POLITYKA OCHRONY DANYCH OSOBOWYCH

W

POLSKIEJ FUNDACJI CHORÓB RZADKICH "POMÓŻMY JASIOWI I MAŁGOSI" Z SIEDZIBĄ W KRAKOWIE

przyjęta w dniu 25 maja 2018 roku

ROZDZIAŁ I
POSTANOWIENIA OGÓLNE

§ 1

Zasady przetwarzania danych osobowych

1. Polskiej Fundacji Chorób Rzadkich "Pomóżmy Jasiowi i Małgosi" z siedzibą w Krakowie (dalej zwane również: **"Fundacją"**) przestrzega przepisów prawnych dotyczących ochrony danych osobowych zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia Dyrektywy 95/46 z dnia 27 kwietnia 2016 r. (Dz. Urz. UE L 119 z 04.05.2016).
2. Fundacja wykorzystuje dane osobowe wyłącznie dla realizacji jej celów statutowych, w tym w szczególności udzielaniu pomocy rzeczowej i finansowej chorym dzieciom i ich rodzicom.
3. Fundacja stosuje odpowiednie środki aby dane osobowe były:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”);
   4) prawidłowe i w razie potrzeby uaktualniane („prawidłowość”);
   5) przechowywane 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”);
   6) przetwarzane 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”);
   7) przetwarzane w sposób zapewniający możliwość wykazania przestrzegania ww. zasad („rozliczalność”).

§ 2
Definicje

Ilekroć w niniejszej Polityce jest mowa o:

1) **Administratorze** – rozumie się przez to Fundację, tj. Polską Fundację Chorób Rzadkich "Pomóżmy Jasiowi i Małgosi" z siedzibą w Krakowie, adres: ul. Radzikowskiego 29, 31-315 Kraków, wpisaną do rejestru stowarzyszeń, innych organizacji społecznych i zawodowych, fundacji oraz samodzielnych publicznych zakładów opieki zdrowotnej

KRS po numerem 0000286932, jako podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,

2) **aktywach** – rozumie się przez to środki materialne i niematerialne mające wpływ na przetwarzanie danych osobowych,
3) **danych osobowych** – rozumie się przez to 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,
4) **naruszeniu ochrony danych osobowych, incydencie** – rozumie się przez to naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych,
5) **odbiorcy** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Unii lub prawem państwa członkowskiego, nie są jednak uznawane za odbiorców; przetwarzanie tych danych przez te organy publiczne musi być zgodne z przepisami o ochronie danych mającymi zastosowanie stosownie do celów przetwarzania,
6) **organie nadzorczym** – rozumie się przez to Prezesa Urzędu Ochrony Danych Osobowych,
7) **podmiocie przetwarzającym** – rozumie się przez to osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora,
8) **Polityce** – rozumie się przez to niniejszy dokument Polityki Ochrony Danych Osobowych,
9) **przetwarzaniu** – rozumie się przez to operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie,
10) **RODO –** rozumie się przez to 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),

11) **ryzyku** – rozumie się przez to prawdopodobieństwo, że określone zagrożenie wystąpi i spowoduje straty lub zniszczenie zasobów.
12) **skutkach (w odniesieniu do materializacji zagrożeń)** – rozumie się przez to rezultaty niepożądanego incydentu (straty w wypadku wystąpienia zagrożenia),
13) **zagrożeniu** – rozumie się przez to potencjalne naruszenie (potencjalny incydent),
14) **zgodzie osoby, której dane dotyczą –** rozumie się przez to 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.

ROZDZIAŁ II
Administrator i podmioty przetwarzające dane osobowe
§ 3
Administrator

1. Administratorem danych osobowych przetwarzanych w ramach działalności Fundacji jest Fundacja.
2. Administrator decyduje o celach i sposobach przetwarzania danych osobowych, oraz ponosi odpowiedzialność za ich przetwarzanie zgodnie z prawem.
3. Administrator po przeanalizowaniu zasadności (uwzględniając w szczególności wymogi RODO) podejmuje decyzję o powołaniu lub niepowołaniu inspektora ochrony danych, o którym mowa w art. 37 RODO. W zakresie nieuregulowanym w Polityce, zadania inspektora ochrony danych określają przepisy RODO, w szczególności art. 38 i 39 RODO.

