FUNDACJA FORMY

Załącznik nr 2 do Uchwały Zarządu Fundacji FORMY z dnia 17 marca 2025 r.

POLITYKA BEZPIECZEŃSTWA DANYCH OSOBOWYCH

Spis treści

FUNDACJA FORMY

1. Cel i zakres dokumentu

1. Celem Polityki Bezpieczeństwa jest zapewnienie bezpieczeństwa danych osobowych poprzez wskazanie odpowiednich rozwiązań technicznych i organizacyjnych oraz określenie obowiązków i odpowiedzialności osób zobowiązanych do przetwarzania danych osobowych, przy jednoczesnym spełnieniu wszelkich wymogów obowiązującego prawa.

2. W dokumencie tym zawarto najważniejsze zasady, zgodnie z którymi realizowany jest proces ochrony informacji zawierających dane osobowe przetwarzane w Fundacji FORMY (dalej zwanej: „Fundacją").

3. Zasady określone w Polityce mają zastosowanie do wszystkich danych osobowych zawartych w zbiorach danych, jak również poza nimi, przetwarzanych w systemach informatycznych oraz w sposób tradycyjny, których Fundacja jest Administratorem lub Podmiotem przetwarzającym.

2. Dokumenty związane

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016 r.).

2. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2019 poz. 1781 z późn. zm.).

3. Instrukcja zarządzania systemami Informatycznymi.

3. Definicje i Skróty

Administrator Danych Osobowych lub ADO – Fundacja FORMY, z siedzibą w Częstochowie 42-202 przy ul. Wypalanki, reprezentowana przez Zarząd.

Dane osobowe – informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej (zgodnie z RODO).

Dostępność informacji – zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy istnieje taka potrzeba, tzn. w odpowiednim zakresie, miejscu i czasie).

Inspektor Ochrony Danych lub IOD – osoba wyznaczona przez Administratora Danych Osobowych do nadzorowania oraz przestrzegania zasad ochrony Danych osobowych, w tym wykonywania zadań, o których mowa w art. 39 RODO. W przypadku niepowołania IOD, czynności jemu przypisane wykonuje Administrator Danych Osobowych.

Integralność informacji – właściwość zapewniająca dokładność i kompletność informacji oraz metod jej przetwarzania.

Incydent bezpieczeństwa – zdarzenie lub seria zdarzeń, które bezpośrednio zagraża bezpieczeństwu informacji ze względu na poufność, dostępność i integralność informacji.

Naruszenie ochrony Danych osobowych – incydent bezpieczeństwa prowadzący do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

Odbiorca danych – osoba fizyczna lub prawna, organ publiczny, jednostka 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 postepowania zgodnie z powszechnie obowiązującym prawem, nie są uznawane za odbiorców.

Organ nadzorczy – Prezes Urzędu Ochrony Danych Osobowych lub ewentualnie właściwy organ nadzorczy w zakresie Danych osobowych, wyznaczony przez inne państwo członkowskie Unii Europejskiej.

Osoba upoważniona – osoba upoważniona przez ADO do przetwarzania Danych osobowych w Fundacji za pomocą pisemnego Upoważnienia. Podmiot danych – osoba fizyczna, której dotyczą Dane osobowe przetwarzane przez Administratora.

Podmiot przetwarzający lub Procesor – osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu administratora. Poufność informacji – zapewnienie o nieudostępnianiu i nieujawnianiu danych nieautoryzowanym osobom, podmiotom lub procesom.

Polityka – niniejsza Polityka Bezpieczeństwa Danych Osobowych.

Profilowanie – dowolna forma zautomatyzowanego przetwarzania Danych osobowych, które 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.

Przetwarzanie – operacja lub zestaw operacji wykonywanych na Danych osobowych lub zestawach Danych osobowych, w sposób zautomatyzowany lub niezautomatyzowany, takie jak: zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie, modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie, udostępnianie, dopasowywanie, łączenie, ograniczanie, usuwanie lub niszczenie.

Pseudonimizacja – 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.

RODO – ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych). Ryzyko – prawdopodobieństwo wykorzystania przez określone zagrożenie podatności aktywów, czego skutkiem mogą być określone straty. Ryzyko można opisać jako prawdopodobieństwo wystąpienia niepożądanego incydentu oraz związanych z nim następstw.

System informatyczny – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych, poczty elektronicznej, gdzie dochodzi do przetwarzania Danych osobowych.

Tradycyjny nośnik informacji – przedmiot fizyczny niezwiązany z informatyką i komputerami, na którym możliwe jest zapisanie informacji oraz z którego możliwe jest późniejsze odczytanie tej informacji. Przykładami tradycyjnych nośników mogą być wydruki papierowe, folia, taśmy itp.

Usuwanie danych – nieodwracalne zniszczenie Danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą. Strona 5 z 21 Użytkownik Systemu Informatycznego lub (USI) – osoba upoważniona do dostępu do zasobów Systemu informatycznego posiadająca upoważnienie do przetwarzania danych osobowych w tym systemie. Użytkownikami są podwykonawcy oraz pracownicy etatowi Fundacji. Uwierzytelnianie – działanie, którego celem jest weryfikacja deklarowanej tożsamości podmiotu. Zagrożenie – potencjalna przyczyna niepożądanego incydentu/naruszenia, którego skutkiem może być szkoda dla systemu bądź aplikacji przetwarzającej Dane osobowe. Każda sytuacja, która powoduje niedostępność danych (czasowa lub trwała), uniemożliwienie przetwarzania danych, niekontrolowany wypływ, ujawnienie, utratę lub przekłamanie – jest zagrożeniem dla przetwarzanych danych, niezależnie od tego czy stanowiła celowy sabotaż, czy przypadkowe działanie.

Zbiór Danych osobowych – uporządkowany zestaw Danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Zgoda (osoby, której dane dotyczą) – 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.

4. Postanowienia ogólne

1. Niniejsza Polityka stanowi podstawowy dokument regulujący zasady przetwarzania Danych osobowych przez Administratora.

2. Wdrożenie Polityki ma na celu zapewnienie zgodności z RODO procesów przetwarzania Danych osobowych przez Administratora, bez względu na formę (elektroniczną bądź papierową), w jakiej to przetwarzanie następuje.

