|  |  |
| --- | --- |
| **Identyfikator dokumentu:** | PB |
| **Nazwa dokumentu:** | Polityka Bezpieczeństwa Informacji i Danych Osobowych |
| **Data:**  |  |
| **Wersja** | 1 |
| **Autor dokumentu:** | Justyna Chomicz |
| **Właściciel dokumentu:** | Joanna Lotko |
| **Osoba zatwierdzająca:** | Joanna Lotko |

**Spis treści**

[1. Wprowadzenie 3](#_Toc8187514)

[2. Zakres 3](#_Toc8187515)

[3. Definicje 3](#_Toc8187516)

[4. Postanowienia ogólne 6](#_Toc8187517)

[5. Odpowiedzialność 7](#_Toc8187518)

[6. Obowiązki Administratora 7](#_Toc8187519)

[7. Inspektor Ochrony Danych 9](#_Toc8187520)

[8. Analiza ryzyka 10](#_Toc8187521)

[9. Przetwarzanie danych 11](#_Toc8187522)

[10. Zgody 12](#_Toc8187523)

[11. Szczególne kategorie danych osobowych 13](#_Toc8187524)

[12. Uprawnienia osób fizycznych i obsługa ich żądań 14](#_Toc8187525)

[13. Prawo dostępu przysługujące osobie, której dane dotyczą 16](#_Toc8187526)

[14. Prawo do sprostowania danych (art. 16 RODO) 16](#_Toc8187527)

[15. Prawo do usunięcia danych („prawo do bycia zapomnianym” art. 17 RODO) 17](#_Toc8187528)

[16. Prawo do ograniczenia przetwarzania (art. 18 RODO) 17](#_Toc8187529)

[17. Obowiązek Administratora powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania 18](#_Toc8187530)

[18. Prawo do przenoszenia danych (art. 20 RODO) 18](#_Toc8187531)

[19. Prawo do sprzeciwu (art. 21 RODO) 18](#_Toc8187532)

[20. Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie (art. 22 RODO) 19](#_Toc8187533)

[21. Informacje podawane podczas zbierania danych 19](#_Toc8187534)

[22. Powierzanie danych osobowych 20](#_Toc8187535)

[23. Budynki i pomieszczenia w których przetwarzane są dane osobowe 20](#_Toc8187536)

[24. Zabezpieczenia techniczne 21](#_Toc8187537)

[25. Rejestr czynności przetwarzania danych osobowych oraz Rejestr kategorii 22](#_Toc8187538)

[26. Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych 22](#_Toc8187539)

[27. Obowiązki pracowników i współpracowników 23](#_Toc8187540)

[28. Środki organizacyjne i techniczne 24](#_Toc8187541)

[29. Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu technicznego lub fizycznego 26](#_Toc8187542)

[30. Szkolenia 27](#_Toc8187543)

[31. Sprawdzenia i audyty 27](#_Toc8187544)

[32. Upoważnienia do przetwarzania danych osobowych 28](#_Toc8187545)

[33. Osoby uprawnione do wystawiania upoważnień 28](#_Toc8187546)

[34. Ewidencja upoważnień 28](#_Toc8187547)

[35. Postanowienia końcowe 29](#_Toc8187548)

[36. Spis załączników 29](#_Toc8187549)

[37. Dokumenty powiązane 30](#_Toc8187550)

[38. Historia wersji dokumentu 30](#_Toc8187551)

# Wprowadzenie

1. Fundacja Familijny Poznań przykłada najwyższą staranności do ochrony danych osobowych pracowników, współpracowników, osób, korzystających z usług Fundacji. Niniejsza Polityka Bezpieczeństwa Informacji i Danych Osobowych, zwana dalej Polityką, ma na celu uzyskanie optymalnego i zgodnego z wymogami obowiązujących aktów prawnych, sposobu przetwarzania informacji, a przede wszystkim zapewnienie ochrony danych osobowych.
2. Polityka została utworzona w oparciu o wymagania zawarte w przepisach obowiązującego prawa, w tym Rozporządzenia 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), zwanego dalej RODO oraz ustawy z dnia 10 maja 2018r. o ochronie danych osobowych.
3. Polityka zawiera w szczególności opis zasad ochrony danych osobowych obowiązujących
w Fundacji Familijny Poznań. Ponadto Polityka odwołuje się do załączników uszczegóławiających, które tworzą uzupełnienie dokumentacji ochrony danych osobowych i bezpieczeństwa informacji.
4. Ochrona danych osobowych jest realizowana poprzez: zabezpieczenia fizyczne, procedury organizacyjne, oprogramowanie systemowe, aplikacje oraz przez użytkowników.
5. Odpowiedzialny za wdrożenie i wypełnianie niniejszej Polityki jest zarząd Fundacji Familijny Poznań.
6. Poprzez bezpieczeństwo danych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, osiągane poprzez wdrożenie i eksploatację niezbędnych do tego celu mechanizmów i zabezpieczeń technicznych i organizacyjnych.

# Zakres

1. Zakres stosowania niniejszej Polityki obejmuje wszystkie dane, przede wszystkim dane osobowe, przetwarzane przez Fundację Familijny Poznań. Polityka obejmuje zarówno dane w formie elektronicznej jak i papierowej, a w szczególności:
	1. wszystkie istniejące, wdrażane obecnie lub w przyszłości systemy informatyczne oraz papierowe, w których przetwarzane są dane osobowe podlegające ochronie;
	2. wszystkie lokalizacje - budynki i pomieszczenia, w których są lub będą przetwarzane informacje podlegające ochronie;
2. Do stosowania zasad określonych przez dokumenty Polityki zobowiązani są wszyscy pracownicy w rozumieniu Kodeksu Pracy, współpracownicy, wykonawcy oraz inne osoby mające dostęp do informacji podlegających ochronie, w tym członkowie zarządu podmiotu.

# Definicje

1. W Polityce oraz pozostałych dokumentach związanych z ochroną danych używanie są poniższe określenia i skróty, które należy rozumieć następująco:
2. **Administrator –** rozumie się przez to Fundację Familijny Poznań z siedzibą w Poznaniu, ul. Staszica 15;
3. **Fundację** **–** rozumie się przez to Fundację Familijny Poznań;
4. **Dane biometryczne** - oznaczają dane osobowe, które wynikają ze specjalnego przetwarzania technicznego, dotyczą cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej oraz umożliwiają lub potwierdzają jednoznaczną identyfikację tej osoby, takie jak wizerunek twarzy lub dane daktyloskopijne;
5. **Dane genetyczne** - oznaczają dane osobowe dotyczące odziedziczonych lub nabytych cech genetycznych osoby fizycznej, które ujawniają niepowtarzalne informacje o fizjologii lub zdrowiu tej osoby i które wynikają w szczególności z analizy próbki biologicznej pochodzącej od tej osoby fizycznej;
6. **Dane dotyczące zdrowia** - oznaczają dane osobowe o zdrowiu fizycznym lub psychicznym osoby fizycznej – w tym o korzystaniu z usług opieki zdrowotnej – ujawniające informacje o stanie jej zdrowia;
7. **Dane osobowe** – oznaczają 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;
8. **Identyfikator** – często określany mianem „login”. Rozumie się przez to ciąg znaków jednoznacznie identyfikujący osobę w systemie informatycznym;
9. **Inspektor Ochrony Danych** – **IOD**, osoba powołana przez zarząd, pełniąca nadzór nad przetwarzaniem danych osobowych. Zadania IOD sprecyzowane są w RODO.
10. **Naruszenie ochrony danych osobowych** - oznacza 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;
11. **Odbiorca** - oznacza 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;
12. **Ograniczenie przetwarzania** - oznacza oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;
13. **Organ nadzorczy** - oznacza Głównego Inspektora Ochrony Danych Osobowych lub Urząd Ochrony Danych Osobowych
14. **Osoba upoważniona** – rozumie się przez to osobę, która otrzymała od Administratora upoważnienie do przetwarzania danych;
15. **Podmiot przetwarzający** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który przetwarza dane osobowe w imieniu administratora;
16. **Polityka Bezpieczeństwa Informacji i Danych Osobowych** – dalej jako **Polityka**.Rozumie się przez to Politykę Bezpieczeństwa Informacji i Danych Osobowych w przedsiębiorstwie;
17. **Prezes Urzędu Ochrony Danych Osobowych** – dalej jako **PUODO**. Rozumie się przez to organ nadzorczy ochrony danych osobowych.
18. **Profilowanie** - oznacza dowolną formę 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;
19. **Pseudonimizacja** - oznacza 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;
20. **Przetwarzane** - oznacza 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;
21. **RODO** – używane zamiennie z **Rozporządzenie**, 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);
22. **Rozporządzenie** – używane zamiennie z **RODO**,
23. **Siedziba** – siedziba Fundacji Familijny Poznań znajdująca się w Poznaniu, ul. Staszica 15;
24. **Strona trzecia** - oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe;
25. **System informatyczny** - rozumie się przez to zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych osobowych;
26. **System papierowy** - rozumie się przez to zespół procedur organizacyjnych, związanych z mechanicznym przetwarzaniem informacji oraz wyposażenia i środków trwałych używanych w celu przetwarzania danych osobowych na papierze;
27. **Urząd Ochrony Danych Osobowych** - dalej jako **UODO**. Rozumie się przez to organ nadzorczy ochrony danych osobowych;
28. **Upoważnienie** – rozumie się przez to oświadczenie Administratora wskazujące osobę uprawnioną do przetwarzania danych osobowych;
29. **Usuwanie danych** – rozumie się przez to zniszczenie danych osobowych lub taką ich modyfikację, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
30. **Użytkownik** - rozumie się przez to osobę upoważnioną przez Administratora do przetwarzania danych osobowych w systemie komputerowym;
31. **Użytkownik uprzywilejowany** – rozumie się przez to osobę upoważnioną o uprawnieniach administratora systemu informatycznego;
32. **Zabezpieczenie danych w systemie informatycznym** - rozumie się przez to wdrożenie i eksploatację stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem;
33. **Zgoda osoby, której dane dotyczą** - oznacza 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;

