POLITYKA BEZPIECZEŃSTWA PRZETWARZANIA DANYCH OSOBOWYCH

Fundacja Pro NGO

1. WSTĘP

1.1. INFORMACJE OGÓLNE

1. Wskazanie Administratora Danych, który wdraża Politykę Bezpieczeństwa.

2. Wyjaśnienie celu wprowadzania dokumentu.

   Głównym celem wprowadzenia Polityki Bezpieczeństwa jest zapewnienie zgodności działania Administratora Danych z Rozporządzeniem Parlamentu Europejskiego i Rady (UE)2016/679 z 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 – Dz.Urz. UE L 119, s. 1 (dalej RODO), ustawą o ochronie danych osobowych oraz z rozporządzeniami wykonawczymi do ustawy.

3. Wskazanie podstaw prawnych.

   Dokument Polityki Bezpieczeństwa został opracowany w oparciu o wytyczne zawarte w następujących aktach prawnych:

   - rozporządzenie Parlamentu Europejskiego i Rady (UE)2016/679 z 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 – Dz.Urz. UE L 119, s 1
   - ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (t.j. Dz.U. z 2018 r., poz. 1000)

1.2. ZAKRES INFORMACJI OBJĘTYCH POLITYKĄ BEZPIECZEŃSTWA ORAZ ZAKRES ZASTOSOWANIA

1. Dokument Polityki Bezpieczeństwa opisuje zasady i procedury przetwarzania danych osobowych i ich zabezpieczenia przed nieuprawnionym dostępem.
2. Na Politykę Bezpieczeństwa składają się następujące informacje:
   1) wykaz zbiorów danych osobowych wraz ze wskazaniem programów zastosowanych do przetwarzania tych danych,
   2) opis struktury zbiorów danych wskazujący zawartość poszczególnych pól informacyjnych i powiązania między nimi,
   3) sposób przepływu danych pomiędzy poszczególnymi systemami,

5) określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych.

1.3. WYJAŚNIENIE TERMINÓW UŻYWANYCH W DOKUMENC IE POLITYKI BEZPIECZEŃSTWA

Polityka Bezpieczeństwa posługuje się następującymi terminami, których znaczenie jest następujące:

1) **ustawa** – ustawa z dnia r. o ochronie danych osobowych ( ), oraz przepisy wykonawcze wydane na podstawie delegacji ustawowej zwane dalej „ustawą",
2) **dane osobowe** – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej,
3) **przetwarzanie danych** – jakiekolwiek operacje wykonywane na danych osobowych, takie jak: zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie, a zwłaszcza te, które wykonuje się w systemach informatycznych,
4) **poufność danych** – właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym podmiotom.

2. OSOBY ODPOWIEDZIALNE ZA OCHRONĘ DANYCH OSOBOWYCH

2.1. INFORMACJE OGÓLNE

1) Punkt ten wskazuje osoby odpowiedzialne za przetwarzanie danych osobowych oraz ich ochronę zgodnie z postanowieniami RODO, Ustawy, Polityki Bezpieczeństwa oraz załączników do niej.
2) Osoby wykonujące pracę bądź świadczące usługi cywilnoprawne na rzecz Administratora Danych Osobowych, która uzyskała upoważnienie do przetwarzania danych osobowych.

2.2. ADMINISTRATOR DANYCH

1. Podrozdział wskazuje, kto jest Administratorem Danych i jakie są jego obowiązki.
2. Administrator danych: Fundacja Pro NGO z siedzibą w Krakowie przy ul. T. Chałubińskiego 18, KRS: 0000846484, NIP: 6793200954.
3. Obowiązki Administratora Danych:
   1) spełnienie wskazanych w ustawie przesłanek legalizujących przetwarzanie danych osobowych;

2) obowiązek informacyjny związany z pozyskaniem danych;
3) obowiązek dochowania szczególnej staranności przy przetwarzaniu danych, w celu ochrony interesów osób, których dane dotyczą;
4) obowiązek zabezpieczenia danych;
5) obowiązek prowadzenia dokumentacji związanej z przetwarzaniem danych osobowych;
6) obowiązek prowadzenia rejestru przetwarzania danych.