3. W związku z prowadzoną działalnością Administrator zbiera i przetwarza Dane osobowe zgodnie z właściwymi przepisami prawa, w tym w szczególności RODO i przewidzianymi w nich zasadami przetwarzania, tj.:

a) Administrator zapewnia, że przetwarzanie przez niego Danych osobowych jest zgodne z prawem i odbywa się w oparciu o jedną z podstaw przetwarzania określonych w RODO, tj. w art. 6 ust. 1, art. 9 ust. 2 albo art. 10 (zasada zgodności z prawem);

b) Administrator zapewnia rzetelność i przejrzystość przetwarzania Danych osobowych, w szczególności zawsze informuje o przetwarzaniu Danych osobowych w momencie ich zbierania, w tym o celu i podstawie prawnej przetwarzania (zasada rzetelności i przejrzystości);

c) Administrator zapewnia, że Dane osobowe są zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nie są przetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczenia celu);

d) Administrator zapewnia, że przetwarza dane wyłącznie w zakresie niezbędnym do realizacji celu, dla którego Dane osobowe zostały zebrane (zasada minimalizacji);

e) Administrator zapewnia, że przetwarzane przez niego Dane osobowe są prawidłowe i w razie potrzeby uaktualniane oraz że podejmuje on wszelkie rozsądne działania, aby Dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane (zasada prawidłowości);

f) Administrator zapewnia, że Dane osobowe są przetwarzane tylko przez okres, w jakim jest to niezbędne dla zrealizowania celów przetwarzania (zasada ograniczenia czasowego);

g) Administrator zapewnia bezpieczeństwo Danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, poprzez wdrożenie odpowiednich środków technicznych lub organizacyjnych (zasada integralności i poufności).

4. Administrator poprzez odpowiednie środki techniczne i organizacyjne zapewnia możliwość wykazania zgodności przetwarzania Danych osobowych z RODO oraz pozostałymi przepisami dotyczącymi Danych osobowych (rozliczalność).

5. Za stosowanie niniejszego dokumentu odpowiedzialni są wszyscy pracownicy i współpracownicy mający dostęp do Danych osobowych.

4.1. Upoważnienia do przetwarzania Danych osobowych, Oświadczenia o zachowaniu poufności

1. Przed udzieleniem dostępu do przetwarzania Danych osobowych Administrator zapoznaje każdego Pracownika, Współpracownika lub inne osoby przetwarzające Dane osobowe z jego upoważnienia z Polityką, w tym procedurami i zasadami dotyczącymi ochrony Danych osobowych obowiązującymi w organizacji Administratora

2. Do przetwarzania Danych osobowych zgromadzonych w zbiorach i ewidencjach w Fundacji mogą być dopuszczone wyłącznie osoby posiadające upoważnienie wydane przez ADO. Wzór upoważnienia do przetwarzania danych osobowych w Fundacji stanowi Załącznik nr 1 do Polityki.

3. Zmiana zajmowanego stanowiska służbowego lub komórki organizacyjnej wymaga zmiany upoważnienia, jeżeli wpływa na zakres przetwarzanych przez pracownika Danych osobowych.

4. Upoważnienie obowiązuje od daty wystawienia do dnia nadania nowego upoważnienia lub jego wygaśnięcia.

5. Upoważnienie wygasa automatycznie z chwilą rozwiązania umowy o pracę lub stosunku cywilnoprawnego, łączącego upoważnionego z Fundacją.

6. ADO prowadzi Ewidencję Osób upoważnionych do przetwarzania danych osobowych, której wzór stanowi Załącznik nr 2 do Polityki.

7. Administrator zobowiązuje osoby upoważnione do zachowania poufności Danych osobowych oraz informacji dotyczących zabezpieczeń Danych osobowych, a także do przestrzegania Polityki, w tym procedur i zasad dotyczących ochrony Danych osobowych obowiązujących w organizacji Administratora. Wzór oświadczenia określa Załącznik nr 3 do Polityki.

8. Obowiązek zachowania tajemnicy nie jest ograniczony w czasie i obowiązuje także po ustaniu stosunku pracy lub stosunku cywilnoprawnego w Fundacji i nie podlega wypowiedzeniu.

9. Każda osoba przetwarzająca dane osobowe ma obowiązek przetwarzania ich zgodnie z celem, w granicach udzielonego jej upoważnienia.

10. Każda osoba przetwarzająca dane osobowe jest zobowiązana do zachowania ich w tajemnicy oraz zapewnienia ich Poufności, Integralności i Rozliczalności.

4.2. Powierzenie przetwarzania danych osobowych

1. Rozporządzenie (art. 28) oraz Polityka przewidują możliwość powierzenia przetwarzania Danych osobowych przez ADO zewnętrznym podmiotom (Podmiotom przetwarzającym).

2. Powierzenie przetwarzania danych osobowych Podmiotowi przetwarzającemu następuje w formie pisemnej umowy powierzenia lub innego instrumentu prawnego, które podlega prawu Unii lub prawu polskiemu.

3. Przed podpisaniem umowy Podmiot przetwarzający musi zagwarantować, że wdrożył odpowiednie środki techniczne i organizacyjne celem spełnienia wymogów Rozporządzenia i innych obowiązujących przepisów prawa dotyczących ochrony danych osobowych.

4. Umowa powierzenia danych osobowych musi określać:

a. przedmiot i czas trwania przetwarzania,

b. charakter i cel przetwarzania,

c. rodzaj danych osobowych oraz kategorie osób, których dane dotyczą,

d. obowiązki i prawa ADO,

e. obowiązki Podmiotu przetwarzającego.

5. ADO na podstawie zebranych informacji, czy podmiot zewnętrzny do realizacji zleconego procesu musi przetwarzać dane osobowe – określa maksymalny zakres danych osobowych podlegających powierzeniu.

6. ADO przygotowuje Umowę powierzenia przetwarzania danych osobowych zgodnie ze wzorem umowy powierzenia przetwarzania danych osobowych stanowiącym Załącznik nr 4 do Polityki. Dopuszcza się stosowanie innego wzoru umowy powierzenia przetwarzania danych osobowych, z zastrzeżeniem, iż będzie ona zawierała wszystkie elementy wskazane w przedstawionym w załączniku wzorze.