# Postanowienia ogólne

1. Administratorem Państwa danych osobowych jest Fundacja Familijny Poznań z siedzibą w Poznaniu przy ul. Staszica 15, 60-526 Poznań, zarejestrowana w Sądzie Rejonowym Poznań – Nowe Miasto i Wilda w Poznaniu, VIII Wydział Gospodarczy Krajowego Rejestru Sądowego pod numerem KRS 0000044866, NIP: 7781395875.
2. W celu zapewnienia ochrony informacji i danych osobowych Administrator wdraża niniejszą politykę i deklaruje swoje pełne zaangażowanie w ochronę danych osobowych.
3. Administrator zapewnia przetwarzanie danych osobowych zgodnie z prawem. Dane zbierane są w wyznaczonym celu, w zakresie adekwatnym do tego celu.
4. Ochrona bezpieczeństwa danych osobowych rozumiana jest, jako zapewnienie ich poufności, integralności, rozliczalności oraz dostępności na odpowiednim poziomie. Miarą bezpieczeństwa jest poziom ponoszonego ryzyka.
5. Zastosowane zabezpieczenia zapewniają:
	1. poufność danych – rozumiana jako właściwość zapewniającą, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;
	2. integralność danych - rozumiana jako niemożność jakiejkolwiek nieautoryzowanej modyfikacji, zarówno zamierzonej, jak i przypadkowej;
	3. dostępność informacji - rozumiana jako zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią zasobów wtedy, gdy jest to potrzebne;
	4. rozliczalność - rozumiana jako podejmowanie działań w celu udokumentowania działań pozostających w zgodności z zasadami ochrony danych osobowych;
	5. zarządzanie ryzykiem - rozumiane jako proces identyfikowania, kontrolowania i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa przetwarzania danych osobowych,
	6. legalność – rozumianą jako przetwarzanie danych zgodnie z prawem.
6. Polityka wraz z wymienionymi w niej dokumentami opisuje środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych osobowych odpowiednią dla zidentyfikowanych zagrożeń.

# Odpowiedzialność

1. Odpowiedzialność Inspektora Ochrony Danych, jeżeli zostanie powołany:
	1. nadzorowanie przestrzegania zasad ochrony danych osobowych zarówno w systemach informatycznych, jak również w zbiorach danych osobowych prowadzonych w formie papierowej lub elektronicznej,
	2. monitorowanie przestrzegania strategii Administratora lub Podmiotu przetwarzającego w dziedzinie ochrony danych osobowych,
	3. informowanie Administratora lub Podmiotu przetwarzającego oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy przepisów prawa w tym RODO i doradzanie im w tej sprawie;
	4. udzielanie porad na żądanie co do oceny skutków pod kątem ochrony danych oraz monitorowanie ich wykonania;
	5. współpraca z organem nadzorczym,
	6. pełnienie funkcji punktu kontaktowego wobec organu nadzorczego,
	7. pełnienie funkcji punktu kontaktowego dla podmiotów danych.
2. Odpowiedzialność osób upoważnionych do przetwarzania danych:
	1. znajomość, zrozumienie i stosowanie w możliwie najszerszym zakresie wszelkich dostępnych środków ochrony danych osobowych,
	2. przetwarzanie danych osobowych zgodnie z obowiązującymi przepisami prawa oraz przyjętymi regulacjami, w tym ustalonymi regulacjami wewnętrznymi,
	3. zachowanie w tajemnicy danych osobowych oraz informacji o sposobach ich zabezpieczenia i przetwarzania, również po odwołaniu upoważnienia, a także po ustaniu zatrudnienia,
	4. ochrona danych osobowych oraz środków przetwarzających dane osobowe przed nieuprawnionym dostępem, ujawnieniem, modyfikacją, zniszczeniem lub zniekształceniem,
	5. informowanie o wszelkich incydentach, podejrzeniach naruszenia oraz słabościach systemu przetwarzającego dane osobowe do przełożonego,
	6. poinformowanie wyznaczonych osób, w tym przełożonych o wystąpieniu incydentu związanego z ochroną danych osobowych.

# Obowiązki Administratora

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia wynikające z przetwarzania, administrator – zarówno przy określaniu sposobów przetwarzania, jak i w czasie samego przetwarzania wdraża odpowiednie środki techniczne i organizacyjne, takie jak pseudonimizacja, zaprojektowane w celu skutecznej realizacji zasad ochrony danych, takich jak minimalizacja danych, oraz w celu nadania przetwarzaniu niezbędnych zabezpieczeń, tak by spełnić wymogi RODO, chronić prawa osób, których dane dotyczą i aby móc to wykazać. Środki te są w razie potrzeby poddawane przeglądom i uaktualniane.
2. Administrator jest odpowiedzialny za przestrzeganie przepisów RODO i musi być w stanie wykazać ich przestrzeganie („rozliczalność”).
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. Stosowanie zatwierdzonych kodeksów postępowania, lub zatwierdzonego mechanizmu certyfikacji, o których mowa w RODO w art. 40 i 42 może być wykorzystane, jako element dla stwierdzenia przestrzegania przez administratora ciążących na nim obowiązków.
5. Administrator w szczególności zapewnia:
	1. nadzór nad bezpieczeństwem danych osobowych,
	2. przetwarzanie danych zgodnie z uregulowaniami Polityki;
	3. wydawanie i anulowanie upoważnień do przetwarzania danych;
	4. dopuszczenie do przetwarzania danych osobowych wyłącznie osób posiadających upoważnienie;
	5. prowadzenie ewidencji osób upoważnionych;
	6. zapoznanie osób upoważnionych do przetwarzania danych z przepisami o ochronie danych osobowych, organizowanie regularnych szkoleń;
	7. środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych;
	8. odpowiednio zabezpieczone systemy i sprzęt informatyczny;
	9. terminowe udzielanie informacji na wniosek osób, które zwróciły z wnioskiem o udzielenie informacji;
	10. w przypadku naruszenia ochrony danych osobowych, bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłaszania go organowi nadzorczemu, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych;
	11. inicjowanie i podejmowanie przedsięwzięć w zakresie doskonalenia ochrony danych osobowych,
	12. zgłoszenie powołania Inspektora Ochrony Danych do Prezesa Urzędu Ochrony Danych Osobowych.
6. W razie wykazania przez osobę, której dane są przetwarzane, że dane są nieaktualne, niekompletne, błędne lub zostały zebrane z naruszeniem prawa, Administrator bez zbędnej zwłoki podejmuje odpowiednie działania, w tym uzupełnienie, uaktualnienie, usunięcie danych i zaprzestanie ich przetwarzania.
7. W przypadku uaktualnienia danych, Administrator informuje o naniesionych zmianach bez zbędnej zwłoki innych administratorów, którym udostępnił zbiór danych.
8. Administrator i podmiot przetwarzający oraz – gdy ma to zastosowanie – ich przedstawiciele na żądanie współpracują z organem nadzorczym w ramach wykonywania przez niego swoich zadań.
9. 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 zgodnie z artykułem 35 RODO.
10. 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 zgodnie z artykułem 36 RODO.
11. Administrator danych ma obowiązek zapoznać z treścią Polityki każdą osobę zaangażowaną w przetwarzanie danych osobowych.

