Polityka

bezpieczeństwa danych osobowych w Banku Spółdzielczym w Szczytnie

Szczytno, 2023

SPIS TREŚCI

Załączniki

Rozdział 1. **Podstawy prawne**

§ 1.

1. Polityka bezpieczeństwa danych osobowych w Banku Spółdzielczym w Szczytnie., zwana dalej Polityką, została opracowana na podstawie:
   1) ustawy z dnia 29 sierpnia 1997 r. Prawo bankowe (t. j. Dz. U. z 2016 r., poz. 1988, z późn. zm.);
   2) 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 („Rozporządzenie”);
   3) Ustawy z dnia 10 maja 2018 roku o ochronie danych osobowych;
   4) Uchwały Nr 7/2013 r. Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji D dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach (Dz. Urz. KNF z 2013 r. poz. 5),
   5) Uchwały Nr 8/2013 r. Komisji Nadzoru Finansowego z dnia 8 stycznia 2013 r. w sprawie wydania Rekomendacji M dotyczącej zarządzania ryzykiem operacyjnym w bankach (Dz. Urz. KNF z 2013 r. poz. 6).

Rozdział 2. **Cel i zakres regulacji**

§ 2.

1. Zarząd Banku, świadomy odpowiedzialności za bezpieczeństwo przetwarzanych w Banku danych osobowych, wprowadza Politykę bezpieczeństwa danych osobowych w Banku Spółdzielczym w Szczytnie.
2. Celem Polityki jest stworzenie podstaw organizacyjno-technicznych do wdrożenia systemu ochrony danych osobowych w Banku zgodnego z wymogami obowiązujących aktów prawnych w zakresie ochrony danych osobowych.
3. Bank w szczególności zapewnia:
   1) środki techniczne i organizacyjne niezbędne dla zapewnienia bezpiecznego przetwarzania danych w pomieszczeniach do tego przeznaczonych,
   2) systemy i sprzęt informatyczny umożliwiający bezpieczne przetwarzanie danych,
   3) że każda osoba działająca z upoważnienia administratora danych osobowych lub podmiotu przetwarzającego i mająca dostęp do danych osobowych przetwarzają je wyłącznie na polecenie administratora danych osobowych,
   4) uwzględnianie ochrony danych w fazie projektowania oraz uwzględnianie mechanizmów domyślnej ochrony zgodnie z art. 25 RODO;
   5) korzystanie 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 zgodnie z art. 28 RODO,
   6) prowadzenie rejestru czynności przetwarzania danych oraz rejestru wszystkich kategorii czynności przetwarzania dokonywanych w imieniu administratora zgodnie z art. 30 RODO,

7) należyte i terminowe udzielanie informacji na wniosek osób, których dane osobowe są przetwarzane i które zwróciły się z wnioskiem w związku z realizacja jej praw, o których mowa w art. 12-23 RODO,
8) bezpieczeństwo przetwarzania danych, o którym mowa w art. 32 RODO w tym kontrolę nad tym, jakie dane, kiedy i przez kogo zostały do zasobów Administratora wprowadzone, usunięte oraz komu i przez kogo przekazane;
9) zgłaszanie naruszenia ochrony danych osobowych organowi nadzorczemu zgodnie z art. 34 RODO,
10) zawiadamianie osoby, której dane dotyczą, o naruszeniu ochrony danych osobowych zgodnie z art. 34 RODO,
11) dokonywanie oceny skutków dla ochrony danych (DPIA) zgodnie z art. 35 RODO,
12) wyznaczenie Inspektora Ochrony Danych zgodnie z art. 37 RODO.

§ 3.

1. Zakres przedmiotowy stosowania Polityki obejmuje wszystkie zbiory danych osobowych przetwarzane w Banku, zarówno w formie tradycyjnej (kartoteki, skorowidze, księgi, wykazy i inne zbiory ewidencyjne), jak i w systemach informatycznych.
2. Zakres podmiotowy Polityki obejmuje wszystkich pracowników Banku oraz osoby przy pomocy, których Bank wykonuje swoje czynności, mające dostęp do danych osobowych.