7. Podmiot, któremu powierzono przetwarzanie danych osobowych, może przetwarzać dane wyłącznie w zakresie i celu przewidzianym w umowie.

4.3. Obowiązek informacyjny

1. Fundacja może pozyskać dane osobowe bezpośrednio od osoby, której dane dotyczą, jak i z innych źródeł w tym źródeł publicznie dostępnych.

2. Fundacja realizuje obowiązek informacyjny względem osób, których dane dotyczą, a które ma zamiar przetwarzać, zamieszczając odpowiednie klauzule informacyjne (spełniające wymagania art. 13 ust. 1 i ust. 2 Rozporządzenia) w miejscach, w których zbierane są dane osobowe.

3. W przypadku pozyskania danych osobowych nie bezpośrednio od osoby, której dane dotyczą, Fundacja informuje osobę, której dane pozyskała przedstawiając jej odpowiednią klauzulę informacyjną (spełniającą wymagania art. 14 ust. 1 i 2 Rozporządzenia) w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca.

4. Jeżeli dane osobowe pozyskane niebezpośrednio od osoby, której dotyczą mają być przetwarzane w celu komunikacji z tą osobą, odpowiednia klauzula informacyjna powinna być przedstawiona tej osobie najpóźniej przy pierwszej komunikacji z tą osobą.

5. Wzory klauzul informacyjnych dla poszczególnych kategorii osób oraz wskazanie miejsc, gdzie te klauzule należy zamieścić zawiera Załącznik nr 5 do Polityki.

6. W przypadku braku stosownej klauzuli informacyjnej dla danej kategorii osób w Załączniku nr 5 do Polityki, należy przygotować odpowiedni dokument.

4.4. Realizowanie uprawnień Podmiotów danych

1. Administrator zapewnia, że realizuje uprawnienia Podmiotów danych na zasadach określonych w RODO, w tym:

a. prawo do informacji o przetwarzaniu danych – Administrator przekazuje osobie zgłaszającej żądanie informację o przetwarzaniu Danych osobowych, w tym przede wszystkim o celach i podstawach prawnych przetwarzania, zakresie posiadanych Danych osobowych, podmiotach, którym są ujawniane, i planowanym terminie usunięcia Danych osobowych;

b. prawo uzyskania kopii danych – Administrator przekazuje osobie zgłaszającej żądanie kopię Danych osobowych, które jej dotyczą;

c. prawo do sprostowania danych – Administrator usuwa na żądanie ewentualne niezgodności lub błędy przetwarzanych Danych osobowych oraz uzupełnia je, jeśli są niekompletne;

d. prawo do usunięcia danych – Administrator na żądanie usuwa albo anonimizuje Dane osobowe, których przetwarzanie nie jest już niezbędne do realizowania żadnego z celów, dla których zostały zebrane;

e. prawo do ograniczenia przetwarzania danych – Administrator na żądanie zaprzestaje wykonywania operacji na Danych osobowych – z wyjątkiem operacji, na które Podmiot danych wyraził zgodę – oraz ich przechowywania, zgodnie z przyjętymi zasadami retencji lub dopóki nie ustaną przyczyny ograniczenia przetwarzania Danych osobowych (np. zostanie wydana decyzja Organu nadzorczego zezwalająca na dalsze przetwarzanie);

f. prawo do przenoszenia danych – w zakresie, w jakim Dane osobowe są przetwarzane w sposób zautomatyzowany w związku z zawartą umową lub wyrażoną zgodą, Administrator na żądanie wydaje Dane osobowe dostarczone przez osobę, której dotyczą, w formacie pozwalającym na odczyt Danych osobowych przez komputer;

g. prawo wniesienia sprzeciwu wobec przetwarzania danych w celach marketingowych – Podmiot danych może w każdym momencie sprzeciwić się przetwarzaniu Danych osobowych w celach marketingowych, bez konieczności uzasadnienia takiego sprzeciwu;

h. prawo sprzeciwu wobec innych celów przetwarzania danych – Podmiot danych może w każdym momencie sprzeciwić się – z przyczyn związanych z jego szczególną sytuacją – przetwarzaniu Danych osobowych, które odbywa się na podstawie prawnie uzasadnionego interesu Administratora;

i. prawo wycofania zgody – jeśli Dane osobowe przetwarzane są na podstawie wyrażonej zgody, Podmiot danych ma prawo wycofać ją w dowolnym momencie, co jednak nie wpływa na zgodność z prawem przetwarzania dokonanego przed jej wycofaniem.

2. Każde żądanie osoby, której dane dotyczą w zakresie realizacji przysługujących jej praw powinno być skonsultowane z ADO.

3. Przed udzieleniem stosownych informacji Fundacja powinna zweryfikować tożsamość osoby fizycznej składającej żądanie. W tym celu Fundacja może zażądać od tej osoby dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości.

4. Fundacja bez zbędnej zwłoki – najpóźniej w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku z żądaniem na podstawie art. 15-22 RODO. W razie potrzeby termin ten można przedłużyć o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań. W terminie miesiąca od otrzymania żądania Fundacja informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia.

5. Administrator wdraża odpowiednie środki, aby komunikacja z Podmiotem danych odbywała się w zwięzłej, przejrzystej i łatwo dostępnej formie, jasnym i prostym językiem.

6. Administrator udziela Podmiotom danych informacji na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli Podmiot danych tego zażąda, Administrator udziela informacji ustnie, o ile jest możliwe potwierdzenie tożsamości Podmiotu danych innymi sposobami.

7. Fundacja prowadzi Rejestr żądań i realizacji uprawnień osób, których dane dotyczą przy wykorzystaniu wzoru stanowiącego Załącznik nr 6 do Polityki.

4.4.1. Prawa osób trzecich

Realizując prawa osób, których dane dotyczą, Fundacja wprowadza proceduralne gwarancje ochrony praw i wolności osób trzecich. W szczególności w przypadku powzięcia wiarygodnej wiadomości o tym, że wykonanie żądania osoby, której dane dotyczą, może niekorzystnie wpłynąć na prawa i wolności innych osób (np. prawa związane z ochroną danych innych osób, prawa własności intelektualnej, tajemnicę handlową, dobra osobiste), Fundacja może się zwrócić do osoby, której dane dotyczą, w celu wyjaśnienia wątpliwości lub podjąć inne prawem dozwolone kroki, łącznie z odmową zadośćuczynienia żądaniu.