# Inspektor Ochrony Danych

1. Administrator powołuje Inspektora Ochrony Danych (IOD).
2. Administrator zapewnia, by IOD był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.
3. Administrator wspiera IOD w wypełnianiu przez niego zadań, o których mowa w art. 39 RODO, zapewniając mu zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego wiedzy fachowej.
4. Administrator zapewnia, by IOD nie otrzymywał instrukcji dotyczących wykonywania tych zadań. Nie jest on odwoływany ani karany przez administratora ani podmiot przetwarzający za wypełnianie swoich zadań. IOD bezpośrednio podlega najwyższemu kierownictwu, to jest zarządowi.
5. Osoby, których dane dotyczą, mogą kontaktować się z IOD we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.
6. IOD jest zobowiązany do zachowania tajemnicy co do wykonywania swoich zadań.
7. IOD może wykonywać inne zadania i obowiązki. Administrator zapewnia, by takie zadania i obowiązki nie powodowały konfliktu interesów.
8. IOD jest wyznaczany na podstawie kwalifikacji zawodowych, a w szczególności wiedzy fachowej na temat prawa i praktyk w dziedzinie ochrony danych oraz umiejętności wypełnienia zadań, o których mowa w art. 39 RODO.
9. IOD może być członkiem personelu administratora lub wykonywać zadania na podstawie umowy o świadczenie usług.
10. Imię, Nazwisko i dane kontaktowe IOD oraz ewentualnych zastępców zawarte są w załączniku „PB\_01 Lista kontaktowa ochrony danych osobowych”.
11. W przypadku powołania IOD, Administrator publikuje dane kontaktowe IOD i zawiadamia o nich organ nadzorczy.
12. Administrator zgłasza fakt powołania Inspektora Ochrony Danych Osobowych w terminie 14 dni od dnia powołania do Prezesa Urzędu Ochrony Danych Osobowych. W zawiadomieniu Administrator podaje:
	1. imię i nazwisko inspektora,
	2. adres poczty elektronicznej lub numer telefonu inspektora,
	3. imię i nazwisko oraz adres zamieszkania, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna;
	4. firmę przedsiębiorcy oraz adres miejsca prowadzenia działalności gospodarczej, w przypadku gdy administratorem lub podmiotem przetwarzającym jest osoba fizyczna prowadząca działalność gospodarczą;
	5. pełną nazwę oraz adres siedziby, w przypadku gdy administratorem lub podmiotem przetwarzającym jest podmiot inny niż wskazany w pkt c i d powyżej;
	6. numer identyfikacyjny REGON, jeżeli został nadany administratorowi lub podmiotowi przetwarzającemu.
13. IOD wypełnia swoje zadania z należytym uwzględnieniem ryzyka związanego z operacjami przetwarzania, mając na uwadze charakter, zakres, kontekst i cele przetwarzania.
14. Wszelkie czynności, które niniejsza Polityka definiuje, jako obowiązki IOD mogą być również wykonywane przez Administratora, to jest przez zarząd.

# Analiza ryzyka

1. Niniejszy rozdział opisuje procedurę przeprowadzenia analizy ryzyka w celu zabezpieczenia danych osobowych w Fundacji Familijny Poznań adekwatnie do zidentyfikowanych zagrożeń wynikających z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych.
2. Przez ryzyko rozumieć należy wskaźnik stanu lub zdarzenia, które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat, które może spowodować.
3. Mówiąc o ryzyku naruszenia praw i wolności osób fizycznych na gruncie RODO, konieczne jest uwzględnienie prawdopodobieństwa wystąpienia określonego zdarzenia będącego naruszeniem, oraz powagi tego zdarzenia, tj. wielkości szkody, jakie zdarzenie to może spowodować w odniesieniu do osoby, której dane dotyczą.
4. Przy szacowaniu prawdopodobieństwa incydentu zwykle uwzględnia się następujące czynniki: statystyki dotyczące podobnych zdarzeń, atrakcyjność aktywu, czynniki środowiskowe, rodzaje podatności, a także istniejące zabezpieczenia.
5. Przeprowadzenie oceny ryzyka naruszenia praw i wolności osób fizycznych przebiega w następujących etapach:
	1. Identyfikacja czynności przetwarzania
	2. Ocena zagrożeń
	3. Ocena skutków (konsekwencji)
	4. Ocena prawdopodobieństwa wystąpienia zagrożenia
	5. Ocena poziomu ryzyka
6. Po przeprowadzeniu szacowania następstw oraz po określeniu prawdopodobieństwa wystąpienia poszczególnych incydentów przeprowadzane jest określanie poziomu ryzyka. Stosowaną metodą jest zdefiniowanie poziomu ryzyka jako iloczynu prawdopodobieństwa i skutków wystąpienia danego incydentu. Na tym etapie wykorzystuje się macierz ryzyka, która pozwala zobrazować poziomy ryzyka.
7. Wyróżnia się 4 możliwe rodzaje postępowań z ryzykiem. Są to:
	1. modyfikowanie (redukcja) ryzyka – polega na obniżeniu poziomu ryzyka (np. poprzez zmianę prawdopodobieństwa wystąpienia określonego zdarzenia lub zmniejszenie skutków jego wystąpienia),
	2. zachowanie (akceptacja) ryzyka – to świadoma i obiektywna decyzja o niewprowadzaniu żadnych zmian w działaniu organizacji (zabezpieczeń), jeżeli poziom ryzyka spełnia przyjęte kryteria akceptowania ryzyka;
	3. unikanie ryzyka – polega na unikaniu przez organizację działań, które powodują powstanie określonych typów ryzyka, np. w przypadku, gdy zidentyfikowane ryzyka są zbyt wysokie lub koszt wdrożenia zabezpieczeń nie jest adekwatny do zysków;
	4. dzielenie (przeniesienie) ryzyka – polega na wykupieniu ubezpieczenia od jakiegoś zdarzenia lub scedowaniu skutków ryzyka na kontrahenta (np. podwykonawcę).
8. Informacje szczegółowe na temat przeprowadzonej analizy ryzyka zawarte są w dokumentacji:
	1. AR Ogólna ocena ryzyka,
	2. AR\_01 Identyfikacja procesów przetwarzania danych
	3. AR\_02 Szacowanie ryzyka (rejestr ryzyk).
9. Administrator zobowiązuje się do regularnego przeprowadzania analizy ryzyka, co najmniej raz w roku bądź w zależności od potrzeb i wprowadzonych nowych obszarów przetwarzania danych czy też nowych rozwiązań, systemów, zabezpieczeń.
10. Administrator wprowadził procedurę oceny skutków dla ochrony danych, która stanowi załącznik POS Procedura oceny skutków dla ochrony danych.

# Przetwarzanie danych

1. Dane osobowe muszą być zgodnie z zasadami określonymi w artykule 5 RODO, tj. dane osobowe muszą być:
	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; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane ("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; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy niniejszego rozporządzenia w celu ochrony praw i wolności osób, których dane dotyczą ("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").
2. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach określonych w artykule 6 RODO. Przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, 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.
3. Za prawnie uzasadniony interes Administratora wymieniony w artykule 6 RODO uznaje się w szczególności dochodzenie roszczeń z tytułu prowadzonej działalności oraz marketing bezpośredni własnych produktów lub usług, przy czym przy podejmowaniu działań marketingowych za pomocą środków komunikacji elektroniczne należy stosować przepisy ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz.U. z 2013 r. poz. 1422) oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne (Dz.U. z 2014 r. poz. 243), które wprowadzają dodatkową ochronę.
4. W razie wątpliwości, co do podstaw prawnych dla przetwarzania danych należy skontaktować się z IOD lub koordynatorem wymieniony w załączniku PB\_01 lub z członkiem zarządu. Do czasu uzyskania odpowiedzi należy wstrzymać przetwarzanie danych, co do których istnieją wątpliwości.

