|  |
| --- |
| **POLITYKA BEZPIECZEŃSTWA** **DANYCH OSOBOWYCH w BANKU SPÓŁDZIELCZYM** |

Spis treści

[I. WPROWADZENIE 2](#_Toc516600081)

[II. CELE POLITYKI 2](#_Toc516600082)

[III. DEFINICJE 3](#_Toc516600083)

[IV. ZADANIA I ODPOWIEDZIALNOŚĆ 5](#_Toc516600084)

[V. PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH 7](#_Toc516600085)

[1. *Podstawy prawne przetwarzania danych* 8](#_Toc516600086)

[2. Warunki wyrażenia zgody 8](#_Toc516600087)

[3. Przetwarzanie szczególnych kategorii danych osobowych 9](#_Toc516600088)

[VI. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ 9](#_Toc516600089)

[1. Obowiązek informacyjny 10](#_Toc516600090)

[2. Prawo dostępu do danych 11](#_Toc516600091)

[3. Prawo do sprostowania danych 12](#_Toc516600092)

[4. Prawo do usunięcia danych 12](#_Toc516600093)

[5. Prawo do ograniczenia przetwarzania danych 12](#_Toc516600094)

[6. Prawo do przenoszenia danych 13](#_Toc516600095)

[7. Prawo sprzeciwu 13](#_Toc516600096)

[VII. ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU 14](#_Toc516600097)

[VIII. POWIERZENIE PRZETWARZANIA DANYCH 15](#_Toc516600098)

[IX. REJESTROWANIE CZYNNOŚCI PRZETWARZANIA 16](#_Toc516600099)

[X. ZASADY ANALIZY RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH 17](#_Toc516600100)

[XI. POSTANOWIENIA KOŃCOWE 18](#_Toc516600101)

[XII. WYKAZ ZAŁĄCZNIKÓW 18](#_Toc516600102)

# WPROWADZENIE

Polityka bezpieczeństwa danych osobowych w Banku Spółdzielczym w\_\_\_\_\_\_\_\_\_\_, zwana dalej „Polityką”, określa podstawowe zasady i metody zapewniania bezpieczeństwa danych osobowych stosowane przez Bank Spółdzielczy w\_\_\_\_\_\_\_\_\_\_, zwanym dalej „Bankiem”.

Niniejszy dokument jest zgodny z obowiązującymi przepisami prawa, a w szczególności z:

1. Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 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 nazywanego ogólnym Rozporządzeniem o ochronie danych osobowych (RODO);
2. Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. 2018 r., poz. 1000);
3. Ustawą z dnia … przepisy wprowadzające ustawę o ochronie danych osobowych;
4. Ustawą z dnia 29 sierpnia 1997 r. Prawo bankowe (Dz. U. z 2012 r. poz. 1376, z późn. zm.);
5. Ustawą z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. nr 21, poz. 94 z 1998 r. z późn. zm.);
6. Kodeksem dobrych praktyk w zakresie przetwarzania danych osobowych przez banki
i rejestry kredytowe;
7. Rekomendacją D Komisji Nadzoru Finansowego dotyczącą zarządzania obszarem technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, Warszawa 2013;
8. Innymi przepisami branżowymi, krajowymi, jak i Unii Europejskiej.

Polityka dotyczy wszystkich pracowników Banku oraz wszystkich osób mających dostęp do danych osobowych, przy pomocy których Bank wykonuje swoje czynności. Każdy Pracownik zobowiązany jest do zapoznania się z Polityką przed dopuszczeniem do pracy w Banku.

Zabezpieczenie danych osobowych to proces wymagający ciągłego doskonalenia
i modyfikacji, dlatego stosowane w Banku rozwiązania techniczne i organizacyjne w tym zakresie podlegają okresowemu monitoringowi i ocenie pod kątem ich skuteczności i zgodności
z przepisami prawa.

Niniejsza Polityka podlega regularnym przeglądom i aktualizacji, zgodnie z zasadami przeglądu zarządczego uregulowań wewnętrznych, co najmniej raz do roku lub w trakcie roku,
w przypadku wystąpienia znaczących zmian. Przeglądy powinny obejmować weryfikację zasad
i ewentualne dostosowanie Polityki do zmieniających się warunków środowiska organizacyjnego i technicznego Banku, a także w zakresie zachowania zgodności z przepisami prawa i normami nadzorczymi.

Nadzór nad dokumentacją z zakresu ochrony danych osobowych sprawuje wyznaczony w Banku Inspektor ochrony danych.

# CELE POLITYKI

Niniejsza Polityka została opracowana w celu stworzenia i utrzymania wysokiego poziomu bezpieczeństwa danych osobowych przetwarzanych w Banku, w tym:

1. zapewnienia spełnienia wymagań prawnych;
2. zapewnienia poufności, integralności przetwarzanych danych osobowych oraz zapewnienia ciągłości dostępu do tych danych;
3. zarządzania incydentami naruszenia bezpieczeństwa danych;
4. zaangażowania pracowników Banku w ochronę danych osobowych;

Bank zapewnia rozliczalność powyższych działań poprzez zapewnienie odpowiednich procedur wewnętrznych, w tym w szczególności regulacji z zakresu bezpieczeństwa informacji, bezpieczeństwa środowiska teleinformatycznego i zarządzania ryzykiem.