§ 4.

Polityka stanowi uszczegółowienie Polityki Bezpieczeństwa Informacji w Banku Spółdzielczym w Szczytnie pod kątem ochrony danych osobowych.

Rozdział 3. **Definicje**

§ 5.

3. Przez użyte w niniejszej Polityce określenia należy rozumieć:
   1) **Administrator Danych Osobowych (ADO)** – Bank Spółdzielczy w Szczytnie decydujący o celach i środkach przetwarzania danych osobowych, mogący jednocześnie pełnić funkcję Podmiotu przetwarzającego dla innego Administratora Danych
   2) **Bank** – Bank Spółdzielczy w Szczytnie;
   3) **SOA** – Sekcja Organizacyjno-Administracyjna w Banku;
   4) **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;
   5) **ZIT** – Zespół Obsługi Informatycznej i Telekomunikacji (Zespół IT w Banku);
   6) **Radca Prawny** – Radca Prawny Banku;

7) **Inspektor Ochrony Danych Osobowych (IODO)** – osoba wyznaczona przez Zarząd Banku realizująca zadania w zakresie ochrony danych osobowych, zgodnie z art. 39 Rozporządzenia;
8) **naruszenie ochrony danych osobowych** – naruszenie bezpieczeństwa prowadzące do przypadkowego lub niezgodnego z prawem zniszczenia, utracenia, zmodyfikowania, nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych
9) **nośnik informacji** – wszelkiego rodzaju nośniki danych, używane w procesie przetwarzania, w szczególności dyski twarde, płyty CD/DVD, taśmy do streamerów, pamięci przenośne, dyski magnetooptyczne, dokumenty w formie papierowej;
10) **obszar przetwarzania danych osobowych** – budynki i pomieszczenia wszystkich placówek Banku oraz budynki i pomieszczenia Podmiotów przetwarzających;
11) **odbiorca danych osobowych –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią;]
12) **ograniczenie przetwarzania –** oznaczenie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania
13) **Podmiot przetwarzający –** osoba fizyczna lub prawna, organ publiczny, jednostka lub inny podmiot, który przetwarza dane osobowe w imieniu ADO;
14) **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;
15) **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;
16) **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;
17) **Rozporządzenie** – (w skrócie RODO) ogólne rozporządzenie o ochronie danych (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(Dz. U. UE L 119 z dnia 4 maja 2016 r.);
18) **system informatyczny** – zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

19) **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;
20) **UODO** – organ nadzorczy odpowiedzialny za monitorowanie stosowania Rozporządzenia - **Urząd Ochrony Danych Osobowych**;
21) **usuwanie danych osobowych** – niszczenie danych osobowych lub taka ich modyfikacja, która nie pozwoli na ustalenie tożsamości osoby, której dane dotyczą;
22) **Zastępca IODO** osoba wyznaczona przez Zarząd Banku, wykonująca zadania IODO podczas jego nieobecności;
23) **zbiór danych** – uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany, czy rozproszony funkcjonalnie lub geograficznie;
24) **zgoda –** dobrowolne, konkretne, świadome i jednoznaczne okazanie woli przez osobę, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwalające na przetwarzanie dotyczących jej danych osobowych.

Rozdział 4. **Zasady przetwarzania danych osobowych**

§ 6.

1. Bank, dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności zapewnia, aby dane osobowe na każdy etapie były przetwarzane zgodnie z wymaganiami określonymi w art. 5 RODO.
2. W Banku, w każdej realizowanej usłudze i procesie, dane osobowe są:
   1) przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą (zasada legalności);
   2) zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami (zasada ograniczonego celu);
   3) adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane (zasada minimalizacji danych);
   4) prawidłowe i w razie potrzeby uaktualniane (zasada prawidłowości);
   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 (zasada ograniczenia 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 i organizacyjnych ((zasada zachowania integralności danych oraz ich poufności).
3. Przetwarzanie danych osobowych (innych niż dane szczególnej kategorii) jest dopuszczalne tylko wtedy, gdy:
   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 danych;
4) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą lub innej osoby fizycznej;
5) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Administratora danych 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.