# Zgody

1. Jeżeli przetwarzanie odbywa się na podstawie zgody, administrator musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych oraz spełnić pozostałe warunki wymienione w artykułach 7 i 8 RODO, w tym odróżnić zgodę od pozostałych kwestii oraz umożliwić cofnięcie zgody w dowolnym momencie.
2. Zgody należy wzorować na klauzulach zawartych w załączniku „PB\_02 Wzory klauzul informacyjnych i zgód odbieranych od osób, których dane są przetwarzane”.

# Szczególne kategorie danych osobowych

1. Zabrania się przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby za wyjątkiem sytuacji opisanych w artykule 9 RODO.
2. Szczególne kategorie danych osobowych mogą być przetwarzane, jeżeli jest spełniony jeden z poniższych warunków:
	1. osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach, chyba że prawo Unii lub prawo państwa członkowskiego przewidują, iż osoba, której dane dotyczą, nie może uchylić zakazu, o którym mowa w ust. 1;
	2. przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone prawem Unii lub prawem państwa członkowskiego, lub porozumieniem zbiorowym na mocy prawa państwa członkowskiego przewidującymi odpowiednie zabezpieczenia praw podstawowych i interesów osoby, której dane dotyczą;
	3. 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;
	4. przetwarzania dokonuje się w ramach uprawnionej działalności prowadzonej z zachowaniem odpowiednich zabezpieczeń przez fundację, stowarzyszenie lub inny niezarobkowy podmiot o celach politycznych, światopoglądowych, religijnych lub związkowych, pod warunkiem że przetwarzanie dotyczy wyłącznie członków lub byłych członków tego podmiotu lub osób utrzymujących z nim stałe kontakty w związku z jego celami oraz że dane osobowe nie są ujawniane poza tym podmiotem bez zgody osób, których dane dotyczą;
	5. przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
	6. przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
	7. przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie i konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą;
	8. przetwarzanie jest niezbędne do celów profilaktyki zdrowotnej lub medycyny pracy, do oceny zdolności pracownika do pracy, diagnozy medycznej, zapewnienia opieki zdrowotnej lub zabezpieczenia społecznego, leczenia lub zarządzania systemami i usługami opieki zdrowotnej lub zabezpieczenia społecznego na podstawie prawa Unii lub prawa państwa członkowskiego lub zgodnie z umową z pracownikiem służby zdrowia;
	9. przetwarzanie jest niezbędne ze względów związanych z interesem publicznym w dziedzinie zdrowia publicznego, takich jak ochrona przed poważnymi transgranicznymi zagrożeniami zdrowotnymi lub zapewnienie wysokich standardów jakości i bezpieczeństwa opieki zdrowotnej oraz produktów leczniczych lub wyrobów medycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które przewidują odpowiednie, konkretne środki ochrony praw i wolności osób, których dane dotyczą, w szczególności tajemnicę zawodową;
	10. przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie prawa Unii lub prawa państwa członkowskiego, które są proporcjonalne do wyznaczonego celu, nie naruszają istoty prawa do ochrony danych i przewidują odpowiednie, konkretne środki ochrony praw podstawowych i interesów osoby, której dane dotyczą.
3. Przetwarzania danych osobowych dotyczących wyroków skazujących oraz naruszeń prawa wolno dokonywać wyłącznie pod nadzorem władz publicznych lub jeżeli przetwarzanie jest dozwolone prawem.

# Uprawnienia osób fizycznych i obsługa ich żądań

1. Administrator danych (ADO) weryfikuje i zapewnia możliwość efektywnego wykonania praw osoby fizycznej, zapewniając jednocześnie odpowiednie warunki, aby prawa osoby fizycznej były realizowane terminowo, w sposób wymagany przez RODO oraz dokumentowane.
2. Administrator podejmuje odpowiednie środki, aby w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem – w szczególności gdy informacje są kierowane do dziecka – 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. 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.
3. Administrator ułatwia osobie, której dane dotyczą, wykonanie praw przysługujących jej na mocy art. 15–22 RODO. Przyjmuje się następujące sposoby przekazywania informacji służące ułatwianiu zgłaszania żądań z art. 15-22 RODO a także wniosków o wycofanie zgody:
	1. osobiście w siedzibie Administratora,
	2. listownie na adres Administratora,
	3. drogą elektroniczną na adres iod@familijny.pl
4. W ramach zgłoszonych żądań i odpowiedzi osoba upoważniona, wskazana w załączniku PB\_01, będzie odnotowywać m.in. wpływ żądania (kto, kiedy i jakiej treści i w jaki sposób) i udzielenia odpowiedzi na żądanie (kto, kiedy i jakiej treści, w jaki sposób), a także sposób spełnienia obowiązku (np. usunięcie danych) wskazując przy tym termin realizacji prawa podmiotu. Wzór rejestru stanowi załącznik numer PB\_11 Rejestr realizacji praw podmiotów danych.
5. W przypadkach, o których mowa w art. 11 ust. 2 RODO, administrator nie odmawia podjęcia działań na żądanie osoby której dane dotyczą pragnącej wykonać prawa przysługujące jej na mocy art. 15–22 RODO, chyba że wykaże, iż nie jest w stanie zidentyfikować osoby, której dane dotyczą.
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. Jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, administrator może:
* pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań; albo
* odmówić podjęcia działań w związku z żądaniem.
1. Każdy pracownik, do którego mogłoby trafić żądanie w ramach prawa podmiotu, jest zobowiązany do niezwłocznego poinformowania o tym osoby upoważnionej do obsługi praw podmiotu (wskazanej w załączniku PB\_01) lub IOD i przekazania mu treści żądania. Upoważniona osoba ocenia komunikat pod kątem zgodności z przepisami RODO.
2. Osoba upoważnia do obsługi praw podmiotu (wskazana w załączniku PB\_01)/IOD ostatecznie decyduje o tym czy pozytywnie zrealizować żądanie.
3. Osoba technicznie realizująca wniosek odpowiada wyłącznie za techniczny aspekt realizacji praw (działa na polecenie właściciela procesu).
4. Osoba upoważnia do obsługi praw podmiotu (wskazana w załączniku PB\_01)/IOD rejestruje żądanie w ewidencji praw podmiotów:
	1. weryfikuje rodzaj żądania i w razie wątpliwości prosi osobę, żądającą o podanie dodatkowych informacji umożliwiających sprecyzowanie żądania;
	2. ustala w ramach jakiej kategorii podmiotów (np. kandydaci do pracy, pracownicy, byli pracownicy, osoby korzystające z usług świadczonych przez Administratora) należy identyfikować zgłaszającego

 Na tej podstawie należy określić:

* 1. w ramach których procesów przetwarzania danych (wskazanych w rejestrze czynności) dane zgłaszającego (tej kategorii podmiotów) mogą być przetwarzane (może to być jeden lub więcej procesów przetwarzania danych),
	2. (na podstawie rejestru czynności ) jaki zakres danych jest istotny z punktu widzenia identyfikacji danych osoby zgłaszającej żądanie (odszukania tych danych i przypisania do wyodrębnionej osoby) oraz weryfikacji tożsamości osoby żądającej.

 W następnej kolejności należy:

* 1. sprawdzić, czy żądanie jest możliwe do zrealizowania oraz czy nie zachodzą przesłanki wyłączające możliwość realizacji żądania, ewentualnie przesłanki pobrania opłaty,
	2. zweryfikować czas oraz środki potrzebne na realizację żądania a także kto będzie odpowiedzialny za techniczną obsługę żądania oraz podjęcia decyzji o sposobie realizacji żądania;
	3. jeżeli żądanie jest zasadne należy przekazać odpowiedź podmiotowi, który wniósł żądanie, wskazując sposób realizacji żądania, w terminie wskazanym powyżej,
	4. odnotować sposób realizacji żądania ewidencji praw podmiotów.

# Prawo dostępu przysługujące osobie, której dane dotyczą

1. 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 wymienionych w artykule 15 RODO.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana o odpowiednich zabezpieczeniach, o których mowa w RODO w art. 46, związanych z przekazaniem.
3. Administrator dostarcza osobie, której dane dotyczą, kopie danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, administrator może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacji udziela się powszechnie stosowaną drogą elektroniczną.