W Banku funkcjonuje system zarzadzania bezpieczeństwem informacji uwzględniający:

* Organizacyjne założenia ochrony informacji;
* Wymagania wobec systemu przetwarzania informacji;

(zawierające kryteria dopuszczenia systemu do użytkowania)

* Zarządzanie jakością danych;
* Bezpieczeństwo środowiska teleinformatycznego;
* Analizę ryzyka w zakresie bezpieczeństwa środowiska teleinformatycznego;
* Techniczne i organizacyjne środki ochrony przetwarzanych informacji;
* Postępowanie w przypadku wystąpienia incydentów naruszenia bezpieczeństwa informacji;
* Nadzór i kontrolę.

# DEFINICJE

**Administrator Danych (ADO):** Bank Spółdzielczy w\_\_\_\_\_\_\_\_\_\_\_\_\_\_ w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r.;

**Inspektor Ochrony Danych (IOD)**: osoba wyznaczona przez Zarząd, realizująca zadania
w zakresie ochrony danych osobowych, o których mowa w art. 39 Rozporządzenia;

**ASI:** Administrator Systemów Informatycznych;

**UODO:** Ustawa o ochronie danych osobowych z dnia 10 maja 2018 r.

**RODO:** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE;

**Organ nadzorczy:** Prezes Urzędu Ochrony Danych Osobowych, odpowiedzialny za monitorowanie stosowania RODO;

**Zarząd:** Zarząd Banku Spółdzielczego w\_\_\_\_\_\_\_\_\_\_\_;

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

**Szczególne kategorie danych osobowych:** dane, o których mowa w art. 9 ust. 1 Rozporządzenia, ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz dane genetyczne, dane biometryczne w celu jednoznacznego zidentyfikowania osoby fizycznej lub dane dotyczące zdrowia, seksualności lub orientacji seksualnej tej osoby;

**Zbiór danych:** uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie;

**Przetwarzanie:** operacja lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taka 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;

**Ograniczenie przetwarzania:** oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania;

**Podmiot przetwarzający:** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu Administratora;

**Powierzenie przetwarzania danych:** zlecenie przetwarzania danych osobowych podmiotowi przetwarzającemu (procesorowi) w drodze umowy zawartej na piśmie;

**Odbiorca:** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe;

**Profilowanie:** dowolna forma zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się;

**Pseudonimizacja:** przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej;

**Zgoda osoby, której dane dotyczą:** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych;

**Naruszenie ochrony danych osobowych:** 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;

**Ryzyko:** pojęcie odnoszące się do oceny prawdopodobieństwa wystąpienia i wagi skutków wystąpienia zagrożenia naruszenia praw i wolności osób, których dane dotyczą,

**Bezpieczeństwo Informacji (BI):** zachowanie poufności, integralności i dostępności informacji; w ramach bezpieczeństwa informacji mogą być uwzględniane również inne właściwości, takie jak autentyczność, rozliczalność, niezaprzeczalność i niezawodność (na podstawie ISO/IEC 27000:2014);

**System informatyczny:** zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

**Infrastruktura teleinformatyczna:** zespół urządzeń i łączy transmisyjnych obejmujący
w szczególności platformy sprzętowe (w tym: serwery, macierze, stacje robocze), sieć teleinformatyczną (w tym: routery, przełączniki, zapory sieciowe oraz inne urządzenia sieciowe), oprogramowanie systemowe (w tym systemy operacyjne i systemy zarządzania bazami danych) oraz inne elementy umożliwiające bezawaryjną i bezpieczną pracę ww. zasobów (w tym zasilacze UPS, generatory prądotwórcze, urządzenia klimatyzacyjne), także te wykorzystywane
w ośrodkach zapasowych banku;

**Integralność danych:** to właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

**Plan ciągłości działania:** udokumentowany zbiór procedur i informacji, które określają jak
w warunkach poważnego zakłócenia działalności biznesowej zapewnić warunki zastępcze dla tej działalności na akceptowalnym zdefiniowanym poziomie oraz jak zorganizować tok przywracania sytuacji sprzed zakłócenia;

**Podatność:** wady lub luki struktury fizycznej, organizacji, procedur, personelu, zarządzania, administrowania, sprzętu lub oprogramowania, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika;

**Poufność danych:** to właściwość zapewniająca, że dane nie są udostępniane nieupoważnionym osobom lub podmiotom;

**Tajemnica bankowa:** wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której Bank tę czynność wykonuje;

**Właściciel procesu:** osoba zarządzająca przebiegiem procesu, delegująca uprawnienia
i obowiązki związane z jego utrzymaniem oraz odpowiedzialna za jego realizację, w tym za plan ciągłości działania tego procesu;

**Zagrożenie:** potencjalna przyczyna niepożądanego incydentu, który może spowodować szkodę dla systemu lub organizacji (na podstawie ISO/IEC 27000:2009).

