POLITYKA OCHRONY DANYCH W FUNDACJI POMAGAM.

ŁÓDŹ, 25 maja 2018 R.

WSTĘP

Jesteśmy świadomi ważności informacji przetwarzanej w Fundacji POMAGAM (dalej zwana „Fundacją"), dlatego też zobowiązujemy się do stwarzania warunków w celu zapewnienia jej bezpieczeństwa, w tym również poprzez zagwarantowanie na jej ochronę odpowiednich środków finansowych i personalnych. Ponadto zobowiązujemy się do spełnienia wymagań prawnych i kontraktowych związanych z bezpieczeństwem informacji, szczególnie w zakresie przepisów o ochronie danych osobowych.

Nasz system bezpieczeństwa oparty na elementach, które spełniają wymagania ujęte w ustawie o ochronie danych osobowych Ustawa o ochronie danych osobowych z dnia 27 sierpnia 1997 r. (Dz. U. 2002 r. r 101 poz. 925 z późn. zm.) został zaktualizowany i dostosowany do wymogów Ogólnego rozporządzenia UE o ochronie danych 2016/697 (RODO), które weszło w życie z dniem 25.05.2018.

ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe:
    a. zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość"),
    b. zbiera je w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie przetwarza ich dalej w sposób niezgodny z tymi celami („ograniczenie celu"),
    c. adekwatnie, stosownie oraz w sposób ograniczony do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych"),
    d. prawidłowo i w razie potrzeby uaktualnia zebrane dane („prawidłowość"),
    e. przechowuje je w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy niż jest to niezbędne do celów, w których dane te są przetwarzane („ograniczenie przechowywania"),
    f. w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych („integralność i poufność").

2. W celu realizacji tych zasad administrator danych przetwarza dane legalnie, na podstawie przesłanek opisanych w art. 6 RODO. Pobiera dane osobowe adekwatnie do celów przetwarzania i przetwarza je przez określony czas. Wobec osób, których dane przetwarza wypełnia obowiązki informacyjne określone w art. 13 RODO lub w art. 14 RODO (gdy informacje pobierane są w sposób inny niż od osoby, której dane dotyczą) oraz wskazuje przysługujące im uprawnienia takie jak prawo do:
    a. dostępu do danych,
    b. sprostowania danych,
    c. usunięcia danych (prawo do bycia zapomnianym),
    d. przenoszenia,
    e. sprzeciwu wobec przetwarzania,
    f. ograniczenia przetwarzania,
    g. wniesienia skargi do organu nadzorczego,
    h. sprzeciwu wobec bycia profilowanym.

Administrator danych zapewnia ochronę danych w przypadku korzystania z usług podmiotów zewnętrznych w postaci zawierania stosownych umów powierzenia oraz korzystając z usług podmiotów przetwarzających realizujących obowiązki wynikające z RODO. W razie wystąpienia

incydentu technicznego lub fizycznego administrator danych zapewnia zdolność do szybkiego przywrócenia dostępności do danych osobowych i dostępu do nich.

CZYNNOŚCI DOKONANE W MYŚL ZAPISÓW RODO

1. Identyfikacja procesów przetwarzania danych osobowych

Zidentyfikowano procesy, w których dochodzi do powierzenia przetwarzania danych osobowych.

2. Weryfikacja parametrów procesów przetwarzania danych

2.1. Dla każdego zidentyfikowanego procesu przetwarzania danych określono:

a) podstawę przetwarzania danych osobowych zgodną z RODO,
b) zweryfikowano zakres przetwarzanych danych, zgodnie z zasadą minimalizacji, w przypadku, gdy przetwarzanie danych opiera się o zgody zebrane przed 25 maja 2018 r. zweryfikowano ich ważność
c) zweryfikowano treść obowiązków informacyjnych towarzyszących gromadzeniu danych.

3. Określenie poziomów ryzyka związanego z przetwarzaniem danych

Dla wszystkich procesów przetwarzania danych osobowych określono poziom ryzyka związanego z przetwarzaniem danych osobowych oraz zastosowano odpowiednie środki zabezpieczenia danych. Poziom ryzyka związanego z przetwarzaniem danych osobowych podlega ciągłemu monitorowaniu w ramach trwających procesów przetwarzania danych.