§ 4
Osoby upoważnione przez Administratora

1. Administrator nadaje i odbiera upoważnienia do przetwarzania danych osobowych przetwarzanych przez Administratora, w tym w szczególności pracownikom Fundacji. Wzór upoważnienia stanowi Załącznik nr 1 do Polityki.
2. Osoba upoważniona przez Administratora przetwarza dane osobowe wyłącznie na polecenie Administratora, z zastrzeżeniem odpowiednich przepisów prawa.
3. Administrator prowadzi ewidencję osób upoważnionych w celu sprawowania kontroli nad prawidłowym dostępem do danych osób upoważnionych.

§ 5
Podmioty przetwarzające

1. Zlecenie przez Administratora wykonywania określonych czynności związanych z jego działalnością podmiotom zewnętrznym (podwykonawcom), w przypadku którego konieczne będzie przetwarzanie danych osobowych, może być dokonane pod warunkiem zawarcia z takimi podmiotami umowy powierzenia przetwarzania danych.

2. Umowa powierzenia przetwarzania danych osobowych podmiotom przetwarzającym może być zawarta wyłącznie z podmiotami, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi prawne, w tym art. 28 i nast. RODO i chroniło prawa osób, których dane dotyczą.
3. Administrator prowadzi rejestr podmiotów przetwarzających, którego wzór stanowi Załącznik nr 2 do Polityki.

ROZDZIAŁ III
Przetwarzanie danych osobowych - zgodność z prawem
§ 6
Zasady ogólne

1. Administrator dokonuje przetwarzania danych osobowych w związku z prowadzoną działalnością statutową.
2. Administrator nie zamierza przekazywać danych osobowych do państw trzecich lub organizacji międzynarodowych. Gdyby takie przekazanie miało jednak nastąpić Administrator odpowiedzialny jest za zapewnienie zgodności takiego przekazania z art. 44-49 RODO.

§ 7
Podstawy przetwarzania danych osobowych

1. Przetwarzanie danych osobowych (zwykłych) przez Administratora odbywa wyłącznie gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków:
   1) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;
   2) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy;
   3) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze;
   4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
   5) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
   6) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

2. Przetwarzanie danych, o których mowa w art. 9 ust. 1 RODO w tym informacji dotyczących zdrowia, może się odbywać na podstawie jednej z przesłanek wymienionych w art. 9 ust. 2 RODO, a w szczególności gdy:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii Europejskiej lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu przetwarzania tych danych;
   2) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej, a osoba, której dane dotyczą, jest fizycznie lub prawnie niezdolna do wyrażenia zgody.

§ 8

Prawa osoby, której dane dotyczą

1. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem udzielić osobie, której dane dotyczą, wszelkich informacji, o których mowa w art. 13 i 14 RODO, oraz prowadzić z nią wszelką komunikację na mocy art. 15–22 i 34 RODO w sprawie przetwarzania. Informacji udziela się na piśmie lub w inny sposób, w tym w stosownych przypadkach – elektronicznie. Jeżeli osoba, której dane dotyczą, tego zażąda, informacji można udzielić ustnie, o ile innymi sposobami potwierdzi się tożsamość osoby, której dane dotyczą.
2. Obowiązki informacyjne, o których mowa w ust. 1, powyżej obejmują:
   1) informowanie o Administratorze i przetwarzaniu danych osobowych, w przypadku zbierania danych od osoby, których dane dotyczą (art. 13 RODO) - informacji udziela się podczas pozyskiwania danych osobowych (w tym - przy zawieraniu umów),
   2) informowanie o Administratorze i przetwarzaniu danych osobowych, w przypadku zbierania danych nie od osoby, których dane dotyczą (art. 14 RODO) - informacji udziela się w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych; lub jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.
3. Ponadto osoba, której dane dotyczą ma prawo do:
   1) dostępu do swoich danych osobowych - osoba, której dane dotyczą, jest uprawniona do uzyskania od Administratora potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji, których mowa w art. 15 RODO,
   2) żądania od Administratora sprostowania swoich danych osobowych, które są nieprawidłowe - art. 16 RODO,

3) żądania od administratora niezwłocznego usunięcia dotyczących jej danych osobowych, a Administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z okoliczności wymienionych w art. 17 RODO,
4) żądania od administratora ograniczenia przetwarzania w przypadkach określonych w art. 18 RODO,
5) otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła administratorowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony administratora, któremu dostarczono te dane osobowe, w przypadkach określonych w art. 20 RODO,
6) wniesienia sprzeciwu – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na § 7 pkt 5) lub 6), w tym profilowania na tych podstawach. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów - art. 21 RODO.