# Prawo do sprostowania danych (art. 16 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego **sprostowania** dotyczących jej danych osobowych, które są nieprawidłowe. Z uwzględnieniem celów przetwarzania, osoba, której dane dotyczą, ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

# Prawo do usunięcia danych („prawo do bycia zapomnianym” art. 17 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora niezwłocznego **usunięcia** dotyczących jej danych osobowych, a administrator ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:
	1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
	2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie z art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO, i nie ma innej podstawy prawnej przetwarzania;
	3. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO wobec przetwarzania;
	4. dane osobowe były przetwarzane niezgodnie z prawem;
	5. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega administrator;
	6. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.
2. Powyższe zasady nie mają zastosowania, w zakresie w jakim przetwarzanie jest niezbędne:
	1. do korzystania z prawa do wolności wypowiedzi i informacji;
	2. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Unii lub prawa państwa członkowskiego, któremu podlega administrator, lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi;
	3. z uwagi na względy interesu publicznego w dziedzinie zdrowia publicznego zgodnie z art. 9 ust. 2 lit. h) oraz i) RODO i art. 9 ust. 3 RODO;
	4. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO,
	5. do ustalenia, dochodzenia lub obrony roszczeń.

# Prawo do ograniczenia przetwarzania (art. 18 RODO)

1. Osoba, której dane dotyczą, ma prawo żądania od administratora ograniczenia przetwarzania w następujących przypadkach:
	1. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych - na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
	2. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
	3. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
	4. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania - do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

# Obowiązek Administratora powiadomienia o sprostowaniu lub usunięciu danych osobowych lub o ograniczeniu przetwarzania

1. Administrator informuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania, których dokonał zgodnie z art. 16, art. 17 ust. 1 i art. 18 RODO, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Administrator informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.
2. **Prawo do przenoszenia danych (art. 20 RODO)**
3. Osoba, której dane osobowe dotyczą, ma prawo otrzymać 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, jeżeli:
	1. przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) RODO lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO; oraz
	2. przetwarzanie odbywa się w sposób zautomatyzowany.
4. Wykonując prawo do przenoszenia danych na mocy ust. 1, osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez Administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.
5. **Prawo do sprzeciwu (art. 21 RODO)**
6. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw - z przyczyn związanych z jej szczególną sytuacją - wobec przetwarzania dotyczących jej danych osobowych opartego na art. 6 ust. 1 lit. e) lub f) RODO, w tym profilowania na podstawie tych przepisów. 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.
7. 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.
8. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych nie wolno już przetwarzać do takich celów.
9. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie, o którym mowa w ust. 1 i 2, oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.
10. **Zautomatyzowane podejmowanie decyzji w indywidualnych przypadkach, w tym profilowanie (art. 22 RODO)**
11. Osoba, której dane dotyczą, ma prawo do tego, by nie podlegać decyzji, która opiera się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu, i wywołuje wobec tej osoby skutki prawne lub w podobny sposób istotnie na nią wpływa.
12. Powyższy ustęp nie ma zastosowania, jeżeli ta decyzja:
	1. jest niezbędna do zawarcia lub wykonania umowy między osobą, której dane dotyczą, a administratorem,
	2. jest dozwolona prawem Unii lub prawem państwa członkowskiego, któremu podlega administrator i które przewiduje właściwe środki ochrony praw, wolności i prawnie uzasadnionych interesów osoby, której dane dotyczą; lub
	3. opiera się na wyraźnej zgodzie osoby, której dane dotyczą.

# Informacje podawane podczas zbierania danych

1. W sytuacji gdy dane zbierane są od osoby której dotyczą, administrator podczas pozyskiwania danych osobowych, podaje osobie, której dane dotyczą, informacje opisane w artykule 13 RODO, wzorując się na szablonie z załącznika „PB\_02 Wzory klauzul informacyjnych i zgód odbieranych od osób, których dane są przetwarzane”. Osoby nie trzeba informować, jeśli już dysponuje tymi informacjami;
2. W sytuacji, gdy dane nie są pozyskiwane od osoby której dotyczą:
	1. administrator podaje osobie, której dane dotyczą, informacje opisane w artykule 14 RODO, wzorując się na szablonie z załącznika „PB\_02 Wzory klauzul informacyjnych i zgód odbieranych od osób, których dane są przetwarzane”
	2. administrator podaje informacje w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
	3. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
	4. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu;
	5. Jeżeli administrator planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji.
3. W sytuacji, gdy dane nie są pozyskiwane od osoby, której dotyczą administrator może nie informować osoby jeśli zachodzą przesłanki określone w artykule 14 punkt 5 RODO.

# Powierzanie danych osobowych

1. Jeżeli przetwarzanie ma być dokonywane w imieniu administratora, korzysta on wyłącznie z usług takich podmiotów przetwarzających, które zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, by przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dane dotyczą.
2. Podmiot przetwarzający nie korzysta z usług innego podmiotu przetwarzającego bez uprzedniej szczegółowej lub ogólnej pisemnej zgody administratora. W przypadku ogólnej pisemnej zgody podmiot przetwarzający informuje administratora o wszelkich zamierzonych zmianach dotyczących dodania lub zastąpienia innych podmiotów przetwarzających, dając tym samym administratorowi możliwość wyrażenia sprzeciwu wobec takich zmian.
3. Przetwarzanie przez podmiot przetwarzający odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu i wiążą podmiot przetwarzający i administratora, określają przedmiot i czas trwania przetwarzania, charakter i cel przetwarzania, rodzaj danych osobowych oraz kategorie osób, których dane dotyczą, obowiązki i prawa administratora. Ta umowa lub inny instrument prawny stanowią w szczególności, że podmiot przetwarzający spełnia wymagania wymienione w artykule 28 RODO.
4. Wystarczające gwarancje, podmiot przetwarzający może wykazać między innymi poprzez stosowanie zatwierdzonego kodeksu postępowania lub zatwierdzonego mechanizmu certyfikacji o których mowa w RODO.
5. Umowa lub inny akt prawny, mają formę pisemną, w tym formę elektroniczną.
6. Przy podpisywaniu umów powierzenia danych z podmiotami należy stosować klauzule wskazane w załączniku „PB\_03 Wzór umowy powierzenia przetwarzania danych osobowych”.

# Budynki i pomieszczenia w których przetwarzane są dane osobowe

1. Administrator przetwarza dane osobowe w pomieszczeniach do tego przeznaczonych, nazywanych obszarem przetwarzania, w sposób uniemożliwiający dostęp do danych osobom nieupoważnionym.
2. Administrator przetwarza dane w wielu placówkach na terenie Polski.
3. Dostęp do pomieszczeń regulowany jest przez dokument zawierający zasady gospodarowania kluczami, którego wzór stanowi załącznik „PGK Wzór procedur gospodarowania kluczami”. Każda placówka opracowuje osobną Procedurę gospodarowania kluczami.
4. Wykaz budynków i pomieszczeń w których przetwarzane są dane osobowe zawarto w załączniku „PB\_04 Wykaz budynków, placówek, w których przetwarzane są dane osobowe”.