4.4.2. Nieprzetwarzanie

Fundacja informuje Podmiot danych o tym, że nie przetwarza danych jej dotyczących, jeśli taka osoba zgłosiła żądanie dotyczące jej praw.

4.4.3. Odmowa

Fundacja informuje Podmiot danych, w ciągu miesiąca od otrzymania żądania, o odmowie rozpatrzenia żądania i o prawach osoby z tym związanych.

4.4.4. Prawo do ludzkiej interwencji przy zautomatyzowanym podejmowaniu decyzji

Fundacja nie poddaje danych osobowych profilowaniu i nie podejmuje decyzji w sposób zautomatyzowany.

4.5. Uwzględnienie ochrony danych osobowych w fazie projektowania oraz domyślna ochrona danych osobowych

1. Fundacja zobowiązuje się do ochrony danych osobowych na każdym etapie ich przetwarzania począwszy od etapu tworzenia nowych projektów związanych z przetwarzaniem danych osobowych.

2. Każdy nowy projekt, którego częścią jest przetwarzanie danych osobowych (np. zakup i stosowanie nowego systemu informatycznego, serwera, aplikacji; powierzenie administrowanych danych osobowych nowemu Podmiotowi przetwarzającemu) musi gwarantować zastosowanie odpowiednich środków technicznych i organizacyjnych ochrony tych danych przed rozpoczęciem wejścia w życie projektu tzn. przed rozpoczęciem przetwarzania danych osobowych.

3. Podczas projektowania odpowiednich środków technicznych i organizacyjnych ochrony danych osobowych Fundacja bierze pod uwagę:

a. stan wiedzy technicznej,

b. koszt wdrożenia określonych zabezpieczeń,

c. charakter, zakres, kontekst i cele przetwarzania,

d. ryzyko naruszenia praw lub wolności osób fizycznych wynikające z przetwarzania ich danych osobowych.

4. W przypadku wdrażania nowych projektów, Fundacja przeprowadza analizę ryzyka.

4.6. Rejestr Czynności Przetwarzania Danych i Rejestr Kategorii Czynności Przetwarzania Danych

1. Fundacja prowadzi Rejestr Czynności Przetwarzania Danych, w którym inwentaryzuje i monitoruje sposób, w jaki wykorzystuje dane osobowe, których jest Administratorem.

2. Rejestr Czynności Przetwarzania Danych prowadzony jest w wersji elektronicznej przy wykorzystaniu wzoru stanowiącego Załącznik nr 7 do Polityki.

3. Fundacja prowadzi Rejestr Kategorii Czynności Przetwarzania Danych, których jest Podmiotem przetwarzającym.

4. Rejestr Kategorii Czynności Przetwarzania Danych prowadzony jest w wersji elektronicznej zgodnie ze wzorem stanowiącym Załącznika nr 8 do Polityki.

4.7. Retencja danych osobowych

1. Okres przetwarzania danych osobowych przez Fundację zależy od celu i podstawy prawnej przetwarzania.

2. Okres przetwarzania danych może także wynikać z przepisów, gdy stanowią one podstawę przetwarzania.

3. W przypadku przetwarzania danych na podstawie prawnie uzasadnionego interesu Administratora Danych Osobowych – np. ze względów bezpieczeństwa, w celu marketingu bezpośredniego – dane przetwarzane są przez okres umożliwiający realizację tego interesu lub do zgłoszenia skutecznego sprzeciwu względem przetwarzania danych.

4. Jeśli przetwarzanie Danych osobowych odbywa się na podstawie zgody, dane przetwarzane są do czasu jej wycofania.

5. Gdy podstawę przetwarzania stanowi niezbędność do zawarcia i wykonania umowy, dane są przetwarzane do momentu jej rozwiązania.

6. Okres przetwarzania danych może być przedłużony w przypadku, gdy przetwarzanie jest niezbędne do ustalenia lub dochodzenia roszczeń lub obrony przed roszczeniami, a po tym okresie – jedynie w przypadku i w zakresie, w jakim będą wymagać tego przepisy prawa.

7. Po upływie okresu przetwarzania dane są nieodwracalnie usuwane lub anonimizowane.

8. Okresy przechowywania danych osobowych zostały zawarte w Rejestrze Czynności Przetwarzania Danych.

4.8. Przekazywanie Danych osobowych do państw trzecich

Fundacja nie przekazuje danych osobowych do państw trzecich oraz organizacji międzynarodowych w rozumieniu Rozporządzenia z zastrzeżeniem danych osobowych umieszczanych na fanpage'ach w portalach społecznościowych Facebook, Instagram, LinkedIn. Meta Platforms Ireland Limited oraz LinkedIn Ireland Unlimited Company zapewniają odpowiedni poziom ochrony przetwarzanych danych osobowych, akceptowany przez Komisję Europejską.

5. Zarządzanie przetwarzaniem danych osobowych, odpowiedzialności

5.1. Administrator Danych Osobowych (ADO)

W rozumieniu przepisów Rozporządzenia, ADO jest podmiotem ustalającym cele i sposoby przetwarzania danych osobowych. ADO przetwarzając dane osobowe zobowiązany jest do podejmowania stosownych działań w celu ochrony przetwarzanych danych osobowych, a w szczególności:

a. wprowadza dokumentację opisującą sposób przetwarzania danych tj. m.in.: Politykę Bezpieczeństwa Danych Osobowych wraz z załącznikami oraz Instrukcję Zarządzania Systemami Informatycznymi;

b. zapewnia niezbędne środki potrzebne do zagwarantowania bezpieczeństwa przetwarzania danych osobowych w Fundacji;

c. zapewnia przetwarzanie danych osobowych zgodnie z powszechnie obowiązującymi przepisami prawa oraz wewnętrznymi regulacjami Fundacji;

d. zapewnia poprawność merytoryczną danych osobowych i adekwatność w stosunku do celów, w jakich są przetwarzane;

e. zapewnia przechowywanie danych osobowych w sposób umożliwiający identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania;

f. wyznacza osobę odpowiedzialną za nadzorowanie środków zapewniających bezpieczeństwo przetwarzania danych osobowych w Systemach informatycznych;

g. dopuszcza Osoby upoważnione do przetwarzania danych osobowych nadając im upoważnienia;

h. może powierzyć innemu podmiotowi przetwarzanie danych zawierając umowę powierzenia przetwarzania danych osobowych

i. podejmuje odpowiednie działania w przypadku naruszenia lub podejrzenia naruszenia procedur bezpiecznego przetwarzania danych osobowych.