4. Za prawnie uzasadniony cel dla Administratora danych 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 oraz ustawy z dnia 16 lipca 2004 r. prawo telekomunikacyjne, które przewidują dalej idącą ochronę.
5. Dla czynności przetwarzania na podstawie prawnie uzasadnionego interesu Administratora, Bank przeprowadza test równowagi, zgodnie ze wzorem określonym w załączniku nr 8 do Polityki.
6. Przetwarzanie danych osobowych szczególnych kategorii jest dopuszczalne tylko zgodnie z art. 9 ust. 2 RODO, w tym w szczególności, gdy:
   1) osoba, której dane dotyczą, wyraziła wyraźną zgodę na przetwarzanie tych danych osobowych w jednym lub kilku konkretnych celach;
   2) przetwarzanie jest niezbędne do wypełnienia obowiązków i wykonywania szczególnych praw przez Administratora danych lub osobę, której dane dotyczą, w dziedzinie prawa pracy, zabezpieczenia społecznego i ochrony socjalnej,
      o ile jest to dozwolone przepisami prawa lub porozumieniem zbiorowym na mocy przepisów prawa, 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) przetwarzanie dotyczy danych osobowych w sposób oczywisty upublicznionych przez osobę, której dane dotyczą;
   5) przetwarzanie jest niezbędne do ustalenia, dochodzenia lub obrony roszczeń lub w ramach sprawowania wymiaru sprawiedliwości przez sądy;
   6) przetwarzanie jest niezbędne ze względów związanych z ważnym interesem publicznym, na podstawie przepisów prawa, 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;
   7) przetwarzanie jest niezbędne do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych, na podstawie przepisów prawa;

8) przepis prawa zawiera dyspozycję w zakresie przetwarzania danych genetycznych, danych biometrycznych lub danych dotyczących zdrowia.

7. Zgoda na przetwarzanie danych osobowych nie może być domniemana lub dorozumiana z oświadczenia woli o innej treści.
8. Zgoda na przetwarzanie danych osobowych może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.
9. Zgoda może mieć formę pisemnego (w tym elektronicznego) lub ustnego oświadczenia. Zgoda na przetwarzanie danych, z wyłączeniem danych osobowych szczególnej kategorii, może być wyrażona poprzez wyraźne działanie.
10. Administrator danych musi być w stanie wykazać, że osoba, której dane dotyczą, wyraziła zgodę na przetwarzanie swoich danych osobowych, termin w jakim została ona wyrażona oraz jaka była jej treść.
11. Jeżeli osoba, której dane dotyczą, wyraża zgodę w pisemnym oświadczeniu, które dotyczy także innych kwestii, zapytanie o zgodę musi zostać przedstawione w sposób pozwalający wyraźnie odróżnić je od pozostałych kwestii, w zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem.
12. Zgoda na przetwarzanie danych osobowych może zostać odwołana w każdym czasie. Wycofanie zgody musi być równie łatwe jak jej wyrażenie. Wycofanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem. Wycofanie zgody nie wymaga uzasadnienia.
13. ADO stosuje odpowiednie środki techniczne i organizacyjne – zarówno przy określaniu sposobów przetwarzania (w fazie projektowania, zgodnie z zasadą „privacy by design”), jak i w czasie samego przetwarzania (domyślna ochrona danych, zgodnie z zasadą „privacy by default”), aby zapewnić stopień bezpieczeństwa odpowiadający ryzyku naruszenia praw lub wolności osób fizycznych.

Rozdział 5. **Wyznaczenie Inspektora Ochrony Danych**

§ 7.