2.3. INSPEKTOR OCHRONY DANYCH

1. Wyznaczenie Inspektora Ochrony Danych jest czynnością Administratora Danych. Administrator Danych powołał na tę funkcję Grzegorza Ludwina.
2. Określono następujące uprawnienia i obowiązki Inspektora Ochrony Danych, zgodne z art. 39 RODO:

a) informowanie Administratora, podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy niniejszego rozporządzenia oraz innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie;

b) monitorowanie przestrzegania niniejszego rozporządzenia, innych przepisów Unii lub państw członkowskich o ochronie danych oraz polityk administratora lub podmiotu przetwarzającego w dziedzinie ochrony danych osobowych, w tym podział obowiązków, działania zwiększające świadomość, szkolenia personelu uczestniczącego w operacjach przetwarzania oraz powiązane z tym audyty;

c) udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;

d) współpraca z organem nadzorczym i udział w kontrolach prowadzonych przez organ nadzoru;

e) pełnienie funkcji punktu kontaktowego dla organu nadzorczego w kwestiach związanych z przetwarzaniem;

f) stały nadzór nad treścią Polityki Bezpieczeństwa;

g) czynności sprawdzania zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych oraz opracowania sprawozdania;

h) prowadzenie jawnego rejestru zbiorów danych osobowych;

i) udzielanie odpowiedzi na zapytania kierowane do Administratora Danych przez podmioty zewnętrzne, dotyczące administrowanych zbiorów danych osobowych;

j) nadawanie poszczególnym pracownikom upoważnień do przetwarzania danych osobowych oraz przeprowadzanie dla nich szkoleń z zakresu ochrony danych osobowych w trybie określonym w Rozdziale 3 niniejszej Polityki Bezpieczeństwa;

k) nadzór nad nadawaniem uprawnień do przetwarzania danych osobowych w systemach informatycznych;

l) prowadzenie aktualnej ewidencji osób upoważnionych do przetwarzania danych osobowych we wszystkich zbiorach oraz nadzór nad prowadzeniem rejestru nadanych uprawnień do przetwarzania danych w systemach informatycznych;

m) nadzór nad fizycznym zabezpieczeniem obszarów, w których przetwarzane są dane osobowe;

n) monitorowanie działania i skuteczności zabezpieczeń wdrożonych w celu ochrony danych osobowych.

2.4. OSOBY UPOWAŻNIONE DO PRZETWARZANIA DANYCH OSOBOWYCH

1. Każda osoba, która uzyskała upoważnienie do przetwarzania danych osobowych, zobowiązana jest do ich ochrony w sposób zgodny z przepisami RODO, Ustawy, Polityki Bezpieczeństwa oraz załączników do niej.
2. Osoba upoważniona zobowiązana jest do zachowania w tajemnicy danych osobowych oraz sposobów ich zabezpieczenia. Obowiązek ten istnieje także po ustaniu zatrudnienia lub wykonywania usług na podstawie umowy cywilnoprawnej.

3. ZAKRES PPRZETWARZANIA I CELE WYKORZYSTANIA DANYCH OSOBOWYCH

1. W zbiorach danych gromadzonych w systemie informatycznym zabrania się przetwarzania danych ujawniających:
   a) stan zdrowia,
   b) pochodzenie rasowe lub etniczne,
   c) poglądy polityczne,
   d) przekonania religijne lub filozoficzne,
   e) przynależność wyznaniową,
   f) przynależność partyjną lub związkową,
   g) dane genetyczne,
   h) dane biometryczne,
   i) nałogi,
   j) preferencje seksualne