j. prowadzi Rejestr Czynności Przetwarzania Danych i Rejestr Kategorii Czynności Przetwarzania

Danych. 5.2. Inspektor Ochrony Danych (IOD)

1. Fundacja wyznaczyła Inspektora Ochrony Danych.

2. Inspektor Ochrony Danych, że realizuje wszystkie zadania dotyczące ochrony danych osobowych, za które odpowiedzialny byłby IOD w przypadku jego wyznaczenia.

3. Do obowiązków Inspektor Ochrony Danych należy:

a. informowanie pracowników i współpracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO i innych przepisów unijnych lub krajowych o ochronie Danych osobowych oraz doradzanie im w tym zakresie;

b. monitorowanie przestrzegania przez Osoby upoważnione przepisów RODO oraz innych przepisów unijnych i krajowych z zakresu ochrony Danych osobowych, jak również niniejszej Polityki i innych wewnętrznych procedur;

c. podejmowanie działań zwiększających świadomość w zakresie ochrony Danych osobowych, w tym szkoleń personelu uczestniczącego w operacjach przetwarzania oraz prowadzenie powiązanych z tym audytów;

d. przeprowadzanie (jeżeli jest to wymagane) oceny skutków dla ochrony Danych osobowych zgodnie z art. 35 RODO;

e. współpraca z Organem nadzorczym;

f. pełnienie funkcji punktu kontaktowego dla Organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 RODO oraz w stosownych przypadkach prowadzenie konsultacji we wszelkich innych sprawach.

5.3. Osoba odpowiedzialna za nadzór nad systemami informatycznymi

1. Fundacja wyznaczyła osobę odpowiedzialną za sprawowanie nadzoru nad systemami informatycznymi.

2. Do zadań osoby wskazanej w ust. 1 należy:

a. współpraca z ADO przy przygotowaniu i wdrażaniu dokumentacji ochrony danych osobowych,

b. współpraca z ADO przy przeprowadzaniu okresowych planów sprawdzeń tj. systematyczne kontrolowanie zastosowanych środków technicznych i organizacyjnych zapewniających ochronę przetwarzanych danych osobowych,

c. nadawanie lub zmiana uprawnień do przetwarzania danych osobowych w systemach informatycznych na pisemny wniosek uprawnionego,

d. nadzór nad stosowaniem środków zapewniających bezpieczeństwo przetwarzania danych osobowych w systemach informatycznych, a w szczególności przeciwdziałających dostępowi osób niepowołanych do tych systemów,

e. podejmowanie odpowiednich działań w przypadku wykrycia naruszeń w systemie zabezpieczeń, f. identyfikacja i analiza zagrożeń oraz ocena ryzyka, na które może być narażone przetwarzanie danych osobowych w systemach informatycznych,

g. zapewnienie ciągłości działania systemów informatycznych, w tym zabezpieczenie zbiorów danych oraz programów służących do przetwarzania danych osobowych poprzez systematyczne wykonywanie kopii zapasowych i sprawowanie nadzoru nad przechowywanymi kopiami zapasowymi opisanymi w Instrukcji zarządzania systemem informatycznym,

h. nadzorowanie awaryjnego źródła zasilania oraz zabezpieczenia przed zakłóceniami w sieci zasilającej systemów informatycznych (UPS) służących do przetwarzania danych osobowych, których nagła przerwa w pracy mogłaby spowodować utratę danych lub naruszenie ich Integralności,

j. nadzór nad naprawami, konserwacją oraz likwidacją urządzeń komputerowych, na których zapisane są dane osobowe,

j. kontrola przeglądu i konserwacji systemów informatycznych służących do przetwarzania danych osobowych,

k. nadzór nad pracami serwisowymi w sieci informatycznej Fundacji (urządzenia sieciowe, serwery, komputery i notebooki) wykonywanymi przez zewnętrzne podmioty,

l. zabezpieczenie systemów służących do przetwarzania danych osobowych przed działaniem oprogramowania złośliwego,

m. nadzór nad bezpieczeństwem danych zawartych na komputerach przenośnych, dyskach wymiennych, w których przetwarzane są dane osobowe,

n. monitorowanie działania zabezpieczeń wdrożonych w celu ochrony danych osobowych w systemach informatycznych,

o. sprawowanie nadzoru nad funkcjonowaniem mechanizmów uwierzytelniania użytkowników w systemie informatycznym przetwarzającym dane oraz kontrolą dostępu do danych, w tym zewnętrznych punktów dostępu.

p. zabezpieczenie pomieszczenia serwerowni i szaf krosowych przed dostępem osób nieuprawnionych,

q. ochrona przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych zabezpieczeń chroniących przed nieuprawnionym dostępem,

r. nadzorowanie stosowania zasady „czystego ekranu".