4. Przeprowadzenie procedury oceny skutków dla ochrony danych

4.1. Wykonanie oceny skutków dla ochrony danych osobowych może być obowiązkowe dla procesów przetwarzania danych. Zastosowano elementy oceny skutków dla ochrony danych:

a) systematyczny opis bieżących planowanych operacji (procesów) przetwarzania,
b) opis celów przetwarzania oraz podstawa prawna przetwarzania (w tym, gdy ma to zastosowanie prawnie uzasadnionych interesów realizowanych przez administratora),
c) ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów,
d) ocena ryzyka naruszenia praw lub wolności osób, których dane dotyczą,
e) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia,
f) opis mechanizmów bezpieczeństwa mający zapewnić ochronę danych osobowych i wykazać przestrzeganie rozporządzenia, z uwzględnieniem praw i prawnie

uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy.

5. Powierzenie przetwarzania danych

Zidentyfikowano wszystkie procesy przetwarzania danych, w których dochodzi do powierzenia przetwarzania danych. Administrator dokonuje Wyboru podmiotu przetwarzającego, który zapewnia przestrzeganie RODO. Z podmiotami przetwarzającymi zawierane są umowy powierzania.

6. Dodatkowe prawa osób, których dane dotyczą

Wprowadzono dodatkowe uprawnienie dla osób, których dane są przetwarzane (w szczególności prawo do bycia zapomnianym) poprzez:

a) możliwość żądania przez osobę, której dane dotyczą, usunięcia jej danych osobowych przez administratora danych,
b) możliwość żądania, aby administrator danych poinformował innych administratorów danych, którym upublicznił dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych lub ich kopie.

Prawo do bycia zapomnianym można wykonać, jeżeli spełniona jest choć jedna z następujących przesłanek:

a) jeżeli dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane,
b) jeżeli osoba, której dane dotyczą, wycofała zgodę na przetwarzanie danych osobowych i nie istnieje inna podstawa przetwarzania danych,
c) jeżeli osoba, której dane dotyczą, zgłosiła sprzeciw wobec przetwarzania swoich danych w związku ze swoją szczególną sytuacją albo wobec przetwarzania danych dla celów marketingowych,
d) jeżeli dane osobowe były przetwarzane „niezgodnie z prawem",
e) jeżeli dane osobowe „muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator",
f) jeżeli dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego bezpośrednio dziecku.

BEZPIECZEŃSTWO PRZETWARZANIA DANYCH OSOBOWYCH

1. Bezpieczeństwo zasobów Fundacji jest realizowane poprzez opracowanie, wdrażanie i stosowanie odpowiednich środków technicznych i organizacyjnych, uwzględniających charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie i wadze zagrożenia.

2. Bezpieczeństwo danych osobowych w Fundacji rozumiane jest jako zapewnienie:
   a) poufności, czyli zapewnienie, że dane są dostępne jedynie osobom upoważnionym,
   b) integralności, czyli zapewnienie poprawności i kompletności danych oraz metod przetwarzania,
   c) dostępności, czyli zapewnienie, że osoby upoważnione mają dostęp do danych wtedy, gdy jest to potrzebne.

STRUKTURA SYSTEMU BEZPIECZEŃSTWA

Administrator systemów informatycznych (ASI) tj. osoba lub firma zobowiązana do zarządzania systemami informatycznymi wykorzystywanymi do przetwarzania danych osobowych, realizuje zadania w zakresie zarządzania i bieżącego nadzoru nad systemem informatycznym administratora danych.

Wyjątkowej ochrony wymagają tzw. dane wrażliwe, czyli szczególne kategorie danych osobowych. Wyróżniamy wśród nich dane dotyczące pochodzenia rasowego lub etnicznego, orientacji seksualnej, poglądów politycznych, przekonań religijnych lub światopoglądu, przynależności do związków zawodowych, danych genetycznych, biometrycznych i zdrowotnych, a także danych dotyczących wyroków skazujących i naruszeń prawa. Ze względu na ich charakter, możliwość przetwarzania danych wrażliwych jest bardzo ograniczona, dozwolona w wyjątkowych przypadkach i obarczona obowiązkiem spełnienia dodatkowych wymogów, np. większego zakresu zabezpieczeń.

1. **Rolą administratora systemów informatycznych (ASI) jest:**
   a. zarządzanie systemem informatycznym, w którym przetwarzane są dane osobowe, posługując się hasłem dostępu do wszystkich stacji roboczych i serwera z pozycji administratora,
   b. przeciwdziałanie dostępowi osób niepowołanych do systemu informatycznego, w którym przetwarzane są dane osobowe,