   chyba że wymagają tego obowiązujące przepisy prawa lub osoba, której dane dotyczą, wyraziła na to pisemną zgodę.
2. Dane o skazaniach, w tym dane o niekaralności można przetwarzać jedynie zgodnie z art. 10 RODO.
3. W jednostce zabrania się używania danych wymienionych w pkt 1 do profilowania, o ile osoba, której dane dotyczą, wyraziła na to zgodę lub jest to podyktowane ważnym interesem publicznym. O profilowaniu Administrator Danych informuje osobę, której ono dotyczy, na etapie zbierania danych.
4. Dane osobowe mogą być wykorzystywane wyłącznie do celów, dla jakich były, są lub będą zbierane i przetwarzane. Po wykorzystaniu dane osobowe powinny być przechowywane w formie zanonimizowanej, uniemożliwiającej identyfikację osób, których dotyczą.
5. Administrator Danych lub upoważniony przez niego IOD ma obowiązek uzupełnienia, uaktualnienia, sprostowania lub usunięcia danych osobowych w przypadku, gdy dane osobowe osoby, od której zostały

zebrane, są niekompletne, nieaktualne, nieprawdziwe, zostały zebrane z naruszeniem ustawy lub są zbędne do realizacji celu, dla którego zostały zebrane, ADO lub osoba przez niego upoważniona.

4. UPOWAŻNIENIE DO PRZE TWARZANIA DANYCH OSOBOWYCH

1. Niniejszy punkt zawiera opis zasad przyznawania użytkownikowi identyfikatora w systemie informatycznym, jak również zasady nadawania lub modyfikacji uprawnień użytkownika do zasobów systemu informatycznego.
2. Powyższe zasady obejmują operacje związane z nadawaniem użytkownikom uprawnień do pracy w systemie informatycznym, począwszy od utworzenia użytkownikowi konta, poprzez przydzielanie i modyfikację jego uprawnień aż do momentu usunięcia konta z systemu informatycznego.
3. Wszystkie osoby, które przetwarzają dane osobowe, muszą posiadać pisemne upoważnienie do przetwarzania danych oraz podpisać oświadczenie o zachowaniu poufności tych danych.
4. Operacje szczegółowe:
    1) Upoważnienie do przetwarzania danych nadaje Inspektor Ochrony Danych: Grzegorz Ludwin
    2) Upoważnienie nadawane jest na wniosek Zarządu Administratora Danych;
    3) Forma upoważnienia - forma pisemna (Załącznik nr 2 do Polityki Bezpieczeństwa);
    4) Zakres nadanych uprawnień zależny od stanowiska i funkcji pracownika lub współpracownika;
    5) Upoważnienia rejestruje Inspektor Ochrony Danych;
    6) Rejestr nadanych uprawnień prowadzony jest w formie elektronicznej (Excel).

5. UMOWY POWIERZENIA PRZETWARZANIA DANYCH OSOBOWYCH

Spółka zawiera umowy powierzenia przetwarzania danych osobowych podmiotom zewnętrznym, w zakresie niezbędnym do wykonywania czynności administracyjnych jak i formalnoprawnych, m.in. firmie księgowej, podmiotom świadczącym hosting poczty elektronicznej , towarzystwom ubezpieczeniowym i innym.

6. ANALIZA ZAGROŻEŃ I RYZYKA PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Analiza zagrożeń i ryzyka jest głównym elementem procesu zarządzania ryzykiem bezpieczeństwa informacji. Jej celem jest wdrożenie odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie odbywało się zgodnie z RODO.
2. Ze względu na zmieniające się warunki funkcjonowania jednostki analiza ryzyka musi być wykonywana okresowo, przynajmniej raz w roku, przez IOD.
3. Analiza zidentyfikowanego zagrożenia i ryzyka polega na oszacowaniu prawdopodobieństwa jego wystąpienia i skutku jego ewentualnego wystąpienia.