5.4. Użytkownik Systemu Informatycznego (USI)

USI jako Osoba upoważniona do przetwarzania danych osobowych w systemach informatycznych, w których przetwarzane są dane osobowe jest zobowiązany do:

a. znajomości oraz bezwzględnego przestrzegania zasad bezpieczeństwa przetwarzania informacji w Fundacji, określonych w Polityce oraz innych przepisach i dokumentach, mających w tym zakresie zastosowanie,

b. zabezpieczania danych osobowych oraz dokumentów zawierających dane osobowe przed dostępem osób nieupoważnionych za pomocą środków określonych w Polityce, Instrukcjach, jak też wytycznych przełożonych,

c. zgłaszania potrzeby zniszczenia wszystkich zbędnych nośników elektronicznych (np. dyski zewnętrzne, pendrive) zawierających dane osobowe w sposób uniemożliwiający ich odzyskanie,

d. nieudzielania informacji o danych osobowych przetwarzanych w Fundacji innym podmiotom, chyba, że obowiązek taki wynika wprost z przepisów prawa i tylko w sytuacji, gdy przesłanki określone w tych przepisach zostały spełnione,

e. stosowania się do zaleceń ADO oraz osoby odpowiedzialnej za nadzór nad systemami informatycznymi w zakresie przetwarzania danych osobowych,

f. niezwłocznego informowania ADO o wszelkich nieprawidłowościach dotyczących bezpieczeństwa danych osobowych przetwarzanych w Fundacji, a w szczególności zawiadamiania o wszelkich przypadkach utraty lub kradzieży dokumentów lub innych nośników zawierających dane osobowe.

6. Obszar przetwarzania danych osobowych

1. Obszarem przetwarzania danych osobowych są pomieszczenia, w których są przetwarzane dane osobowe zarówno w formie papierowej, jak i w systemie informatycznym.

2. Obiekty, w których przetwarzane są dane osobowe, są zabezpieczone w sposób zapewniający rozliczalność i poufność przetwarzanych danych.

3. Szczegółowy „Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe" stanowi Załącznik nr 9 do Polityki i zawiera następujące informacje: a. określenie obiektu, b. lokalizacja (adres i nr budynku),

6.1. Środki ochrony fizycznej obszaru przetwarzania danych osobowych

1. Pomieszczenia, wchodzące w skład obszaru przetwarzania danych osobowych zamykane są na klucz.

2. Pomieszczenia, w których przetwarzane są dane osobowe, zabezpieczone są przed skutkami pożaru za pomocą wolnostojącej gaśnicy.

3. W siedzibie Fundacji zapewniono kontrolę dostępu do budynku, poprzez wideo domofon.

6.2. Zasady przebywania w obszarze przetwarzania danych osobowych

1. 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 nieuprawnionym dostępem.

2. Dostęp gości do serwerowni lub innych pomieszczeń, w których znajdują się systemy informatyczne, służące do przetwarzania danych osobowych, jest możliwy jedynie pod stałym nadzorem upoważnionego pracownika Fundacji.

3. 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 lub bez opieki osoby upoważnionej. Pracownicy zobowiązani są do dołożenia należytej staranności w celu zabezpieczenia posiadanych kluczy przed nieuprawnionym dostępem.

7. Określenie środków technicznych i organizacyjnych niezbędnych do zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych

7.1. Organizacyjne środki ochrony danych osobowych

1. Wyznaczenie osoby nadzorującej przestrzeganie zasad ochrony oraz prawidłową realizację zadań związanych z bezpieczeństwem danych osobowych przetwarzanych w systemach informatycznych Fundacji.

2. Dopuszczanie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie w przedmiotowym zakresie.

3. Prowadzenie Ewidencji osób upoważnionych do przetwarzania danych osobowych.

4. Opracowanie i wdrożenie dokumentacji w zakresie ochrony danych osobowych.

5. Szkolenia upoważnionych osób w zakresie obowiązujących przepisów ochrony danych osobowych oraz wewnętrznych regulacji stosowanych w celu zabezpieczenia danych w Fundacji.

6. Zobowiązanie osób upoważnionych do przetwarzania danych osobowych do zachowania ich w tajemnicy.

7. Osoby upoważnione do przetwarzania 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 lub wynikających z umowy o współpracy, w ramach udzielonego upoważnienia do przetwarzania danych.

8. Niedopuszczalne jest wynoszenie materiałów zawierających dane osobowe poza obszar ich przetwarzania bez związku z wykonywaniem czynności służbowych lub wynikających z umowy o współpracy bez zgody ADO. Za bezpieczeństwo i zwrot materiałów zawierających dane osobowe odpowiada w tym przypadku osoba dokonująca ich wyniesienia oraz jej bezpośredni przełożony.

7.1.1. Organizacyjne zasady bezpiecznego przetwarzania danych osobowych w wersji papierowej

1. Osoby upoważnione mają obowiązek stosować zasadę czystego biurka nie pozostawiając na nim po pracy dokumentów zawierających dane osobowe.

2. Dokumenty z danymi osobowymi powinny być zamykane na klucz w meblach biurowych (szuflady, szafy).

3. Niszczenie brudnopisów, błędnych lub zbędnych kopii materiałów zawierających dane osobowe musi odbywać się z wykorzystaniem niszczarek, w sposób uniemożliwiający odczytanie zawartej w nich treści.

4. Wydruki zawierające dane osobowe należy niezwłocznie odbierać z drukarek. Zabronione jest pozostawianie wydruków zawierających dane osobowe na ogólnodostępnej drukarce.

7.1.2. Organizacyjne zasady bezpiecznego przetwarzania danych osobowych w wersji elektronicznej

1. Osoby przetwarzające dane osobowe w systemach informatycznych posiadają indywidualne i niepowtarzalne identyfikatory (loginy).

2. Przydzielony raz identyfikator danemu użytkownikowi nie może być przydzielony innej osobie, chyba że zachodzą szczególne ku temu przesłanki, a ponowne przydzielenie tego samego identyfikatora nie będzie prowadziło do możliwości korzystania z tegoż identyfikatora przez więcej niż jedną osobę oraz nie wykluczy możliwości bezpośredniej i nie budzącej wątpliwości identyfikacji osoby korzystającej z tego identyfikatora.

3. Dostęp do systemu informatycznego realizowany jest poprzez podanie identyfikatora oraz dokonaniu uwierzytelnienia hasłem z zachowaniem szczególnej ostrożności podczas jego wprowadzania.

4. Wszyscy USI, korzystający z systemów informatycznych, w których przetwarzane sąd osobowe, mają obowiązek stosowania haseł spełniających wymogi bezpieczeństwa na poziomie wysokim oraz dokonywania zmian haseł nie rzadziej niż co 12 miesięcy.

5. Zabronione jest ujawnianie haseł jak również korzystanie z identyfikatorów innych użytkowników.

6. Haseł dostępu do komputera oraz baz danych zawierających dane osobowe nie wolno umieszczać przy komputerze oraz w niezamykanych szafkach/szufladach (karteczki, notesy, kalendarze itp.), ani zapisywać w pamięci przeglądarek internetowych.