# Zabezpieczenia techniczne

1. Dane osobowe u Administratora mogą być przetwarzane wyłącznie w pomieszczeniach przetwarzania danych osobowych, do których zalicza się
	1. pomieszczenia biurowe, w których zlokalizowane są stacje robocze,
	2. pomieszczenia, w których przechowywane są sprawne oraz uszkodzone elektroniczne nośniki informacji, kopie zapasowe,
	3. pomieszczenia, w których przechowuje się dokumenty źródłowe oraz wydruki z systemu informatycznego,
	4. pomieszczenia, w których zlokalizowane są zbiory nieinformatyczne.
2. Przebywanie wewnątrz obszarów, w których są przetwarzane dane osobowe, osób nieuprawnionych do przetwarzania danych osobowych jest dopuszczalne tylko w obecności osoby upoważnionej do przetwarzania tych danych.
3. Budynki lub pomieszczenia, w których przetwarzane są dane osobowe, powinny być zamykane podczas nieobecności osób upoważnionych do przetwarzania danych osobowych, w sposób ograniczający możliwość dostęp do nich osobom nieupoważnionym.
4. W celu ograniczenia dostępu osób nieupoważnionych do pomieszczeń, w których zlokalizowano przetwarzanie danych osobowych, należy zapewnić:
	1. jasne określenie granic obszaru przetwarzania danych osobowych oraz umiejscowienie dostosowane do wymagań bezpieczeństwa w odniesieniu do aktywów znajdujących się wewnątrz obszaru,
	2. jednolite granice budynków lub pomieszczeń, gdzie zlokalizowano środki przetwarzania danych osobowych (tzn. aby granice nie miały luk lub punktów, przez które łatwo się włamać),
	3. ściany zewnętrzne pomieszczeń solidnej konstrukcji oraz wszystkie drzwi zewnętrzne odpowiednio zabezpieczone przed nieautoryzowanym dostępem za pomocą mechanizmów zabezpieczeń, np. alarmów, zamków itp.,
	4. zamykanie drzwi i okien w pomieszczeniach pozostawianych bez dozoru oraz należy rozważyć zastosowanie mechanizmów zewnętrznej ochrony dla okien, szczególnie tych położonych na poziomie gruntu,
	5. system wykrywania włamań zgodnych z normami w strefach bezpieczeństwa oraz regularne jego testowanie.
5. Obszary bezpieczne powinny być odpowiednio zabezpieczone przed skutkami pożaru.
6. Ochrona obszarów bezpiecznych powinna być zapewniona poprzez odpowiednie fizyczne zabezpieczenia wejścia zapewniające, że tylko osoby upoważnione mogą uzyskać dostęp, w tym celu należy zapewnić:
	1. nadzorowanie pobytu osób nie będących pracownikami Administratora w obszarach bezpiecznych, chyba, że ich dostęp został wcześniej zaakceptowany.
	2. kontrolowanie i ograniczenie dostępu do obszarów, gdzie są przetwarzane dane osobowe tylko dla uprawnionego personelu.
	3. regularne przeglądanie praw dostępu do obszarów bezpiecznych i jeśli zachodzi potrzeba, uaktualnianie ich lub odbieranie.
7. Przetwarzanie danych osobowych jest zakazane w tych pomieszczeniach, w których osoby trzecie wykonują prace techniczne.
8. Nośniki elektroniczne zawierające dane osobowe powinny być ewidencjonowane i należy przechowywać w zamykanych szafach, które znajdują się w obszarach przetwarzania danych osobowych.

# Rejestr czynności przetwarzania danych osobowych oraz Rejestr kategorii

1. Administrator prowadzi rejestr czynności przetwarzania danych osobowych oraz rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora, których wzór stanowi załącznik „PB\_05 Wzór rejestru czynności przetwarzania i rejestru kategorii”.
2. Rejestry podzielone są na części obejmujące następujące obszary: administracja Fundacji, żłobki, przedszkola, szkoły.

# Określenie środków technicznych i organizacyjnych niezbędnych dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych

1. Uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, administrator 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 oraz podmiot przetwarzający podejmują działania w celu zapewnienia, by każda osoba fizyczna działająca z upoważnienia administratora lub podmiotu przetwarzającego, która ma dostęp do danych osobowych, przetwarzała je wyłącznie na polecenie administratora, chyba że wymaga tego od niej prawo.
4. Fundacja posiada metody i zasady zarządzania minimalizacją (privacy by default), a w tym:
	1. zasady zarządzania adekwatnością danych,
	2. zasady reglamentacji i zarządzania dostępem do danych,
	3. zasady zarzadzania okresem przechowywania danych i weryfikacji dalszej przydatności.
5. Fundacja zarządza zmianami mającymi wpływ na prywatność (privacy by design). W tym celu procedury uruchamiania nowych projektów i inwestycji w Fundacji uwzględniają konieczność oceny wpływu zmiany na ochronę danych, zapewnienie prywatności (a w tym zgodności celów przetwarzania, bezpieczeństwa danych i minimalizacji) już w fazie projektowania zmiany, inwestycji czy na początku nowego projektu.

# Obowiązki pracowników i współpracowników

1. Wszystkie osoby (pracownicy, współpracownicy) mające dostęp do danych osobowych, również te, które weszły w posiadanie informacji w sposób niezamierzony, zobowiązane są do:
	1. zachowania w tajemnicy zarówno danych osobowych jak i sposobów ich zabezpieczania, także po ustaniu współpracy z przedsiębiorstwem;
	2. zachowania szczególnej ostrożności podczas przetwarzania danych osobowych;
	3. podjęcia wszelkich środków chroniących dane przez nieuprawnionym dostępem, modyfikacją lub zniszczeniem i kradzieżą;
	4. przestrzegania niniejszej Polityki Bezpieczeństwa Informacji i Ochrony Danych Osobowych (dokument PB);
	5. przestrzegania Regulaminu korzystania z zasobów teleinformatycznych przedsiębiorstwa (dokument RIT);
	6. przestrzegania Procedury gospodarowania kluczami (dokument PGK);
	7. przestrzegania Polityki czystego biurka, wydruku, ekranu (dokument PCB);
	8. przechowywania dokumentów oraz przenośnych nośników danych zawierających dane osobowe w szafach zamykanych na klucz/kod oraz w pomieszczeniach zamykanych na klucz/kod oraz ograniczenia przetrzymywania danych osobowych na biurkach do niezbędnego minimum;
	9. porządkowania stanowiska pracy po zakończeniu pracy tak, aby zabezpieczyć dokumenty i nośniki elektroniczne z danymi osobowymi w przeznaczonych do tego szafkach lub pomieszczeniach;
	10. zamykania pomieszczeń, w których przetwarzane są dane osobowe na klucz/kod w przypadku ich opuszczania oraz podjęcia działań zapobiegających zgubieniu kluczy;
	11. niezwłocznego zgłaszania utraty kluczy do pomieszczeń, w których przetwarzane są dane zarządowi ;
	12. nie pozostawiania w pomieszczeniach, w których przetwarzane są dane osób nieupoważnionych bez nadzoru osoby upoważnionej do przetwarzania danych;
	13. ustawiania monitorów komputerów i laptopów, w taki sposób, aby uniemożliwić podgląd ekranu przez osoby postronne;
	14. w przypadku opuszczania stanowiska pracy, blokowania ekranu komputera tak, aby do odblokowania wymagane było podanie hasła;
	15. niezwłocznego niszczenia niepotrzebnych dokumentów papierowych zawierających dane osobowe za pomocą niszczarki lub przechowywania ich w takich miejscach, do których nie mają dostępu osoby postronne. Dopuszcza się przekazywanie dokumentów do niszczenia wyspecjalizowanej firmie, z którą zawarto umowę powierzenia przetwarzania danych;
	16. niszczenia nośników elektronicznych przy użyciu odpowiednich urządzeń (płyty CD i DVD należy niszczyć w niszczarce) lub odpowiedniego oprogramowania;
	17. zachowania szczególnej ostrożności podczas korzystania z urządzeń wielofunkcyjnych dostępnych dla wielu osób. Dokumenty muszą być odbierane lub wyjmowane z urządzenia niezwłocznie po wykonaniu operacji skanowania, kopiowania lub drukowania;
	18. usuwania danych po tym, gdy przestaną być potrzebne zgodnie z załącznikiem „PB\_10 Okresy retencji”;
	19. zaniechania kopiowania dokumentów identyfikacyjnych takich jak dowody osobiste, chyba że jest to jednoznacznie wymagane przez przepis prawa;
	20. ochrony wymienianych danych osobowych przed przechwyceniem, kopiowaniem, modyfikacją, błędnym wyborem drogi komunikacji i zniszczeniem;
	21. prowadzenia korespondencji w zakresie kadrowo - płacowym za pomocą listów poleconych;
	22. upewnienia się przed przekazaniem danych osobowych, czy rozmówca jest osobą upoważnioną do uzyskania określonych danych osobowych;
	23. zachowania szczególnej ostrożności przy udzielaniu informacji dotyczących danych osobowych przez telefon i poza zakład pracy;
	24. transportu danych osobowych w formie elektronicznej i papierowej pomiędzy obszarami, w których są przetwarzane dane osobowe w sposób ograniczający możliwość ich pozyskania i odczyt przez osoby nieupoważnione;
	25. stosowania zabezpieczeń i ograniczeń związanych z możliwościami przekazywania wiadomości za pomocą środków komunikacji, np. automatyczne przekazywanie poczty elektronicznej na zewnątrz.
	26. przekazywania dokumentów zawierających dane osobowe, sporządzone w formie papierowej, pomiędzy poszczególnymi komórkami organizacyjnymi w zaklejonych kopertach.