# ZADANIA I ODPOWIEDZIALNOŚĆ

Podział zadań w zakresie zapewnienia bezpieczeństwa danych osobowych.

Bank określa standardy zapewniające bezpieczeństwo danych osobowych i wdraża odpowiednie środki techniczne i organizacyjne dostosowane do pojawiających się zagrożeń.

W imieniu Administratora danych osobowych nadzór nad przestrzeganiem zasad ochrony danych osobowych sprawuje Inspektor Ochrony Danych (IOD).

**Do podstawowych zadań IOD należy:**

1. Informowanie Zarządu oraz pracowników, którzy przetwarzają dane osobowe,
o obowiązkach spoczywających na nich na mocy RODO oraz innych przepisów prawa
o ochronie danych i doradzanie im w tej sprawie;
2. Nadzorowanie przestrzegania RODO i innych przepisów prawa o ochronie danych oraz wewnętrznych procedur Banku w zakresie ochrony danych osobowych;
3. Działania zwiększające świadomość pracowników dopuszczonych do przetwarzania danych, w tym szkolenia oraz przeprowadzanie kontroli;
4. Udzielanie na żądanie zaleceń co do oceny skutków dla ochrony danych oraz monitorowanie jej wykonania;
5. Współpraca z Organem nadzorczym;
6. Pełnienie funkcji punktu kontaktowego dla Organu nadzorczego oraz osób, których dane dotyczą;
7. Opracowanie i aktualizowanie dokumentacji opisującej sposób przetwarzania danych osobowych;
8. Monitorowanie skuteczności działania zabezpieczeń wdrożonych w celu ochrony danych osobowych;
9. Prowadzenie rejestru czynności przetwarzania i rejestru wszystkich kategorii czynności przetwarzania, których wzory stanowią Załączniki nr 1 i 2 do niniejszej Polityki;
10. Prowadzenie ewidencji osób upoważnionych do przetwarzania danych – w formie elektronicznej:
11. Nadzorowanie przetwarzania danych osobowych przez podmioty zewnętrzne, którym Bank powierzył przetwarzanie w jego imieniu;
12. Obsługa zdarzeń oraz incydentów związanych z naruszeniem bezpieczeństwa danych osobowych;
13. Prowadzenie postępowań wyjaśniających w przypadku naruszenia bezpieczeństwa danych osobowych.

**Kierownik jednostki/komórki organizacyjnej jest zobligowany do:**

1. Bieżącego nadzoru nad zbiorami danych osobowych, w tym w zakresie kontroli okresów przechowywania danych;
2. Zgłaszania IOD zmian w zakresie i sposobie przetwarzania danych osobowych;
3. Konsultacji z IOD w zakresie ustalenia podstawy prawnej przetwarzania danych osobowych w związku z realizacją zadań przypisanych do danej jednostki/komórki organizacyjnej;
4. Przeprowadzania wstępnej analizy ryzyka naruszenia praw lub wolności osób fizycznych;
5. Zapewnienie ochrony przetwarzanych danych osobowych przed dostępem osób nieuprawnionych zgodnie z obowiązującymi procedurami;
6. Konsultacji i zgłaszania do akceptacji IOD zmian wprowadzanych w regulacjach wewnętrznych/wnioskach/umowach w zakresie przetwarzania danych osobowych.

**Administrator systemu informatycznego jest zobligowany do:**

1. Uzyskania akceptacji IOD przed zakupem nowego systemu informatycznego lub wprowadzeniem zmian do aktualnie eksploatowanego zgodnie z procedurą zarządzania zmianą w systemach informatycznych;
2. Wdrożenia i nadzorowania w systemie informatycznym służącym do przetwarzania danych osobowych środków technicznych i organizacyjnych, wynikających z RODO
i zapewniających ochronę przetwarzanych danych odpowiednią do zagrożeń oraz kategorii danych objętych ochroną;
3. Monitorowanie pracy systemu;
4. Zarządzania prawami dostępu użytkowników, hasłami, funkcjami sieciowymi, na podstawie decyzji Zarządu/Kierownika komórki organizacyjnej/IOD;
5. Rejestrowanie użytkowników i nadawanie im identyfikatorów;
6. Usuwanie identyfikatorów użytkowników, którzy przestali pracować w systemie;
7. Prowadzenie dokumentacji dotyczącej systemu informatycznego;
8. Przechowywanie i udostępnianie użytkownikom aktualnej wersji dokumentacji eksploatacyjnej;