7. Przyznanie, zmiana lub usunięcie uprawnień użytkownika do przetwarzania danych osobowych w poszczególnych aplikacjach realizowane jest na wniosek pisemny bądź ustny przełożonego. Zlecenie przekazywane jest osobie odpowiedzialnej za nadzór nad systemami informatycznymi.

8. Monitory ekranowe powinny być ustawione w taki sposób, aby uniemożliwić osobom nieuprawnionym podgląd wyświetlanych danych osobowych.

9. Udając się na przerwę w pracy należy zastosować blokadę monitora lub wylogować się z systemu.

10. Wysyłając dane osobowe mailem należy upewnić się czy prawidłowo został wpisany e-mail adresata wiadomości.

11. Przed wysłaniem plików zawierających szczególne kategorie danych osobowych, należy te pliki zaszyfrować stosując programy szyfrujące (np. Zip, 7Z, wbudowany mechanizm haseł w plikach pakietu Microsoft Office). Hasło wysyłamy zawsze inną drogą komunikacyjną (telefon, sms).

12. Wysyłając wiadomości do wielu adresatów będących osobami fizycznymi, adresy mailowe należy dodawać do kopii ukrytej tzw. UDW lub BCC (nie dotyczy wysyłania wiadomości do współpracowników).

13. Zabronione jest używanie służbowego konta mailowego do celów prywatnych.

14. Zabronione jest klikanie w linki i otwieranie załączników z nieznanych źródeł.

15. Zabronione jest samodzielne instalowanie programów, samodzielne naprawianie komputera. Jakąkolwiek awarię należy niezwłocznie zgłosić przełożonemu lub/i osobie odpowiedzialnej za nadzór nad systemami informatycznymi.

16. Zabronione jest używanie obcych przenośnych pamięci (dyski ssd, pendrive itp.).

17. W przypadku przetwarzania danych osobowych na komputerach przenośnych należy zachować szczególną ostrożność przy ich transporcie, a Użytkownicy powinni stosować zasady bezpieczeństwa co najmniej takie jak w obszarze przetwarzania.

7.2. Techniczne środki ochrony danych osobowych

1. Komputery służące do przetwarzania danych osobowych są połączone z lokalną siecią komputerową.

2. Zastosowano urządzenia typu UPS, chroniące system informatyczny służący do przetwarzania danych osobowych przed skutkami awarii zasilania.

3. Dostęp do danych osobowych przetwarzanych na komputerach przenośnych, zabezpieczony został przed nieautoryzowanym uruchomieniem za pomocą haseł BIOS.

4. System informatyczny służący do przetwarzania danych osobowych jest wyposażony w mechanizmy uwierzytelnienia użytkownika oraz kontroli dostępu do tych danych.

5. Zastosowano środki uniemożliwiające wykonywanie nieautoryzowanych kopii danych osobowych przetwarzanych przy użyciu systemów informatycznych.

6. Zastosowano systemowe mechanizmy wymuszające okresową zmianę haseł.

7. Zastosowano system rejestracji dostępu do systemów, w których znajdują się dane osobowe.

8. Zastosowano środki kryptograficznej ochrony danych dla danych osobowych przekazywanych drogą teletransmisji.

9. Dostęp do środków teletransmisji zabezpieczono za pomocą mechanizmów uwierzytelnienia.

10. Zastosowano nadzorowany przez informatyka system antywirusowy na wszystkich stanowiskach.

11. Zastosowano system Firewall do ochrony dostępu do sieci komputerowej.

12. Wykorzystano środki pozwalające na rejestrację zmian wykonywanych na poszczególnych dokumentach zawierających danych osobowych.

13. Zastosowano systemowe środki pozwalające na określenie odpowiednich praw dostępu do zasobów informatycznych, w tym zbiorów danych osobowych dla poszczególnych użytkowników systemu informatycznego.

14. Zastosowano mechanizm automatycznej blokady dostępu do systemu informatycznego służącego do przetwarzania danych osobowych w przypadku dłuższej nieaktywności pracy użytkownika.

15. Sieć Wifi (sieć zamknięta, szyfrowana z ograniczonym dostępem) nie jest połączona z siecią wewnętrzną zawierającą dane osobowe.

16. Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przed utratą poprzez wykonywanie kopii zapasowych.

8. Postępowanie w sytuacji Naruszenia ochrony danych osobowych

1. Do incydentów bezpieczeństwa mogących prowadzić do naruszenia ochrony danych osobowych należą:

a. zdarzenia losowe zewnętrzne – pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności;

b. zdarzenia losowe wewnętrzne – awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków i Użytkowników, utrata/zagubienie dokumentów, utrata/zagubienie przenośnych komputerów, pendrive'ów, dysków zewnętrznych;

c. umyślne incydenty zewnętrzne – włamanie do systemu informatycznego lub pomieszczeń; kradzież danych/sprzętu przez osobą z zewnątrz firmy; atak hackerski, którego skutkiem może być wyciek informacji; atak phishingowy; działanie wirusów i innego szkodliwego oprogramowania;

d. umyślne incydenty wewnętrzne – ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych; kradzież dokumentacji z danymi przez pracownika.

2. W przypadku stwierdzenia lub podejrzenia wystąpienia naruszenia ochrony danych osobowych, pracownik/współpracownik ma obowiązek:

a. powiadomić ADO i bezpośredniego przełożonego o podejrzeniu lub fakcie wystąpienia naruszenia;

b. niezwłocznie podjąć czynności niezbędne dla powstrzymania niepożądanych skutków, a następnie ustalić przyczyny, lub sprawców zaistniałego zdarzenia, jeżeli jest to możliwe;

c. zaniechać dalszych planowanych przedsięwzięć, które wiążą się z zaistniałym naruszeniem i mogą utrudnić jego udokumentowanie i analizę;

d. udokumentować wstępnie zaistniałe naruszenie;

e. nie opuszczać bez uzasadnionej potrzeby miejsca zdarzenia; f. zabezpieczyć pomieszczenie do czasu przybycia ADO (jeśli będzie to konieczne).