1. W imieniu ADO nadzór nad przestrzeganiem zasad ochrony danych osobowych w Banku sprawuje IODO, a w czasie jego nieobecności, Zastępca IODO. W Banku funkcję IODO pełni wyznaczony uchwałą Zarządu Banku pracownik bezpośrednio podlegający Prezesowi Zarządu Banku.
2. IODO 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.
3. IODO jest zobowiązany do zachowania tajemnicy uzyskanych informacji oraz poufności wykonywanych zadań.
4. ADO publikuje na stronie internetowej Banku dane kontaktowe IODO i zawiadamia o nich Urząd Ochrony Danych Osobowych.
5. ADO zapewnia by IODO był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych, w szczególności w proces opiniowania umów powierzenia przetwarzania danych osobowych, umów związanych z ochroną danych osobowych oraz opiniowania projektów informatycznych i zmian w projektach

informatycznych dotyczących systemów informatycznych, w których przetwarzane są dane osobowe.

6. Administrator może wyznaczyć Zastępcę IODO, którego dane kontaktowe publikuje na stronie internetowej Banku oraz zawiadamia Urząd Ochrony Danych Osobowych o jego wyznaczeniu.

§ 8.

1. IODO jest odpowiedzialny za:
   1) zapewnianie przestrzegania przepisów o ochronie danych osobowych, w szczególności Rozporządzenia poprzez cykliczne sprawdzanie zgodności przetwarzania danych osobowych z przepisami o ochronie danych osobowych;
   2) raz w roku opracowywanie raportu do Zarządu Banku „Raport na temat stanu zagrożeń i bezpieczeństwa w Banku”;
   3) prowadzenie nadzoru nad procesem opracowania i aktualizacji dokumentacji przetwarzania danych osobowych poprzez weryfikację:
      a. opracowania i kompletności dokumentacji przetwarzania danych,
      b. zgodności dokumentacji przetwarzania danych z obowiązującymi przepisami prawa,
      c. stanu faktycznego w zakresie przetwarzania danych osobowych,
      d. zgodności ze stanem faktycznym przewidzianych w dokumentacji przetwarzania danych osobowych środków technicznych i organizacyjnych służących przeciwdziałaniu zagrożeniom dla ochrony danych osobowych,
      e. przestrzegania zasad i obowiązków określonych w dokumentacji przetwarzania danych osobowych;
      f. zatwierdzanie klauzul dotyczących RODO w regulacjach wewnętrznych.
   4) informowanie ADO o wykrytych nieprawidłowościach w procesach ochrony danych osobowych oraz inicjowanie działań naprawczych;
   5) pełnienie roli „punktu kontaktowego" dla organu nadzorczego w kwestiach związanych z przetwarzaniem, w tym z uprzednimi konsultacjami, o których mowa w art. 36 Rozporządzenia oraz wszystkich zainteresowanych osób fizycznych, których dane osobowe przetwarzane są w Banku;
   6) udział w kontrolach przeprowadzanych przez kontrolerów organu nadzorczego;
   7) opiniowanie w sprawie możliwości oraz prawidłowości zbierania danych osobowych w celu utworzenia zbioru danych osobowych, zbierania nowych kategorii danych do istniejącego już zbioru lub przetwarzania danych w innym celu niż ten, dla którego dane zostały zebrane;
   8) opiniowanie i nadzór w zakresie wykonania obowiązku informacyjnego; wzór obowiązku informacyjnego stanowi złącznik nr 3 do „Instrukcji obsługi praw klienta w zakresie danych osobowych w Banku Spółdzielczym w Szczytnie”;
   9) opiniowanie umów dotyczących powierzenia przetwarzania danych osobowych;
   10) rekomendowanie wdrożenia zasad: legalności, ograniczonego celu, minimalizacji danych, prawidłowości, ograniczenia przechowywania oraz rozliczalności;
   11) opiniowanie w sprawie udostępniania danych osobowych odbiorcom danych;
   12) wydawanie rekomendacji co do wprowadzenia zmian w strukturach informatycznych lub organizacyjnych pożądanych lub koniecznych ze względu na ochronę danych

osobowych, w tym ze względu na zmianę przepisów, orzecznictwa lub praktyki w powyższym zakresie;