**Każdy pracownik przetwarzający dane osobowe jest zobligowany do:**

1. Znajomości i przestrzeganie postanowień niniejszej Polityki Bezpieczeństwa;
2. Zgłoszenia IOD każdego przypadku:
3. Naruszenia ochrony danych osobowych lub uzasadnionym podejrzeniu takiego naruszenia;
4. Otrzymania od Klienta wniosku o udzielenie informacji, żądania zaprzestania przetwarzania danych osobowych lub ograniczenia przetwarzania danych osobowych, sprzeciwu wobec przetwarzania danych osobowych, wniosku
o przeniesienie danych osobowych;
5. Uczestniczenia w cyklicznych szkoleniach dotyczących przetwarzania danych osobowych (nie rzadziej niż raz na dwa lata lub w przypadku istotnych zmian w tym zakresie);
6. Zachowania w tajemnicy, również po ustaniu zatrudnienia, wszelkich danych osobowych oraz sposobie ich zabezpieczenia;
7. Przetwarzania danych osobowych wyłącznie w zakresie ustalonym w nadanym upoważnieniu;
8. Ochrony haseł i przestrzeganie zasad dostępu;
9. Wykonywania wszelkich operacji w systemach informatycznych przy użyciu swoich identyfikatorów oraz haseł;
10. Zachowania szczególnej staranności w trakcie wykonywania operacji przetwarzania danych osobowych w celu ochrony interesów osób, których dane dotyczą.

# PODSTAWOWE ZASADY PRZETWARZANIA DANYCH OSOBOWYCH

Bank realizując postanowienia niniejszej Polityki podejmuje wszelkie niezbędne działania
w celu ochrony prywatności osób, których dane przetwarza w związku z wykonywaniem swoich zadań, w tym poprzez:

1. Przetwarzanie danych osobowych zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”);
2. Zbierane danych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach
i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”);
3. Przetwarzanie danych adekwatnych, stosownych oraz ograniczonych do celów przetwarzania („minimalizacja danych”);
4. Podejmowanie wszelkich rozsądnych działań, aby dane osobowe, które są nieprawidłowe
w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane („prawidłowość”);
5. Przechowywanie danych 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. Przetwarzanie danych w sposób zapewniający odpowiednie bezpieczeństwo, 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”).

**Do przetwarzania danych osobowych mogą być dopuszczone wyłącznie pracownicy posiadający upoważnienie nadane przez Administratora/IOD. Ewidencja pracowników upoważnionych do przetwarzania danych prowadzona jest przez IOD w postaci elektronicznej.**

## Podstawy prawne przetwarzania danych

Przetwarzanie danych w Banku jest dopuszczalne tylko wtedy, gdy spełniony zostanie, co najmniej jeden warunek:

1. Osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych;
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 Banku;
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;
6. Przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Bank, 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.

Za prawnie usprawiedliwiony cel uważa się w szczególności:

1) Marketing bezpośredni własnych produktów lub usług Banku,

2) Dochodzenie roszczeń z tytułu prowadzonej działalności przez Bank.

## Warunki wyrażenia zgody

Jeśli zgoda osoby ma stanowić wyłączną podstawę prawną przetwarzania danych w określonym celu, wyrażenie zgody przez osobę powinno nastąpić przed faktycznym rozpoczęciem przetwarzania danych w tym celu.

Zapytanie o zgodę musi być wyrażone w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem, a także stanowić odrębną deklarację.

Bank umożliwia osobie, która wyraziła zgodę, wycofanie tej zgody w dowolnym momencie oraz w sposób równie łatwy, jak jej wyrażenie. Nie oznacza to jednak, że wycofanie zgody musi nastąpić dokładnie w taki sam sposób jak jej wyrażenie.

## Przetwarzanie szczególnych kategorii danych osobowych

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.

Przetwarzanie danych, o których mowa powyżej, jest dopuszczalne, jeżeli spełniony jest 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 obowiązujące przepisy prawa przewidują, iż osoba, której dane dotyczą nie może uchylić zakazu, o którym mowa powyżej;
2. Przetwarzanie jest niezbędne do wypełnienia obowiązku i wykonywania szczegółowych prawa przez Administratora lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej, o ile jest to dozwolone obowiązującymi przepisami prawa;
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, do czasu ustanowienia opiekuna prawnego lub kuratora;
4. Przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń;
5. Przetwarzanie jest niezbędne do wykonania zadań Administratora odnoszących się do zatrudnienia pracowników i innych osób, a zakres przetwarzanych danych jest określony
w ustawie;
6. Przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
7. Przetwarzanie danych jest prowadzone przez Administratora w celu realizacji praw
i obowiązków wynikających orzeczenia wydanego w postępowaniu sądowym lub administracyjnym.

# PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ

Bank w celu realizacji obowiązków w zakresie przejrzystego informowania
i przejrzystej komunikacji z osobą, której dane dotyczą, wdraża odpowiednie procedury i wzorce dokumentów w zakresie:

1. realizacji obowiązku informacyjnego, o którym mowa w art. 13 i 14 RODO (informacje podawane w przypadku zbierania danych),
2. prowadzenia komunikacji w sprawie przetwarzania na mocy art. 15–22 RODO (informacje przekazywane w ramach realizacji praw przysługujących osobie, której dane dotyczą).

Informacji udziela się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym
i prostym językiem, na piśmie lub w inny sposób, w tym w stosownych przypadkach drogą elektroniczną.