4. Administrator ma obowiązek zadośćuczynić prawom realizowanym, przez osobę, której dane dotyczą, zgodnie z przepisami RODO.
5. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 RODO.
6. Administrator bez zbędnej zwłoki – a w każdym razie 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 Administrator informuje osobę, której dane dotyczą o takim przedłużeniu terminu, z podaniem przyczyn opóźnienia. Jeśli osoba, której dane dotyczą, przekazała swoje żądanie elektronicznie, w miarę możliwości informacje także są przekazywane elektronicznie, chyba że osoba, której dane dotyczą, zażąda innej formy.
7. Jeżeli Administrator nie podejmuje działań w związku z żądaniem osoby, której dane dotyczą, to niezwłocznie – najpóźniej w terminie miesiąca od otrzymania żądania – informuje osobę, której dane dotyczą, o powodach niepodjęcia działań oraz o

możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem.

8. Informacje podawane na mocy art. 13 i 14 RODO oraz komunikacja i działania podejmowane na mocy art. 15–22 i 34 RODO są wolne od opłat, z zastrzeżeniem odpowiednich przepisów RODO.
9. Jeżeli Administrator ma uzasadnione wątpliwości co do tożsamości osoby fizycznej składającej żądanie, o którym mowa w art. 15–21 RODO, może zażądać dodatkowych informacji niezbędnych do potwierdzenia tożsamości osoby, której dane dotyczą.
10. Administrator nie podejmuje decyzji, które opierają się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołują wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływają.

ROZDZIAŁ IV
Czynności przetwarzania danych osobowych i analiza ryzyka

§ 9
Rejestr czynności przetwarzania

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych, za które odpowiada, którego wzór stanowi Załącznik nr 3 do Polityki. W rejestrze czynności wyróżnia się poszczególne procesy przetwarzania danych z uwzględnieniem rodzaju danych osobowych których dotyczą. Wykaz ten jest na bieżąco aktualizowany przez Administratora, z zastrzeżeniem spełnienia innych obowiązków wymienionych poniżej.
2. W przypadku powierzenia przetwarzania danych osobowych podmiotowi przetwarzającemu, podmiot ten prowadzi rejestr kategorii czynności przetwarzania dokonywanych w imieniu Administratora.
3. Administrator udostępnia rejestr na żądanie organu nadzorczego.

§ 10
Analiza ryzyka - postanowienia ogólne

1. Administrator dokonuje analizy ryzyka związanego z przetwarzaniem danych osobowych w celu ich zabezpieczenia w sposób adekwatny do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
2. Analiza ryzyka przeprowadzana jest dla poszczególnych procesów przetwarzania. Analiza ryzyka może być przeprowadzona łącznie dla podobnych procesów przetwarzania, z uwzględnieniem rodzaju danych osobowych których dotyczą, wiążących się z potencjalnie porównywalnym ryzykiem dla przetwarzania tych danych. W analizie ryzyka wskazuje się aktywa, które są wykorzystywane w procesie przetwarzania.

§ 11

Analiza ryzyka - wyznaczanie zagrożeń

1. Administrator określa listę zagrożeń, które mogą wystąpić w przetwarzaniu danych w danym procesie przetwarzania.
2. W przypadku pojawienia się nowych zagrożeń lista potencjalnych zagrożeń jest niezwłocznie uzupełniania i dokonuje się szacowania ryzyka w odniesieniu do tych nowych zagrożeń.

§ 12

Analiza ryzyka - szacowanie ryzyka

1. Administrator uwzględnia w szacowaniu ryzyka istniejące na dzień przeprowadzenia analizy ryzyka zabezpieczenia, w tym zabezpieczenia organizacyjne, techniczne, fizyczne i personalne.

2. Dla każdego procesu przetwarzania danych Administrator dokonuje sprawdzenia, czy dane osobowe są przetwarzane zgodnie z zasadami, o których mowa w § 1 ust. 3 Polityki, na podstawie jednej z przesłanek, o której mowa w § 7 Polityki, przy zapewnieniu osobom, których dane dotyczą, możliwości realizacji ich praw, o których mowa w § 8 Polityki.

3. Administrator określa prawdopodobieństwo wystąpienia poszczególnych zagrożeń w procesie przetwarzania. Przy szacowaniu prawdopodobieństwa incydentu uwzględnia się w szczególności następujące czynniki: statystyki występowania podobnych zdarzeń, czynniki środowiskowe, rodzaje podatności, a także istniejące zabezpieczenia.