7. OGÓLNE ZASADY BEZPIECZEŃSTWA OBOWIĄZUJĄCE PRZY PRZETWARZANIU DANYCH OSOBOWYCH

1. Postanowienia dotyczące ogólnych zasad przetwarzania danych:
   1) Za bezpieczeństwo przetwarzania danych osobowych w określonym zbiorze indywidualną odpowiedzialność ponosi przede wszystkim każdy pracownik mający dostęp do danych;
   2) Pracownicy mający dostęp do danych osobowych nie mogą ich ujawniać zarówno w miejscu pracy, jak i poza nim, w sposób wykraczający poza czynności związane z ich przetwarzaniem w zakresie obowiązków służbowych, w ramach udzielonego upoważnienia do przetwarzania danych;
   3) W miejscu przetwarzania danych osobowych utrwalonych w formie papierowej pracownicy zobowiązani są do stosowania zasady tzw. czystego biurka. Zasada ta 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;
   4) Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się w sposób uniemożliwiający odczytanie zawartej w nich treści, np. z wykorzystaniem niszczarek;
   5) Niedopuszczalne 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;
   6) Przebywanie osób nieuprawnionych w pomieszczeniu, w którym przetwarzane są dane osobowe, jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania danych osobowych, chyba że dane te są w odpowiedni sposób zabezpieczone przed dostępem;

7) Pracownicy zobowiązani są do zamykania na klucz wszelkich pomieszczeń lub budynków wchodzących w skład obszarów, w których przetwarzane są dane osobowe w czasie ich chwilowej nieobecności w pomieszczeniu pracy, jak i po jej zakończeniu, a klucze nie mogą być pozostawione w zamku w drzwiach. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem;
8) Dokumenty o szczególnym znaczeniu przechowywane są w szafie pancernej, a dostęp do nich ma Zarząd Administratora Danych;
9) Osoby uprawnione do przetwarzania danych w formie elektronicznej (komputerowej) uzyskują dostęp do danych za pomocą nadanego im indywidualnego hasła przez Inspektora Ochrony Danych;
10) W przypadku niekorzystania z komputera przez osobę uprawnioną do przetwarzania danych przez Okres 5 minut następuje blokada dostępu do danych i osoba taka może uzyskać dostęp do danych po ponownym wprowadzeniu hasła;
12) Hasła dostępu są zmieniane okresowo, ale nie rzadziej niż co 6 miesięcy .
13) Wszystkie komputery połączone są w sieć komputerową, która posiada odpowiednie zabezpieczenia antywirusowe oraz zabezpieczenia uniemożliwiające dostęp do sieci bez uprawnień (firewall);
14) Wszystkie komputery oraz serwery podlegają okresowym przeglądom antywirusowym.

8. OBOWIĄZKI INFORMACYJNE PRZY ZBIERANIU DANYCH OSOBOWYCH

1. W przypadku zbierania danych osobowych od osoby, której one dotyczą, Administrator Danych jest obowiązany poinformować tę osobę o:
   a) swojej tożsamości i podać dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
   b) gdy ma to zastosowanie - dane kontaktowe Inspektora Ochrony Danych;
   c) cele przetwarzania danych osobowych oraz podstawę prawną przetwarzania;
   d) prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią ;
   e) informacje o 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 oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, wzmiankę 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) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

i) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO- informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

j) informacje o prawie wniesienia skargi do organu nadzorczego;

k) informację, 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) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

2. W przypadku pozyskania danych osobowych z innego źródła, niż osoba, której dane dotyczą, Administrator Danych jest zobowiązany poinformować tę osobę o:

a) swojej tożsamości i podać dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;

b) gdy ma to zastosowanie - dane kontaktowe Inspektora Ochrony Danych;

c) cele przetwarzania, do których mają posłużyć dane osobowe oraz podstawę prawną przetwarzania;

d) kategorie odnośnych danych osobowych;

e) informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;

f) gdy ma to zastosowanie - informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę 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) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. f) RODO - prawnie uzasadnione interesy realizowane przez Administratora lub przez stronę trzecią;

i) informacje o prawie do żądania od Administratora dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;

j) jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO - informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;

k) informacje o prawie wniesienia skargi do organu nadzorczego;

f) źródło pochodzenia danych osobowych, a gdy ma to zastosowanie - czy pochodzą one ze źródeł publicznie dostępnych;

g) informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz - przynajmniej w tych przypadkach - istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

3. Obowiązek poinformowania wymieniony w pkt 1 niniejszego paragrafu powinien być wykonany w momencie zbierania danych z wyjątkiem sytuacji, w której Administrator planuje dalej 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 oraz udziela jej wszelkich innych stosownych informacji.