3. Przykłady incydentów, mogących powodować naruszenie bezpieczeństwa przetwarzania danych osobowych, które należy zgłaszać do ADO i osoby odpowiedzialnej za nadzór nad systemami informatycznymi zawiera Załącznik nr 10 do Polityki.

4. Po otrzymaniu zgłoszenia o wystąpieniu lub podejrzeniu wystąpienia naruszenia ochrony danych osobowych, ADO prowadzi postepowanie wyjaśniające, w toku którego:

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

b. ustala datę, czas, miejsce wystąpienia naruszenia, jego zakres, przyczyny ujawnienia, skutki oraz wielkość szkód, które zaistniały

c. rekomenduje działania naprawcze i prewencyjne.

5. ADO, osoba odpowiedzialna za nadzór nad systemami informatycznymi i inni zainteresowani pracownicy/współpracownicy Fundacji konsultują i oceniają czy powstałe naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, a jeśli tak, to jaka jest waga ryzyka (ryzyko niskie, średnie, wysokie).

6. Ryzyko wystąpienia naruszenia praw i wolności osób fizycznych oceniane jest pod kątem możliwości wystąpienia: uszczerbku fizycznego, szkód majątkowych, szkód niemajątkowych (np. dyskryminacja, kradzież tożsamości lub oszustwa dotyczące tożsamości, strata finansowa, naruszenie dobrego imienia, naruszenie poufności danych osobowych chronionych tajemnicą zawodową, nieuprawnione odwrócenie pseudonimizacji lub wszelka inna znaczna szkoda gospodarcza lub społeczna).

7. W przypadku stwierdzenia, że naruszenie może skutkować ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je Prezesowi UODO.

8. Zgłoszenie naruszenia do organu nadzorczego 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 ochrony danych 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.

9. W przypadku stwierdzenia, że naruszenie może skutkować WYSOKIM ryzykiem naruszenia praw lub wolności osób fizycznych, ADO bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie musi zawierać wszystkie elementy wskazane w pkt 9 powyżej i powinno być sformułowane jasnym i prostym językiem.

10. Zawiadomienie, o którym mowa w pkt 10 powyżej nie jest wymagane, jeżeli spełniono wymagania art. 34 ust. 3 Rozporządzenia.

11. ADO dokumentuje na bieżąco zaistniały przypadek naruszenia sporządzając Raport z naruszenia ochrony danych osobowych, którego wzór stanowi Załącznik nr 11 do Polityki. Raport zawiera m.in. ocenę skutków naruszenia ochrony danych osobowych.

12. Po wyczerpaniu niezbędnych środków doraźnych po zaistniałym naruszeniu, ADO w porozumieniu z osobą odpowiedzialną za nadzór nad systemami informatycznymi, zasięga niezbędnych opinii i proponuje działania naprawcze (w tym ustosunkowuje się do kwestii ewentualnego odtworzenia danych z zabezpieczeń) i zarządza termin wznowienia przetwarzania danych.

13. ADO wpisuje zaistniałe naruszenie do Rejestru naruszeń ochrony danych osobowych, którego wzór stanowi Załącznik nr 12 do Polityki,

14. ADO w porozumieniu z osobą odpowiedzialną za nadzór nad systemami informatycznymi ocenia skuteczność zakończonych działań naprawczych związanych z naruszeniem i wpisuje swoją ocenę w Rejestrze naruszeń ochrony danych osobowych (Załącznik nr 12 do Polityki

9. Szkolenia

1. Szkolenia z zakresu bezpieczeństwa informacji danych osobowych w Fundacji dokonywane są dla nowo zatrudnionych pracowników/współpracowników, jak również po wystąpieniu incydentu naruszającego bezpieczeństwo danych osobowych, w odniesieniu do osoby lub osób, którzy dopuścili się uchybień skutkujących tymże incydentem.

2. Oprócz szkoleń określonych w pkt 1 powyżej, odbywają się również szkolenia okresowe prowadzone przez ADO, w tym szkolenia przedstawiające zmiany w przepisach prawa o ochronie danych osobowych lub zmiany zasad ochrony danych osobowych obowiązujących w Fundacji.

3. Dopuszcza się przeprowadzanie szkoleń e-learningowych. Celem szkoleń jest podniesienie świadomości pracowników w zakresie bezpieczeństwa, ochrony oraz przetwarzania danych osobowych.

10. Postanowienia końcowe

1. Polityka jest wewnętrznym dokumentem Fundacji objętym obowiązkiem zachowania w poufności przez wszystkie osoby, którym zostanie ujawniona. Do spraw nieuregulowanych w Polityce stosuje się powszechnie obowiązujące przepisy prawa o ochronie danych osobowych.

2. Niezależnie od odpowiedzialności określonej w przepisach powszechnie obowiązującego prawa, naruszenie zasad określonych w niniejszej Polityce może zostać uznane za ciężkie naruszenie przez pracownika podstawowych obowiązków pracowniczych.

3. Pracownicy Fundacji zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w niniejszej Polityce.

4. Zmiany niniejszej Polityki wymagają każdorazowo formy pisemnej w postaci aktualizacji Polityki.

5. Uaktualnienia załączników nie powodują konieczności wprowadzenia nowej wersji Polityki.

11. Załączniki

1. Wzór upoważnienia do przetwarzania danych osobowych

2. Ewidencja Osób Upoważnionych do przetwarzania danych osobowych

3. Wzór oświadczenia 0 zachowaniu danych osobowych i sposobu ich zabezpieczenia w tajemnicy

4. Wzór umowy powierzenia przetwarzania danych osobowych

5. Wzory klauzul informacyjnych

6. Rejestr żądań i realizacji uprawnień osób, których dane dotyczą;

7. Rejestr Czynności Przetwarzania Danych

8. Rejestr Kategorii Czynności Przetwarzania Danych

9. Wykaz budynków, pomieszczeń lub części pomieszczeń w których przetwarzane są dane osobowe

10. Wzór Raportu z naruszenia ochrony danych osobowych

11. Rejestr naruszeń ochrony danych osobowych

12. Postanowienia końcowe

1. Polityka wchodzi w życie z dniem 13.03.2025 r.