4. Prawdopodobieństwo (P) wystąpienia zagrożenia ocenia się według poniżej skali:

PRAWDOPODOBIEŃSTWO WYSTĄPIENIA ZAGROŻENIA	**POZIOM**
ZAGROŻENIE NISKIE (nie występujące, rzadkie/występujące raz na pół roku)	1
ZAGROŻENIE ŚREDNIE (możliwe, występujące raz na kwartał)	2
zagrożenie wysokie (prawdopodobne, występujące raz w miesiącu lub częściej)	3

5. Administrator określa skutki (S) zmaterializowania się zagrożeń, powodujących naruszenie praw i wolności osób, których dane dotyczą, uwzględniając również straty biznesowe, utratę reputacji, nałożenie kar finansowych.

6. Skutki materializacji zagrożeń ocenia się według poniższej skali:

SKUTKI WYSTĄPIENIA ZAGROŻENIA	**POZIOM**
NISKIE (do 10.000 PLN/negatywne opinie bez udziału mediów)	1

ŚREDNIE (10.000-100.000 PLN/negatywne opinie w mediach lokalnych)	2
DUŻE (od 100.000 PLN/potencjalna konieczność zakończenia działalności	3

7. Administrator wylicza ryzyko dla wszystkich zagrożeń i ich skutków jako iloczyn ich wartości (poziomów), tj. w/g formuły: **R = P * S**
8. Administrator porównuje wyliczone ryzyka ze skalą i podejmuje decyzje dotyczące dalszego postępowania z ryzykiem.
9. Administrator dokonuje oceny ryzyka według następującej skali:

POZIOM RYZYKA	**WARTOŚĆ** [**R = P*S**]
NISKI (ryzyko pomijalne i akceptowalne)	1-2
ŚREDNI (ryzyko nie jest akceptowalne, ale działanie może zostać przesunięte w czasie i wymaga okresowego monitorowania)	3-6
WYSOKI (ryzyko jest nieakceptowalne – należy niezwłocznie wdrożyć dodatkowe zabezpieczenia)	9

10. Arkusz służący do szacowania ryzyka zawierający listę potencjalnych zagrożeń, według stanu na dzień przyjęcia Polityki stanowi Załącznik nr 4 do Polityki.
11. Administrator dokonuje analizy ryzyka regularnie, nie rzadziej niż raz na dwa lata lub po znaczących zmianach w przetwarzaniu danych (np. przetwarzanie nowych zbiorów, nowych procesów przetwarzania, w sytuacji zmiany przepisów prawnych).

§ 13
Zarządzanie ryzykiem

1. Administrator podejmuje następujące działania w związku z wyznaczonym ryzykiem:

1) akceptacja ryzyka – brak konieczności wprowadzania zmian (stosowania dodatkowych zabezpieczeń),
2) działania obniżające ryzyko:
    a) modyfikowanie (redukcja) – zastosowanie zabezpieczeń w celu obniżenia poziomu ryzyka (prawdopodobieństwa wystąpienia lub skutku),
    b) dzielenie (przeniesienie) – wykupienie ubezpieczenia od jakiegoś zdarzenia (ubezpieczenie) lub przeniesienie skutków ryzyka na podmiot trzeci (outsourcing),

c) unikanie – eliminacja działań powodujących ryzyko (np. zakaz wynoszenia komputerów przenośnych poza obszar organizacji) – w przypadku gdy zidentyfikowane ryzyka są zbyt wysokie, a koszt wdrożenia zabezpieczeń byłby nieadekwatny do działalności prowadzonej przez Administratora.

2. Wszędzie, gdzie Administrator decyduje się obniżyć ryzyko, wyznacza listę zabezpieczeń do wdrożenia, termin realizacji i osoby odpowiedzialne, a po ich wdrożeniu dokonuje ponownej analizy ryzyka dla przedmiotowych zagrożeń.
3. Administrator zobowiązany jest do monitorowania wdrożenia zabezpieczeń.

§ 14

Ocena skutków dla ochrony danych (DPIA)