Bank bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania – udziela osobie, której dane dotyczą, informacji o działaniach podjętych w związku
z żądaniem na podstawie art. 15–22 RODO. W razie potrzeby termin ten można przedłużyć
o kolejne dwa miesiące z uwagi na skomplikowany charakter żądania lub liczbę żądań.

W przypadku nie podjęcia działań w związku z żądaniem osoby, której dane dotyczą, Bank 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.

Informacje podawane na mocy art. 13 i 14 oraz komunikacja i działania podejmowane na mocy art. 15–22 są wolne od opłat, z zastrzeżeniem, że jeżeli żądania osoby, której dane dotyczą, są ewidentnie nieuzasadnione lub nadmierne, w szczególności ze względu na swój ustawiczny charakter, Bank może:

1. pobrać rozsądną opłatę, uwzględniając administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań;

albo

1. odmówić podjęcia działań w związku z żądaniem.

Decyzje dotyczące rozpatrzenia wniosków z żądaniami osób, których dane dotyczą podejmuje

Zarząd na podstawie opinii IOD.

## Obowiązek informacyjny

Bank dopełnia obowiązku informacyjnego w przypadku zbierania danych osobowych oraz
w przypadku zmiany celów przetwarzania danych osobowych.

W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, informacja jest przekazywana podczas pozyskiwania danych, natomiast w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą:

* w rozsądnym terminie, nie później jednak niż w ciągu miesiąca od pozyskania danych,
* najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą,
* najpóźniej przy pierwszym ujawnieniu danych, jeżeli Bank planuje ujawnić dane osobowe innemu odbiorcy danych.

Odstępstwa od wypełnienia obowiązku informacyjnego w stosunku do osoby, której dane dotyczą, są możliwe, jeśli m.in.:

1. osoba posiada stosowne informacje,
2. udzielenie informacji osobie, której dane zostały zebrane nie bezpośrednio od niej, jest niemożliwe lub wymagałoby niewspółmiernego dużego wysiłku albo wymagałoby pozyskiwania informacji dodatkowych z innych źródeł zewnętrznych,
3. pozyskanie lub ujawnienie danych osoby, której dane są zebrane nie bezpośrednio od niej, uregulowane jest wyraźnie w przepisach prawa przewidujących odpowiednie środki chroniące prawnie uzasadnione interesy osoby, której dane dotyczą,
4. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy bankowej oraz innych tajemnic ustawowo chronionych.

## Prawo dostępu do danych

Osoba, której dane dotyczą, jest uprawniona do uzyskania potwierdzenia, czy Bank przetwarza jej dane osobowe, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz informacji o:

a) celach przetwarzania,

b) kategoriach odnośnych danych osobowych,

c) odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione,

d) planowanym okresie przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriach ustalania tego okresu,

e) prawie do żądania od Banku sprostowania, usunięcia lub ograniczenia przetwarzania danych oraz do wniesienia sprzeciwu wobec takiego przetwarzania,

f) prawie wniesienia skargi do organu nadzorczego,

g) jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich dostępnych informacjach o ich źródle,

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

Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana przez Bank o odpowiednich zabezpieczeniach związanych z przekazaniem, o których mowa w art. 46 RODO.

Bank dostarcza osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie Bank może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych.

## Prawo do sprostowania danych

Osoba, której dane dotyczą, ma prawo żądania od Banku niezwłocznego sprostowania dotyczących jej danych osobowych, które są nieprawidłowe oraz uzupełnienia niekompletnych danych osobowych.

## Prawo do usunięcia danych

Osoba, której dane dotyczą, może żądać w formie wyraźnego oświadczenia niezwłocznego usunięcia danych osobowych jej dotyczących (prawo do bycia zapomnianym), wskazując zakres żądania.

Bank ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli:

1. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane lub
2. osoba, której dane dotyczą, cofnęła zgodę, na której opiera się przetwarzanie zgodnie
z art. 6 ust. 1 lit. a) 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 (prawo do sprzeciwu) wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą,
4. wnosi sprzeciw na mocy art. 21 ust. 2 wobec przetwarzania (prawo do sprzeciwu
w związku z marketingiem bezpośrednim),
5. dane osobowe były przetwarzane niezgodnie z prawem,
6. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Unii lub prawie państwa członkowskiego, któremu podlega Administrator,
7. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego.

Obowiązek realizacji prawa do bycia zapomnianym nie obowiązuje w sytuacji, gdy dalsze przetwarzanie jest niezbędne w szczególności do:

1. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy przepisów prawa, którym podlega Administrator;
2. do ustalenia, dochodzenia lub obrony roszczeń.

Bank ustali okresy przechowywania danych, uwzględniając okres nie dłuższy, niż jest to niezbędne dla celów, w których dane są przetwarzane oraz okres dla przechowywania danych
w celach archiwalnych lub statystycznych.