c. przydzielanie każdemu użytkownikowi identyfikator oraz hasło do systemu informatycznego oraz dokonywanie ewentualnych modyfikacji uprawnień, a także usuwanie konta użytkowników,
d. przeprowadzanie szkolenie stanowiskowego użytkownika w zakresie korzystania ze sprzętu komputerowego i zasobów sieci, zapoznawanie z obowiązującymi w tym zakresie dokumentami,
e. nadzorowanie działania mechanizmów uwierzytelniania użytkowników oraz kontroli dostępu do danych osobowych,
f. w sytuacji stwierdzenia naruszenia zabezpieczeń systemu informatycznego informowanie administratora danych o naruszeniu i współdziałanie z nim przy usuwaniu skutków naruszenia,
g. prowadzenie szczegółowej dokumentacji naruszeń bezpieczeństwa danych osobowych, przetwarzanych w systemie informatycznym,
h. sprawowanie nadzoru nad wykonywaniem napraw, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe, nad wykonywaniem kopii zapasowych, ich przechowywaniem oraz okresowym sprawdzaniem pod kątem ich dalszej przydatności do odtwarzania danych w przypadku awarii systemu informatycznego,
i. podejmowanie działań służących zapewnieniu niezawodności zasilania komputerów, innych urządzeń mających wpływ na bezpieczeństwo przetwarzania danych oraz zapewnienie bezpiecznej wymiany danych w sieci wewnętrznej i bezpiecznej teletransmisji.

2. Ochrona zasobów systemowych

a. nowoczesne sprzętowe oraz programowe rozwiązania typu firewall oraz skanery antywirusowe i antyspamowe,
b. pełni kontrolowany dostęp do zasobów sieciowych oraz archiwów (m.in. różne poziomy uprawnień dostępu do danych nadane przez administratora danych), identyfikatory i hasła uwierzytelniające, rejestr operacji na danych osobowych),
c. kopie bezpieczeństwa zapewniane przez dostawce rozwiązań chmurowych,
d. ustalone sposoby postępowania w obszarze bezpiecznego niszczenia nośników danych z wykorzystaniem niszczarek oraz fizycznego niszczenia (dyski).

3. Ochrona pomieszczeń biurowych

a. całodobowy monitoring pomieszczeń biurowych (współpraca z agencją ochrony mienia),

b. całodobowy monitoring video dostępu do biura Fundacji,
c. zabezpieczenie pomieszczeń biurowych poprzez stosowanie atestowanych zamków,
d. zaawansowany elektroniczny system alarmowy,
e. system kontroli dostępu oparty na kartach magnetycznych i czytnikach,
f. ścisłe restrykcje dotyczące przebywania osób postronnych na terenie firmy.

POLITYKA BEZPIECZEŃSTWA

Zasady ogólne polityki bezpieczeństwa

1. Ochrona danych przetwarzanych w Fundacji Pomagam obowiązuje wszystkie osoby, które mają dostęp do informacji zbieranych, przetwarzanych oraz przechowywanych w Fundacji, bez względu na zajmowane stanowisko oraz miejsce wykonywania jak również charakter stosunku pracy, osoby mające dostęp do danych osobowych są zobligowane do stosowania niezbędnych środków zapobiegających ujawnieniu tych danych osobom nieupoważnionym, zachowanie tajemnicy obowiązuje zarówno podczas trwania stosunku pracy jak i po jego ustaniu,

2. Zarząd Fundacji jest odpowiedzialny za :
   a) tworzenie, wdrażanie, administrację i interpretację polityki bezpieczeństwa informacji,
   b) tworzenie standardów, zaleceń oraz procedur w całym systemie organizacji,
   c) polecenia osób delegowanych i wyznaczonych przez Zarząd Fundacji do działań związanych z ochroną w zakresie ochrony informacji i bezpieczeństwa systemu informatycznego muszą być bezwzględnie wykonywane przez wszystkich pracowników i użytkowników systemu,
   d) dostęp do pomieszczeń, w których przetwarzane są dane osobowe oraz do pomieszczeń, w których znajdują się serwery baz danych lub przechowywane są kopie zapasowe mogą mieć wyłącznie osoby, które posiadają do tego upoważnienie wydane przez Zarząd Fundacji,
   e) za bezpieczeństwo informacji w Fundacji odpowiada każdy właściciel zasobów na swoim stanowisku pracy,
   f) w przypadku zlecania przetwarzania danych osobowych podmiotom zewnętrznym administrator danych zobowiązany jest zawrzeć umowę powierzenia, zaś w jednostce prowadzony jest rejestr umów powierzenia przetwarzania danych osobowych.