1. Jeżeli dany rodzaj przetwarzania – w szczególności z użyciem nowych technologii – ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, administrator przed rozpoczęciem przetwarzania dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych. Dla podobnych operacji przetwarzania danych wiążących się z podobnym wysokim ryzykiem można przeprowadzić pojedynczą ocenę.
2. Dokonanie oceny skutków dla ochrony danych jest obligatoryjne dla operacji przetwarzania danych, która znajduje się w ustanowionym i ogłoszonym przez organ nadzorczy wykazie rodzajów operacji przetwarzania podlegających wymogowi dokonania oceny skutków dla ochrony danych, a także w przypadku:
   a) systematycznej, kompleksowej oceny czynników osobowych odnoszących się do osób fizycznych, która opiera się na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i jest podstawą decyzji wywołujących skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływających na osobę fizyczną;
   b) przetwarzania na dużą skalę szczególnych kategorii danych osobowych, o których mowa w art. 9 ust. 1 RODO, lub danych osobowych dotyczących wyroków skazujących i naruszeń prawa, o czym mowa w art. 10; lub
   c) systematycznego monitorowania na dużą skalę miejsc dostępnych publicznie.
3. Dokonując oceny skutków dla ochrony danych, Administrator konsultuje się z inspektorem ochrony danych, jeżeli został on wyznaczony.
4. Ocena zawiera co najmniej:
   1) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania, w tym, gdy ma to zastosowanie – prawnie uzasadnionych interesów realizowanych przez administratora;
   2) ocenę, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów;
   3) ocenę ryzyka naruszenia praw lub wolności osób, których dane dotyczą; oraz
   4) środki planowane w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych i

wykazać przestrzeganie niniejszego rozporządzenia, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą, i innych osób, których sprawa dotyczy;

5) ocenę czy przetwarzanie będzie powodować wysokie ryzyko nawet, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka.

5. Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Administrator nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Administrator konsultuje się z organem nadzorczym.

ROZDZIAŁ IV
Zarządzanie incydentami
§ 15

1. Niniejsze zasady zarządzania incydentami mają na celu minimalizację skutków wystąpienia incydentów bezpieczeństwa oraz ograniczenie ryzyka powstania zagrożeń i występowania incydentów w przyszłości.
2. Każda osoba upoważniona do przetwarzania danych osobowych zobowiązana jest do powiadamiania o wystąpieniu incydentu bezpośredniego przełożonego oraz, jeśli jest powołany – inspektora ochrony danych.
3. Osoby upoważnione do przetwarzania danych osobowych powinny zwracać uwagę w szczególności na następujące podatności utraty bezpieczeństwa danych osobowych:
   1) niewłaściwe zabezpieczenie fizyczne pomieszczeń, urządzeń i dokumentów,
   2) niewłaściwe zabezpieczenie sprzętu IT, oprogramowania przed wyciekiem, kradzieżą i utratą danych osobowych,
   3) nieprzestrzeganie zasad ochrony danych osobowych (np. niestosowanie zasady czystego biurka oraz ekranu, ochrony haseł, niezamykanie pomieszczeń, szaf, biurek).
4. Do typowych incydentów bezpieczeństwa danych osobowych należą:
   1) zdarzenia losowe zewnętrzne (pożar obiektu/pomieszczenia, zalanie wodą, utrata zasilania, utrata łączności),
   2) zdarzenia losowe wewnętrzne (awarie serwera, komputerów, twardych dysków, oprogramowania, pomyłki informatyków, użytkowników, utrata/zagubienie danych),
   3) umyślne incydenty (włamanie do systemu informatycznego lub pomieszczeń, kradzież danych/sprzętu, wyciek informacji, ujawnienie danych osobom nieupoważnionym, świadome zniszczenie dokumentów/danych, działanie wirusów i innego szkodliwego oprogramowania).
5. W przypadku stwierdzenia wystąpienia incydentu, Administrator prowadzi postępowanie wyjaśniające w toku, którego:
   1) ustala zakres i przyczyny incydentu oraz jego ewentualne skutki,
   2) inicjuje ewentualne działania dyscyplinarne,
   3) działa na rzecz przywrócenia funkcjonowania organizacji po wystąpieniu incydentu,

4) rekomenduje działania prewencyjne (zapobiegawcze) zmierzające do eliminacji podobnych incydentów w przyszłości lub zmniejszenia strat w momencie ich zaistnienia.

6. Administrator dokumentuje naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, ich skutki oraz podjęte działania zaradcze, zgodnie ze wzorem, który stanowi Załącznik nr 5 do Polityki.

§ 16

W przypadku naruszenia ochrony danych osobowych skutkującego ryzykiem naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu. Treść zgłoszenia powinna być zgodna z art. 33 ust. 3 RODO.