Bank może przechowywać dane po osiągnięciu pierwotnych celów przetwarzania, pod warunkiem, że ich dalsze przechowywanie znajduje podstawę prawną

## Prawo do ograniczenia przetwarzania danych

Osoba, której dane dotyczą, ma prawo żądania od Banku ograniczenia przetwarzania
w przypadkach:

1. kwestionowania prawidłowości danych osobowych – na okres pozwalający sprawdzić prawidłowość tych danych,
2. przetwarzania niezgodnego z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania,
3. Bank 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.

Jeżeli przetwarzanie zostało ograniczone, takie dane osobowe można przetwarzać, z wyjątkiem przechowywania, wyłącznie za zgodą osoby, której dane dotyczą, lub w celu ustalenia, dochodzenia lub obrony roszczeń, lub w celu ochrony praw innej osoby fizycznej lub prawnej, lub z uwagi na ważne względy interesu publicznego Unii lub państwa członkowskiego.

Bank informuje o ograniczeniu przetwarzania danych osobowych, każdego odbiorcę, któremu ujawniono dane osobowe, chyba że okaże się to niemożliwe lub będzie wymagać niewspółmiernie dużego wysiłku. Bank informuje osobę, której dane dotyczą, o tych odbiorcach, jeżeli osoba, której dane dotyczą, tego zażąda.

## Prawo do przenoszenia danych

Osoba, której dane 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 Banku, jeżeli:

1. przetwarzanie odbywa się na podstawie zgody w myśl art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO lub na podstawie umowy w myśl art. 6 ust. 1 lit. b) RODO (zgoda osoby) oraz
2. przetwarzanie odbywa się w sposób zautomatyzowany.

Wykonując prawo do przenoszenia danych osoba, której dane dotyczą, ma prawo żądania, by dane osobowe zostały przesłane przez administratora bezpośrednio innemu administratorowi, o ile jest to technicznie możliwe.

Prawo do przenoszenia danych nie może niekorzystnie wpływać na prawa i wolności innych.

## Prawo sprzeciwu

Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania jej danych osobowych, wskazując jednocześnie, wobec jakiego konkretnego celu przetwarzania składa sprzeciw i wykazać, na czym polega szczególny charakter jej sytuacji.

Bank ma prawo odmowy uwzględnienia sprzeciwu po dokonaniu analizy, czy szczególna sytuacja osoby, której dane dotyczą, ma charakter nadrzędny wobec prawnie uzasadnionych podstaw do przetwarzania. Jednocześnie Bank wyjaśni przyczyny, dla których uważa, że interesy, prawa
i wolności tej osoby, nie mają charakteru nadrzędnego.

Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, Bank zaprzestaje przetwarzania danych do takich celów.

# ZGŁASZANIE NARUSZENIA OCHRONY DANYCH OSOBOWYCH ORGANOWI NADZORCZEMU

Bank definiuje katalog podatności i incydentów zagrażających bezpieczeństwu danych osobowych oraz opisuje sposób reagowania na nie. Sposób postępowania z incydentami bezpieczeństwa informacji, w tym danych osobowych opisuje oddzielna Instrukcja……

Za naruszenie ochrony danych podlegające obowiązkowi zgłoszenia Organowi nadzorczemu uznać należy każdą sytuację wywołującą prawdopodobieństwo naruszenia praw lub wolności osób fizycznych. W szczególności do naruszenia mogą prowadzić następujące sytuacje:

1. Utrata poufności danych osobowych w wyniku:
2. wycieku danych z powodu błędnego działania systemu informatycznego, zdarzeń losowych lub środowiskowych,
3. niezasadnego ujawnienia danych,
4. błędu ludzkiego,
5. niepożądanych działań osób, w tym osób trzecich (kradzież, zniszczenie, uniemożliwienie dostępu, modyfikacja, ujawnienie danych).
6. Brak dostępu do danych osobowych,
7. Naruszenia integralności danych osobowych.

W przypadku naruszenia ochrony danych osobowych, Bank bez zbędnej zwłoki, nie później niż
w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je organowi nadzorczemu właściwemu zgodnie z art. 55 RODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

Zgłoszenia można dokonać online poprzez udostępniony przez UODO formularz zgłoszenia, dostępny pod adresem: <https://ewnioski.biznes.gov.pl>

Zgłoszenie musi zawierać co najmniej:

1. opis charakteru naruszenia ochrony danych osobowych, w tym wskazanie kategorii
i przybliżonej liczby osób, których dane dotyczą, oraz kategorii i przybliżonej liczby wpisów danych osobowych, których dotyczy naruszenie,
2. imię i nazwisko oraz dane kontaktowe inspektora ochrony danych,
3. opis możliwych konsekwencji naruszenia ochrony danych osobowych,
4. opis środków zastosowanych lub proponowanych przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

Bank dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. W Banku prowadzony jest rejestr incydentów.

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 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 zastosowany zostaje podobny środek, za pomocą którego osoby, których dane dotyczą, zostają poinformowane w równie skuteczny sposób.

# POWIERZENIE PRZETWARZANIA DANYCH

Powierzenie przetwarzania danych osobowych innemu podmiotowi następuje na podstawie umowy zawartej na piśmie. Umożliwienie dostępu do tych danych bez uprzedniego zawarcia umowy nie jest możliwe.