4. Obowiązek poinformowania wymieniony w pkt 2 niniejszego paragrafu powinien zostać spełniony bezpośrednio po utrwaleniu zebranych danych, a więc po zapisaniu danych w sposób umożliwiający ich dalsze przetwarzanie z wyjątkiem sytuacji, w której:
   a) w rozsądnym terminie po pozyskaniu danych osobowych - najpóźniej w ciągu miesiąca - mając na uwadze konkretne okoliczności przetwarzania danych osobowych;

   b) jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą - najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub

   c) jeżeli planuje się ujawnić dane osobowe innemu odbiorcy - najpóźniej przy ich pierwszym ujawnieniu.

9. INSTRUKCJA POSTĘPOWANIA W SYTUACJI NARUSZENIA OCHRONY DANYCH OSOBOWYCH

1. Administrator Danych zobowiązany jest do stworzenia ogólnego trybu postępowania w sytuacji naruszenia ochrony danych osobowych, który odpowiada organizacji pracy pracowników lub specjalizacji prowadzonej działalności.
2. Instrukcja postępowania w sytuacji naruszenia ochrony danych osobowych:
   1) Każda osoba, która poweźmie wiadomość w zakresie naruszenia bezpieczeństwa danych przez osobę przetwarzającą dane osobowe, bądź posiada informacje mogące mieć wpływ na bezpieczeństwo danych osobowych, jest zobowiązana fakt ten niezwłocznie zgłosić Inspektorowi Ochrony Danych;
   2) Do czasu przybycia na miejsce naruszenia ochrony danych osobowych Inspektora Ochrony Danych, osoba powiadamiająca powinna:

- niezwłocznie podjąć czynności niezbędne do powstrzymania niepożądanych skutków, a następnie ustalić przyczyny lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe,
- zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę,
- udokumentować wstępnie zaistniałe naruszenie,

- nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia do czasu przybycia Inspektora Ochrony Danych lub osoby upoważnionej;

3) Po przybyciu na miejsce naruszenia ochrony danych osobowych Inspektor Ochrony Danych lub osoba go zastępująca:

zapoznaje się z zaistniałą sytuacją i dokonuje wyboru metod dalszego postępowania,

wysłuchuje relacji osoby zgłaszającej z zaistniałego naruszenia, jak również relacji każdej innej osoby, która może posiadać informacje związane z zaistniałym naruszeniem;

4) Inspektor Ochrony Danych dokumentuje zaistniały przypadek naruszenia oraz sporządza raport. Raport, o którym mowa powyżej, Inspektor Ochrony Danych niezwłocznie przekazuje zarządowi jednostki;

5) Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu Inspektor Ochrony Danych zasięga niezbędnych opinii i proponuje postępowanie naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych;

6) 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 organowi nadzorczemu, 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.

10. KONTROLA PRZETWARZANIA I STANU ZABEZPIECZENIA DANYCH OSOBOWYCH

1. Niniejszy rozdział reguluje system kontroli przetwarzania i stanu zabezpieczenia danych osobowych, kto jest odpowiedzialny za ich przeprowadzenie i jak często należy badać stan zabezpieczeń.
2. Nadzór i kontrolę nad ochroną danych osobowych przetwarzanych w Fundacji Pro NGO sprawuje Inspektor Ochrony Danych - w odniesieniu do danych osobowych przetwarzanych w systemach informatycznych służących do przetwarzania danych osobowych.
3. Czynności kontrolne przeprowadzane są co pół roku przed końcem maja i listopada każdego roku;
4. Z czynności kontrolnych sporządzany jest protokół, w którym dokonuje się dokładnego opisu zakresu kontroli i przeprowadzonych czynności;
5. Protokół podpisywany jest przez osoby wykonujące czynności kontrolne. Dołącza się go do dokumentacji przechowywanej u Inspektora Ochrony Danych;
6. Wzór protokołu z kontroli lub czynności sprawdzających, o których mowa w niniejszym Rozdziale stanowi Załącznik nr 10 do niniejszej Polityki.