§ 17

1. Jeżeli naruszenie ochrony danych osobowych może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, Administrator bez zbędnej zwłoki zawiadamia osobę, której dane dotyczą, o takim naruszeniu. Zawiadomienie to jasnym i prostym językiem opisuje charakter naruszenia ochrony danych osobowych oraz zawiera przynajmniej informacje i środki, o których mowa w art. 33 ust. 3 lit. b), c) i d) RODO.
2. Zawiadomienie, o którym mowa w ust. powyżej, nie jest wymagane, w następujących przypadkach:
   1) Administrator wdrożył odpowiednie techniczne i organizacyjne środki ochrony i środki te zostały zastosowane do danych osobowych, których dotyczy naruszenie, w szczególności środki takie jak szyfrowanie, uniemożliwiające odczyt osobom nieuprawnionym do dostępu do tych danych osobowych;
   2) Administrator zastosował następnie środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osoby, której dane dotyczą;
   3) wymagałoby ono niewspółmiernie dużego wysiłku. W takim przypadku wydany zostaje publiczny komunikat lub zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

ROZDZIAŁ V
Bezpieczeństwo przetwarzania danych osobowych

§ 18

1. Administrator, uwzględniając stan wiedzy technicznej, koszt wdrożenia oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania - wdraża odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi w stosownym przypadku:
   1) pseudonimizację i szyfrowanie danych osobowych;

2) zdolność do ciągłego zapewnienia poufności, integralności, dostępności i odporności systemów i usług przetwarzania;
3) zdolność do szybkiego przywrócenia dostępności danych osobowych i dostępu do nich w razie incydentu fizycznego lub technicznego;
4) regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania.

2. Oceniając, czy stopień bezpieczeństwa jest odpowiedni, uwzględnia się w szczególności ryzyko wiążące się z przetwarzaniem, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.
3. Administrator wdraża odpowiednie środki techniczne i organizacyjne, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia każdego konkretnego celu przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności. W szczególności środki te zapewniają, by domyślnie dane osobowe nie były udostępniane bez interwencji danej osoby nieokreślonej liczbie osób fizycznych.
4. Opis stosowanych przez Administratora zabezpieczeń technicznych i organizacyjnych zawiera przyjęta przez Administratora Instrukcja zarządzania bezpieczeństwem środowiska przetwarzania danych osobowych.

ROZDZIAŁ VI
Zapewnienie stosowania procedur ochrony danych osobowych
§ 19

1. Przestrzeganie zasad określonych w Polityce oraz innych przyjętych przez Administratora procedurach dotyczących ochrony danych osobowych jest obowiązkiem osób reprezentujących Administratora oraz wszystkich osób zatrudnionych przez Administratora, na podstawie umowy o pracę albo świadczących na rzecz Administratora usługi na podstawie umowy zlecenia, umowy o dzieło lub innej podobnej umowy cywilnoprawnej.
2. Przed rozpoczęciem wykonywania obowiązków przez osoby, o których mowa w ust. 1, oraz udzieleniem im upoważnienia do przetwarzania danych osobowych, Administrator zapoznaje te osoby z zasadami ochrony danych osobowych, w tym w szczególności z postanowieniami Polityki oraz innych przyjętych przez Administratora procedurach dotyczących ochrony danych osobowych. Osoby te podpisują oświadczenie o zapoznaniu się z zasadami dotyczącymi ochrony danych osobowych, które wzór stanowi Załącznik nr 6 do Polityki.
3. W przypadku zmian w otoczeniu prawnym, zmian procedur dotyczących ochrony danych osobowych lub zakresu przetwarzania przez Administratora danych osobowych, Administrator informuje o wprowadzonych zmianach osoby

upoważnione do przetwarzania danych osobowych i w razie potrzeby organizuje odpowiednie szkolenie.

4. Obowiązki w zakresie stosowania zasad dotyczących ochrony danych osobowych przez podmioty przetwarzające, z którymi Administrator zawarł umowy powierzenia przetwarzania danych osobowych powinny zostać uregulowane w umowach powierzenia przetwarzania danych osobowych, zgodnie z RODO.
5. Administrator jest odpowiedzialny za regularne testowanie, mierzenie i ocenianie skuteczności środków technicznych i organizacyjnych mających zapewnić bezpieczeństwo przetwarzania. W tym celu Administrator organizuje regularnie audyty w zakresie przestrzegania zasad ochrony danych osobowych. Administrator przeprowadza audyt wewnętrzny lub korzysta z usług audytu zewnętrznego. Celem audytu jest ocena, czy system ochrony danych osobowych jest skutecznie wdrożony i funkcjonuje zgodnie z wymaganiami RODO.

ROZDZIAŁ VII
Postanowienia końcowe
§ 20

1. Polityka obowiązuje od dnia jej podpisania.
2. Zmiana Polityki wymaga decyzji Prezesa