Bank może powierzyć przetwarzanie danych osobowych wyłącznie w zakresie przewidzianym w umowie oraz o ile podmiot przetwarzający zapewnia wystarczające gwarancje – w szczególności jeżeli chodzi o wiedzę fachową, wiarygodność i zasoby – wdrożenia środków technicznych i organizacyjnych odpowiadających wymogom RODO.

Umowa o powierzeniu przetwarzania danych osobowych oraz zachowania tajemnicy bankowej określa w szczególności:

1. cel przetwarzania danych osobowych,
2. zakres przetwarzania danych osobowych (rodzaj danych osobowych),
3. kategorie osób, których dane dotyczą,
4. zasady współpracy Administratora z Podmiotem przetwarzającym,
5. zasady kontroli przeprowadzanych przez uprawnionych przedstawicieli Banku w zakresie sposobu przetwarzania danych i zastosowanych metod zabezpieczających,
6. zakres odpowiedzialności Podmiotu przetwarzającego, któremu powierzono przetwarzanie danych osobowych,
7. postanowienia o przysługującym Bankowi prawie kontroli sposobu przetwarzania danych osobowych i ich zabezpieczenia,
8. postanowienia o możliwości żądania natychmiastowego ograniczenia przetwarzania powierzonych danych osobowych w razie stwierdzenia ich niedostatecznej ochrony,
9. postanowienia o obowiązku powiadomienia Administratora w formie pisemnej
o fakcie usunięcia usterek przez Podmiot przetwarzający, któremu powierzono przetwarzanie danych osobowych,
10. postanowienia o zachowaniu tajemnicy bankowej,
11. postanowienia o zgłaszaniu Administratorowi naruszenia powierzonych danych osobowych.

Wzór „Umowy powierzenia przetwarzania danych osobowych” stanowi załącznik nr 3 do niniejszej Polityki. W przypadku umowy, sporządzonej na innym wzorze, wymagana jest pozytywna opinia IOD.

# REJESTROWANIE CZYNNOŚCI PRZETWARZANIA

W Banku prowadzone są:

* Rejestr czynności przetwarzania, za które Bank odpowiada jako Administrator danych;
* Rejestr wszystkich kategorii czynności przetwarzania danych osobowych, w których Bank jest podmiotem przetwarzającym, tj. wykonuje czynności w imieniu zlecających administratorów danych.

Za prowadzenie ww. rejestrów w postaci elektronicznej odpowiedzialny jest IOD. Wzory rejestrów stanowią odpowiednio załączniki nr 1 i 2 do niniejszej Polityki.

W rejestrze czynności przetwarzania znajdują się następujące informacje:

1. Oznaczenie Administratora, adres jego siedziby, dane kontaktowe oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej;
2. Cel przetwarzania danych osobowych;
3. Opis kategorii osób, których dane dotyczą oraz kategorii danych osobowych;
4. Planowane terminy usunięcia poszczególnych kategorii danych;
5. Kategorie odbiorców, którym dane mogą być przekazywane;
6. Informacja dotyczącą ewentualnego przekazywania danych do państwa trzeciego;
7. Opis technicznych i organizacyjnych środków bezpieczeństwa.

W rejestrze wszystkich kategorii czynności przetwarzania znajdują się następujące informacje:

* + - 1. Oznaczenie podmiotu przetwarzającego, adres jego siedziby, dane kontaktowe oraz numer identyfikacyjny rejestru podmiotów gospodarki narodowej;
			2. Kategorie przetwarzań dokonywanych w imieniu Administratora;
			3. Kategorie odbiorców, którym dane mogą być przekazywane;
			4. Informacja dotyczącą ewentualnego przekazywania danych do państwa trzeciego;
			5. Opis technicznych i organizacyjnych środków bezpieczeństwa.

Za bieżący nadzór i aktualizacje nad prowadzonymi rejestrami odpowiada IDO we współpracy
z poszczególnymi Kierownikami jednostek/komórek organizacyjnych Banku.

Prowadzenie rejestrów podlega kwartalnym przeglądom pod kątem ich aktualności i zgodności
z RODO, wytycznymi Organu nadzorczego oraz kodeksem dobrych praktyk.

# ZASADY ANALIZY RYZYKA I OCENA SKUTKÓW DLA OCHRONY DANYCH

W Banku przeprowadza się analizę ryzyka, a w przypadku możliwości wystąpienia wysokiego ryzyka naruszenia praw i wolności osób fizycznych także ocenę skutków planowanych operacji przetwarzania dla ochrony danych osobowych.

W ramach analizy ryzyka przeprowadza się następujące czynności:

1. analizę charakteru, zakresu, kontekstu i celów przetwarzania danych dla czynności przetwarzania wskazanych w „Rejestrze czynności przetwarzania” lub „Rejestrze kategorii czynności przetwarzania”;
2. identyfikację i analizę możliwych zagrożeń;
3. analizę podatności i ustalenie poziomu ryzyka naruszenia praw i wolności osób, których dane dotyczą w razie wystąpienia incydentów naruszeń ochrony danych;
4. identyfikację środków jakie należy wdrożyć w celu ograniczania ryzyka i mających zapewnić ochronę danych osobowych.