# Środki organizacyjne i techniczne

1. Budynki, w których przetwarza się dane osobowe nie mogą być narażone na wysoki poziom ryzyka. Należy unikać wyboru budynków znajdujących się na terenach zalewowych, narażonych na wyładowania atmosferyczne, sąsiadujących ze stajami benzynowymi lub zakładami przetwórstwa chemicznego.
2. W budynkach, w których przetwarzane są dane osobowe, stosuje się systemy ochrony przeciwpożarowej.
3. Danych w postaci papierowej nie można przechowywać w obszarach, nad którymi przebiegają rury stwarzające ryzyko zalania dokumentów lub w których występuje wysokie ryzyko zaprószenia ognia.
4. Szczegółowe środki techniczne zastosowane w pomieszczeniach zostały wymienione w załączniku „PB\_04 Wykaz budynków, placówek, w których przetwarzane są dane osobowe”.
5. W przypadku prowadzenia projektów, tworzenia lub modyfikowania procesów wymagane jest przestrzeganie wymagań ochrony danych osobowych określonych w RODO oraz niniejszym dokumencie.
6. Ryzyka związane z ochroną danych osobowych są regularnie identyfikowane, dokumentowane i przeglądane, nie rzadziej niż raz w roku kalendarzowym. Ryzyka mają przypisanych właścicieli odpowiedzialnych za ich monitorowanie oraz minimalizację (o ile analiza ryzyka wykaże, że jest to niezbędne). Dokumentacja dotycząca ryzyka jest utrzymywana w dokumencie „AR Analiza ryzyka” wraz z załącznikami.
7. Do niszczenia dokumentów wykorzystuje się niszczarki, które zapewniają odpowiedni stopień rozdrobnienia, zgodne z normą DIN 66399 o klasie nie niższej niż trzecia.
8. Dopuszczalne jest korzystanie z usług profesjonalnych firm specjalizujących się w niszczeniu dokumentów i nośników elektronicznych, po zawarciu z nimi odpowiednich umów powierzenia przetwarzania danych osobowych.
9. Do przetwarzania danych dopuszcza się wyłącznie osoby posiadające upoważnienia nadane przez Administratora.
10. Wdrożono procedurę postępowania w sytuacji naruszenia ochrony danych osobowych, zgodną w wymaganiami RODO, która stanowi załącznik „IPPN - Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych i zaistnienia zagrożeń dla ochrony danych”.
11. Osoby zatrudnione przy przetwarzaniu danych są zaznajomione z przepisami dotyczącymi ochrony danych osobowych oraz w zakresie zabezpieczeń systemu informatycznego i zabezpieczania danych papierowych.
12. Przetwarzanie danych osobowych dokonywane jest w warunkach zabezpieczających dane przed dostępem osób nieupoważnionych.
13. Przebywanie osób nieuprawnionych w pomieszczeniach, gdzie przetwarzane są dane osobowe jest dopuszczalne tylko w warunkach zapewniających bezpieczeństwo danych, w obecności osoby upoważnionej do przetwarzania danych osobowych.
14. Dane są usuwane po tym, gdy przestaną być potrzebne zgodnie z załącznikiem „PB\_10 Okresy retencji”.
15. W przypadku zakończenia przez Fundację Familijny Poznań współpracy z pracownikiem/współpracownikiem, Administrator wycofuje upoważnienie do przetwarzania danych i blokuje jakiekolwiek konta używane przez współpracownika/pracownika.
16. W przypadku zmiany roli przez pracownika/współpracownika, Administratora aktualizuje upoważnienie i dostępy do systemów nadane pracownikowi/współpracownikowi.
17. Sprzątanie pomieszczeń z danymi osobowymi jest wykonywane przez pracownika firmy, od którego odebrano oświadczenie o zachowaniu poufności.
18. Środki techniczne i organizacyjne dotyczące systemów informatycznych są zawarte w dokumentach załącznikach „RIT Regulamin korzystania z zasobów teleinformatycznych” oraz „PB\_04 Wykaz budynków i pomieszczeń".
19. Zasady pracy z dokumentami, wydrukami opisane są w załączniku „PCB Polityka czystego biurka, wydruku, ekranu”.

# Procedury przywrócenia dostępności danych osobowych w razie wystąpienia incydentu technicznego lub fizycznego

1. Administrator wyznaczył następujące obszary krytyczne dla organizacji systemu ochrony danych osobowych:
	1. z wykorzystaniem systemów informatycznych,
	2. bez udziału systemu informatycznego
2. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych z udziałem systemów informatycznych.
	1. Każda osoba jest zobowiązana do zgłaszania:
		* awarii systemów informatycznych wykorzystywanych do przetwarzania danych osobowych w przedsiębiorstwie,
		* awarii urządzeń wykorzystywanych do przetwarzania danych osobowych w przedsiębiorstwie,
		* braku zasilania sieci energetycznej przedsiębiorstwa,
		* braku dostępu do sieci internetowej przedsiębiorstwa;
	2. W sytuacji wystąpienie awarii należy niezwłocznie poinformować Administratora danych oraz odpowiednie podmioty technicznej dostawcy.
	3. Administrator zawiadamia niezwłocznie o wystąpieniu awarii podmiot pomocy technicznej.
	4. Czas reakcji i czas naprawy określa umowa pomiędzy Administratorem a osobą wykonującą naprawy, z zastrzeżeniem, że podjęcie czynności naprawczych powinno zostać podjęte niezwłocznie.
	5. Do czasu usunięcia awarii systemu informatycznego, Administrator wykorzystuje dokumentację papierową, która po usunięciu awarii systemu informatycznego jest niezwłocznie wprowadzana przez upoważnioną osobę do systemu.
	6. Wzór dokumentacji papierowej wykorzystywanej alternatywnie w trakcie awarii systemu informatycznego nie musi być ściśle określony. Powinien jednak zawierać elementy niezbędne do kompletnego wprowadzenia danych osobowych do systemu informatycznego. Jeśli dostawca oprogramowania informatycznego przewidział taką sytuację, stosuje się szablony dokumentów papierowych dostarczonych przez dostawcę oprogramowania.
	7. W sytuacji uszkodzenia bazy danych, należy wykorzystać kopię zapasową w celu przywrócenia poprawności systemu informatycznego.
	8. Z czynności mających na celu przywrócenie pracy systemu Administrator sporządza stosowną notatkę.
	9. W przypadku konieczności użytkowania sieci i przedłużającej się awarii należy skorzystać z Internetu mobilnego jako alternatywne źródło.
3. Zapewnienie ciągłości pracy systemu przetwarzania danych osobowych bez udziału systemów informatycznych:
	1. Sytuacjami, które mogą uniemożliwiać przetwarzanie danych osobowych bez wykorzystania systemów informatycznych mogą być:
		* brak możliwości dostępu do pomieszczeń, w których przetwarzane są dane osobowe,
		* brak możliwości wykorzystania pomieszczeń, w których przetwarzane są dane osobowe ze względu na awarię np. zalanie pomieszczenia, awaria ogrzewania.
	2. W przypadku wystąpienia sytuacji, o których mowa w niniejszym rozdziale każda osoba przetwarzająca dane osobowe ma obowiązek kontaktu telefonicznego i zgłoszenia tego faktu Administratorowi.
	3. Administrator według najlepszej wiedzy i uznania niezwłocznie zgłasza zaistniałe usterki kompetentnym podmiotom według właściwości ich działania.
	4. W przypadku braku możliwości wykorzystania pomieszczeń do przetwarzania danych osobowych z powodu awarii, Administrator jest zobowiązany wskazać użytkownikowi inne, spełniające wszystkie normy pomieszczenie na terenie przedsiębiorstwa, w którym będzie on mógł kontynuować swoje obowiązki oraz ewentualnie czasowo udostępnić klucze zapasowe do wybranych pomieszczeń.
4. Nadrzędnym obowiązkiem administratora jest zapewnienie ochrony życia i zdrowia pracowników oraz gości, w stosunku do ochrony danych osobowych.