11. OPIS STRUKTURY ZBIOR ÓW DANYCH

1. Dla każdego zidentyfikowanego zbioru danych wskazany jest opis struktury zbioru i zakres informacji gromadzonych w danym zbiorze.
2. Opisy poszczególnych pól informacyjnych gromadzonych w strukturze zbioru danych wskazuje, jakie kategorie danych są w nich przechowywane.
3. Opis pola danych w przypadkach, gdy możliwa jest jednoznaczna interpretacja jego zawartości, wskazuje nie tylko kategorie danych, ale również format zapisu.
4. Przez format zapisu należy rozumieć program informatyczny lub przetwarzanie w formie papierowej.
5. W identyfikacja zbioru danych opiera się o kryterium klienta (firmy), któremu świadczone są usługi.

6. Przetwarzanie danych ma formę komputerową oraz papierową ze względu na wymogi przepisów o rachunkowości. Papierowa forma przetwarzania danych osobowych służy głównie narzuconym ustawowo celom archiwizacji.
7. Opis struktury zbiorów danych sporządzono w formie tabelarycznej. Stanowi on Załącznik nr 5 do niniejszej Polityki Bezpieczeństwa.

12. SPOSÓB PRZEPŁYWU DAN YCH OSOBOWYCH POMIĘDZY SYSTEMAMI INFORMATYCZNYMI

W punkcie tym przedstawiono sposób współpracy pomiędzy różnymi systemami informatycznymi oraz relacje, jakie istnieją pomiędzy danymi zgromadzonymi w zbiorach, do których systemy te są wykorzystywane. Określić systemy, jakimi dane są przesyłane i formy przesyłu (chmura, hosting), określić zbiory danych przesyłane

13. OBSZAR W KTÓRYM PRZE TWARZANE SA DANE OSOBOWE

1. Określenie struktury pomieszczeń, w których przetwarzane są dane osobowe, obejmuje zarówno miejsca, w którym wykonuje się operacje na danych osobowych (wpisuje, modyfikuje, kopiuje), jak również miejsca, gdzie przechowuje się wszelkie nośniki informacji zawierające dane osobowe.

14. ŚRODKI TECHNICZNE I ORGANIZACYJNE NIEZBĘ DNE DLA ZAPEWNIENIA POUF NOŚCI, INTEGRALNOŚCI I ROZLICZALNOŚCI PRZETWARZANYCH DANYCH OSOBOWYCH

Fundacja Pro NGO dysponuje środkami technicznymi i organizacyjnymi, które zostały zastosowane przez Administratora Danych w celu zapewnienia odpowiedniego poziomu bezpieczeństwa przetwarzania a także dla zagwarantowania poufności, integralności i rozliczalności przetwarzanych danych osobowych.

Załączniki:

Załącznik nr 1 – Ustanowienie Inspektora Ochrony Danych
Załącznik nr 2 – Upoważnienie Inspektora Ochrony Danych do nadawania upoważnień
Załącznik nr 3 – Wzór upoważnienia do przetwarzania danych osobowych dla osób zatrudnionych na podstawie umowy o pracę
Załącznik nr 4 – Wzór oświadczenia o zobowiązaniu się do zachowania poufności
Załącznik nr 5 – Opis struktury zbiorów danych Administratora Danych
Załącznik nr 6 – Opis struktury zbiorów danych podmiotów przetwarzających
Załącznik nr 7 - Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych
Załącznik nr 8 – Wzór zgody na przetwarzanie danych osobowych
Załącznik nr 9 – Opis środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych
Załącznik nr 10 – Protokół z kontroli przetwarzania i stanu zabezpieczenia danych osobowych/czynności sprawdzających
Załącznik nr 11 - Ewidencja udostępnień danych osobowych innym podmiotom
Załącznik nr 12 – Wzór oświadczenia o zapoznaniu się z Polityką Bezpieczeństwa
Załącznik nr 13 – Wzór ewidencji incydentów w ochronie danych osobowych Załącznik nr 14 – Protokół incydentu w ochronie danych osobowych

Dokument sporządzono: Kraków, dnia 15.01.2020 r.	**Pełen podpis Administratora Danych:**	**Pieczęć**