Wzorcowy arkusz analizy ryzyka stanowi załącznik nr 4 do niniejszej Polityki.

Na tej podstawie, odpowiednio do prawdopodobieństwa wystąpienia i wagi zagrożenia, Bank wdraża zabezpieczenia techniczne i organizacyjne, zapewniając ochronę przetwarzanych danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem dostępem do danych, przypadkową utratą, ujawnieniem, modyfikacją lub zniszczeniem danych osobowych. Wykaz stosowanych zabezpieczeń znajduje się w załączniku nr 5 do niniejszej Polityki. Wykaz jest aktualizowany po każdej analizie ryzyka.

W Banku wykorzystuje się takie rozwiązania techniczne i organizacyjne, które zapewniają realizację zasady ochrony danych w fazie projektowania oraz zasady domyślnej ochrony danych.

W przypadku konieczności przeprowadzenia oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, tj. w przypadkach, gdy 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, wymagane i dokumentowane są następujące czynności:

a) systematyczny opis planowanych operacji przetwarzania i celów przetwarzania- zawarty
w rejestrze czynności przetwarzania stanowiącym załącznik nr 1 do niniejszej Polityki,

b) ocena, czy operacje przetwarzania są niezbędne oraz proporcjonalne w stosunku do celów, zgodnie z prowadzonym rejestrem czynności przetwarzania,

c) ocena ryzyka przeprowadzona zgodnie z obowiązującą w Banku procedurą analizy ryzyka,

d) określenie środków planowanych w celu zaradzenia ryzyku, w tym zabezpieczenia oraz środki i mechanizmy bezpieczeństwa mające zapewnić ochronę danych osobowych, zgodnie z załącznikiem nr 5 do niniejszej Polityki.

Za ocenę ryzyka i informowanie o tym Zarządu odpowiedzialny jest IOD.

Jeżeli ocena skutków dla ochrony danych wskaże, że przetwarzanie powodowałoby wysokie ryzyko, gdyby Bank nie zastosował środków w celu zminimalizowania tego ryzyka, to przed rozpoczęciem przetwarzania Bank konsultuje się z organem nadzorczym, na zasadach określonych w art. 36 RODO. Decyzję o podjęciu konsultacji podejmuje Zarząd.

# POSTANOWIENIA KOŃCOWE

Pracownicy Banku posiadający dostęp do informacji objętych ochroną danych osobowych oraz tajemnicą bankową zobowiązani są do ścisłego przestrzegania przepisów prawa oraz przepisów wewnętrznych Banku.

Osoby naruszające postanowienia niniejszej Polityki ponoszą odpowiedzialność dyscyplinarną lub karną określoną w obowiązujących przepisach prawa.

Wszelkie działania podejmowane przez pracownika mające na celu nieprzestrzeganie postanowień niniejszej Polityki traktowane będą przez Bank jako rażące naruszenie podstawowych obowiązków pracowniczych.

# WYKAZ ZAŁĄCZNIKÓW

**Załącznik 1**: Rejestr czynności przetwarzania
**Załącznik 2**: Rejestr kategorii czynności przetwarzania
**Załącznik 3**: Wzór umowy PPDO
**Załącznik 4**: Arkusz analizy ryzyka
**Załącznik 5**: Wykaz zabezpieczeń

W celu uzyskania pełnej informacji w omawianych zakresach zapraszamy do kontaktu:

**Ewa Niesiołowska**
Audytor Wiodący SZBI, Członek IIA Polska
+48 531 364 287 ewa.niesiolowska@servus-comp.pl

**Anna Stręk**
Audytor Wiodący SZBI, Członek IIA Polska
+48 781 555 025 anna.strek@servus-comp.pl

**Andrzej Popiołek**Audytor Wiodący SZBI, Członek IIA Polska +48 602 220 749 andrzej.popiolek@servus-comp.pl

**Anna Kramarczyk**Kierownik ds. projektów IT+48 794 671 787anna.kramarczyk@servus-comp.pl

**Servus Comp Sp. z o.o. Sp.k.**ul. Mazowiecka 25/502, 30-019 Kraków Sąd Rejonowy dla Krakowa – Śródmieście, XI Wydział Gospodarczy Krajowego Rejestru Sądowego NIP: 6772394344 | Regon: 362815411 | KRS: 0000582481 <https://zadbajobezpieczenstwo.pl>
<https://premiumbank.zadbajobezpieczenstwo.pl>

**Nota prawna:**

1. Zaprezentowany materiał jest autorskim opracowaniem i jest objęty prawem autorskim.
2. Niniejszy materiał, ani żaden jego fragment nie może być reprodukowany, przetwarzany i rozpowszechniany w jakikolwiek sposób za pomocą urządzeń elektronicznych, mechanicznych, kopiujących, nagrywających i in. do celów innych niż realizacja przedmiotowej umowy u Klienta.