# Szkolenia

1. Każda osoba przed dopuszczeniem do przetwarzania danych osobowych i nadaniem upoważnienia odbywa szkolenie w zakresie ochrony danych osobowych. Szkolenie może zostać przeprowadzone w formie wykładu jak i z wykorzystaniem platformy e-learningowej.
2. Zakres szkolenia obejmuje zaznajomienie z przepisami oraz polityką i instrukcjami obowiązującymi u Administratora.
3. Za przeprowadzenie szkolenia odpowiada Administrator danych.
4. Odbycie szkolenia jest dokumentowane oświadczeniem uczestnika, o wzięciu udziału w szkoleniu, zrozumieniu jego treści oraz zobowiązaniu się do przestrzegania przedstawionych w trakcie szkolenia zasad ochrony danych osobowych oraz zachowaniu poufności. Oświadczenie może mieć formę papierową lub elektroniczną. Wzór oświadczenia stanowi załącznik „PB\_06 Wzór oświadczenia o zachowaniu poufności”.

# Sprawdzenia i audyty

1. Sprawdzenia i audyty są dokonywane dla Administratora lub organu nadzorczego. Sprawdzenie może być doraźne, planowe lub na żądanie organu nadzorczego.
2. Jeśli powołano IOD, to IOD odpowiada za wykonanie kontroli.
3. Administrator lub IOD działając w porozumieniu z Administratorem może zlecać sprawdzenia firmom zewnętrznym.
4. Sprawdzenia dokonuje się nie rzadziej niż raz w każdym roku kalendarzowym.
5. Po zakończeniu sprawdzenia przygotowywane jest sprawozdanie w postaci elektronicznej lub papierowej przedstawiane zarządowi.

# Upoważnienia do przetwarzania danych osobowych

1. Administrator wydaje upoważnienia każdej osobie, która będzie przetwarzać dane osobowe.
2. Upoważnienie zawiera datę nadania oraz zakres upoważnienia.
3. Upoważnienia wydawane są na czas nieokreślony lub określony.
4. Upoważnienie może mieć formę papierową lub elektroniczną.
5. Osoby upoważnione, mogą przetwarzać dane osobowe tylko w zakresie wskazanym w upoważnieniu.
6. Osoba upoważniona nie ma prawa do nadawania dalszych upoważnień.
7. Procedura nadawania upoważnień do przetwarzania danych osobowych stanowi załącznik do niniejszej Polityki, tj. „PB\_12 Procedura nadawania upoważnień do przetwarzania danych osobowych”.
8. Wzór upoważnienia stanowi załącznik „PB\_07 Wzór upoważnienia do przetwarzania danych osobowych”.
9. Wzór odwołania upoważnienia stanowi załącznik „PB\_08 Wzór odwołania upoważnienia do przetwarzania danych osobowych”.

# Osoby uprawnione do wystawiania upoważnień

1. Upoważnienia uprawniające do przetwarzania danych osobowych dla pracowników Administratora wydaje Zarząd lub osoba upoważniona przez Zarząd.
2. Upoważnienia do przetwarzania danych osobowych obowiązują do czasu ustania stosunku pracy, współpracy, obowiązków związanych z przetwarzaniem danych osobowych lub upływu terminu, na jaki upoważnienie wydano.
3. Osoby upoważnione do wystawiania i odwoływania upoważnień wymienione są w załączniku „PB\_01 Lista kontaktowa ochrony danych osobowych”.

# Ewidencja upoważnień

1. Administrator prowadzi ewidencję osób upoważnionych, zgodnie ze wzorem „PB\_09 Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych”.
2. Ewidencja może być prowadzona w wersji papierowej lub elektronicznej.
3. Ewidencja zawiera imię, nazwisko, datę nadania, datę ustania, zakres upoważnienia.
4. Co najmniej raz w roku kalendarzowym dokonuje się przeglądu ewidencji upoważnień oraz przeglądu dostępów do systemów informatycznych w celu weryfikacji aktualności upoważnień oraz nadanych dostępów do systemów informatycznych.

# Postanowienia końcowe

1. Polityka jest dokumentem wewnętrznym i poufnym, dostępnym dla pracowników oraz współpracowników. Może być udostępniana innym podmiotom jedynie za zgodą Administratora.
2. Niektóre załączniki do Polityki są poufne i dostępne jedynie dla osób wskazanych przez zarząd.
3. Pracownicy i współpracownicy zobowiązani są do stosowania przy przetwarzaniu danych osobowych postanowień zawartych w Polityce.
4. Polityka obowiązuje od dnia jej zatwierdzenia.
5. Wobec osoby, która w przypadku naruszenia postanowień Polityki lub uzasadnionego domniemania takiego naruszenia nie podjęła działania określonego w niniejszym dokumencie, a w szczególności nie powiadomiła odpowiedniej osoby zgodnie z określonymi zasadami, a także, gdy nie zrealizowała stosownego działania dokumentującego ten przypadek, można wszcząć postępowanie dyscyplinarne.
6. Kara dyscyplinarna orzeczona wobec osoby uchylającej się od powiadomienia nie wyklucza odpowiedzialności karnej tej osoby oraz możliwości wniesienia wobec niej sprawy z powództwa cywilnego przez pracodawcę o zrekompensowanie poniesionych strat.
7. Treść polityki będzie przeglądana, i jeśli zajdzie taka konieczność aktualizowana, po zmianie przepisów ochrony danych osobowych, ale nie rzadziej niż raz w każdym roku kalendarzowym.
8. Zatwierdzenie nowej wersji Polityki wymaga uchwały zarządu.
9. Zatwierdzenie zmian w załącznikach polityki wymaga jedynie akceptacji osoby wskazanej w załączniku „PB\_01 Lista kontaktowa ochrony danych osobowych”.
10. W sprawach nieuregulowanych w Polityce mają zastosowanie przepisy prawa, w szczególności RODO.

# Spis załączników

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **Tytuł dokumentu** | **Typ dokumentu** |
| PB\_01 | Lista kontaktowa ochrony danych osobowych | Wewnętrzny |
| PB\_02 | Wzory klauzul informacyjnych i zgód odbieranych od osób, których dane są przetwarzane | Wewnętrzny |
| PB\_03 | Wzór umowy powierzenia przetwarzania danych osobowych | Wewnętrzny |
| PB\_04 | Wykaz budynków, placówek, w których przetwarzane są dane osobowe | Wewnętrzny poufny |
| PB\_05 | Wzór rejestru czynności przetwarzania i Rejestru kategorii | Wewnętrzny  |
| PB\_06 | Wzór oświadczenia o zachowaniu poufności i zapoznaniu się z przepisami | Wewnętrzny |
| PB\_07 | Wzór upoważnienia do przetwarzania danych osobowych | Wewnętrzny |
| PB\_08 | Wzór odwołania upoważnienia do przetwarzania danych osobowych | Wewnętrzny |
| PB\_09 | Wzór ewidencji osób upoważnionych do przetwarzania danych osobowych  | Wewnętrzny poufny |
| PB\_10 | Okresy retencji danych | Wewnętrzny |
| PB\_11 | Wzór rejestru realizacji praw podmiotów danych | Wewnętrzny poufny |
| PB\_12 | Procedura nadawania upoważnień do przetwarzania danych osobowych | Wewnętrzny |
| RIT | Regulamin korzystania z zasobów teleinformatycznych | Wewnętrzny |
| PGK | Procedura gospodarowania kluczami | Wewnętrzny |
| IPPN | Instrukcja postępowania w przypadku naruszenia ochrony danych osobowych i zaistnienia zagrożeń dla ochrony danych | Wewnętrzny |
| PCB | Polityka czystego biurka, wydruku i ekranu | Wewnętrzny |
| POS | Procedura oceny skutków dla ochrony danych osobowych | Wewnętrzny |
| POS\_01 | Wzór oceny skutków dla ochrony danych osobowych | Wewnętrzny |
| POS\_02 | Wykaz rodzajów operacji wymagających oceny skutków dla ochrony danych osobowych | Wewnętrzny |

# Dokumenty powiązane

|  |  |  |
| --- | --- | --- |
| **Identyfikator** | **Tytuł dokumentu** | **Typ dokumentu** |
| AR | Ocena ryzyka ochrony danych osobowych | Wewnętrzny |

# Historia wersji dokumentu

|  |  |  |
| --- | --- | --- |
| **Wersja** | **Data** | **Opis zmian** |
| 1 |  | Pierwsza wersja |