat SSL oraz protokół https/.

§17.

Pracownicy, wolontariusze i współpracownicy, z którymi podpisano umowy cywilnoprawne, którzy mają do czynienia z danymi osobowymi, zostali poinstruowani o sposobach postępowania przy ich przetwarzaniu. Wyżej wymieniony osoby zostały zobowiązane do utrzymywania przetwarzania danych osobowych w ścisłej tajemnicy.

§18.

Instalowane jest tylko oprogramowanie z zaufanych źródeł.

§19.

ADO przeprowadza wewnętrzne szkolenia z zakresu ochrony danych osobowych.