g) Na podstawie niniejszej Polityki zostały sformułowane poszczególne cele w zakresie bezpieczeństwa informacji. Są one realizowane poprzez odpowiednie polityki i inne zabezpieczenia, które w szczególności obejmują:

h) zapewnienie przeszkolenia i podniesienie świadomości pracowników w zakresie bezpieczeństwa informacji,
   - przedstawienie pracownikom konsekwencji wynikających z naruszenia bezpieczeństwa informacji,
   - zapewnienie ciągłości działania dostępu do informacji,
   - monitorowanie, zarządzanie i raportowanie o incydentach związanych z bezpieczeństwem informacji,
   - szacowanie ryzyka będzie stałym elementem naszego działania,
   - stałe udoskonalanie wdrożonego Systemu Zarządzania Bezpieczeństwem Informacji poprzez systematyczne szkolenia personelu w zakresie bezpieczeństwa danych i przedsiębiorstwa, aktualizację procedur i instrukcji, wynikającą z rozwoju i powstawania produktów oferowanych przez Fundację,
   - zakomunikowanie niniejszej Polityki Bezpieczeństwa Informacji pracownikom i osobom współpracującym w organizacji.

Rejestr czynności przetwarzania

Administrator danych prowadzi rejestr czynności przetwarzania. W rejestrze tym zamieszcza się:

a) dane oraz dane kontaktowe administratora,
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) gdy ma to zastosowanie, informacje na temat przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej, w tym nazwę tego państwa trzeciego lub organizacji międzynarodowej, a w przypadku przekazań, o których mowa w art. 49 ust. 1 akapit drugi RODO, dokumentację odpowiednich zabezpieczeń,
f) jeżeli jest to możliwe, planowane terminy usunięcia poszczególnych kategorii danych,
g) jeżeli jest to możliwe, ogólny opis technicznych i organizacyjnych środków bezpieczeństwa, o których mowa w art. 32 ust. 1 RODO.

Procedura postępowania z incydentami

Administrator danych wprowadza do stosowania procedurę postępowania z incydentami naruszenia ochrony danych osobowych. Celem tej procedury jest wypełnienie obowiązku wynikającego z art. 33 RODO. Procedura określa sposób definiowania incydentów zagrażających bezpieczeństwu danych osobowych oraz sposób reagowania na nie, a także procedurę wprowadzenia działań naprawczych. Każda osoba upoważniona do przetwarzania danych osobowych ma obowiązek poinformowania o możliwości wystąpienia incydentu lub o jego wystąpieniu. Taka informacja powinna być przekazana bezpośredniemu przełożonemu.

Powiadomienia wymagają:

a) niewłaściwe zabezpieczenie sprzętu elektronicznego, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych, udostępnienie haseł osobom postronnym,
b) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
c) nieprzestrzeganie zasad ochrony danych osobowych przez pracowników (np. niestosowanie zasady czystego biurka/ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek, przyklejanie kartek z hasłami w szufladach),
d) ślady na drzwiach, oknach i szafach wskazujące na próbę włamania,
e) dokumentacja zawierająca dane osobowe niszczona bez użycia niszczarki,
f) otwarte drzwi do pomieszczeń, szaf, gdzie przechowywane są dane osobowe,
g) obecność osób postronnych w jednostce,
h) złe ustawienie monitorów pozwalające na wgląd osób postronnych w dane osobowe,
i) wynoszenie danych osobowych w wersji papierowej i elektronicznej na zewnątrz jednostki bez upoważnienia administratora danych,
j) awarie serwera, komputerów, twardych dysków, oprogramowania,
k) udostępnienie danych osobowych osobom nieupoważnionym,
l) telefoniczne próby wyłudzenia danych osobowych,
m) kradzież, zagubienie komputerów lub CD, twardych dysków, pendrive z danymi osobowymi,
n) maile nakłaniające do ujawnienia identyfikatora lub hasła,
o) zainfekowanie komputerów wirusem lub inne błędne zachowanie komputerów,
p) zdarzenia losowe (pożar obiektu, zalanie wodą, utrata zasilania, utrata łączności),
q) włamanie do systemu informatycznego lub pomieszczeń,
r) kradzież danych/sprzętu,
s) świadome zniszczenie dokumentów.

Należy również powiadomić administratora systemów informatycznych. Ponadto należy udokumentować wystąpienie incydentu, jego skutki oraz podjęte działania naprawcze i zaradcze. W przypadku, gdy incydent skutkuje naruszeniem praw lub wolności osób fizycznych, administrator

danych zgłasza je w ciągu 72 godzin Prezesowi Urzędu Ochrony Danych Osobowych oraz gdy istnieje taki wymóg, powiadamia o tym fakcie osoby, których incydent dotyczył.

FUNDACJA
POMAGAM
ul. Piramowicza 9, 90 254 Łódź
tel. 42 6300900 email: biuro@fundacjapomagam.pl
REGON: 100334258 NIP: 7251941933
Konto: 86 1140 1108 0000 2052 2800 1001