13) udzielanie osobom, których dane osobowe są przetwarzane, odpowiedzi wynikającej z prawa tych osób do kontroli przetwarzania danych;
14) wydawanie pisemnych rekomendacji osobom przetwarzającym dane osobowe celem przetwarzania ich zgodnie z przepisami prawa i aktami wewnętrznymi lub zawiadamianie ADO, wskazując osobę odpowiedzialną za naruszenie tych zasad oraz jego zakres;
15) nadzór nad ewidencjonowaniem osób upoważnionych do przetwarzania danych osobowych z uwzględnieniem ich funkcji służbowych i uprawnień;
16) rozstrzyganie kwestii spornych dotyczących przetwarzania danych osobowych;
17) monitorowanie zgodności działania z aktualnie obowiązującymi przepisami prawa, wytycznymi i zaleceniami organu nadzorczego, oraz wskazywanie niezbędnych działań dostosowawczych w przypadku zmian przepisów i zaleceń;
18) zapewnienie szkoleń wstępnych i okresowych dla pracowników Banku z zakresu ochrony danych osobowych;
19) prowadzenie postępowań wyjaśniających naruszenie ochrony danych osobowych zgodnie z Instrukcją zarządzania incydentem bezpieczeństwa w Banku Spółdzielczym w Szczytnie;
20) prowadzenie rejestru czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 1 Rozporządzenia, zgodnie ze wzorem stanowiącym załącznik nr 4 do niniejszej Polityki;
21) prowadzenie rejestru kategorii czynności przetwarzania danych osobowych, o którym mowa w art. 30 ust. 2 Rozporządzenia, zgodnie ze wzorem stanowiącym załącznik nr 5 do niniejszej Polityki;
22) nadzór nad prowadzeniem rejestru incydentów bezpieczeństwa/naruszeń ochrony danych osobowych, zgodnie z zapisami Instrukcji zarządzania incydentem bezpieczeństwa w Banku Spółdzielczym w Szczytnie;
23) niezwłoczne informowanie organu nadzorczego o naruszeniach ochrony danych osobowych zgodnie z zapisami Instrukcji zarządzania incydentem bezpieczeństwa w Banku Spółdzielczym w Szczytnie;
24) koordynowanie procesu zawiadamiania klientów Banku, których dane dotyczą, o naruszeniu ochrony danych osobowych, o którym mowa w art. 34 Rozporządzenia, jeżeli to naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych, zgodnie z zapisami Instrukcji zarządzania incydentem bezpieczeństwa w Banku Spółdzielczym w Szczytnie;
25) koordynowanie działań w procesie przeprowadzania oceny skutków dla ochrony danych zgodnie z art. 35 Rozporządzenia, sporządzane na podstawie załącznika nr 5 do niniejszej Polityki oraz monitorowanie wykonania zaleceń wynikających z tej oceny;
26) informowanie Zarządu Banku, Podmioty przetwarzające oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich, które wynikają z Rozporządzenia oraz z innych przepisów Unii lub państw członkowskich o ochronie danych i doradzanie im w tej sprawie.

2. IODO zobowiązany jest do wykonywania powyższych zadań w trybie priorytetowym.

§ 9.

1. Zespół IT jest zobowiązana do zapewnienia zabezpieczenia danych osobowych w obszarze związanym z ich przetwarzaniem w systemach informatycznych.
2. Zarząd Banku jest zobowiązany do zapewnienia:
   1) fizycznego zabezpieczenia pomieszczeń, w których przetwarzane są dane osobowe;
   2) zasilania gwarantowanego urządzeniom, przy pomocy których przetwarzane są dane osobowe.
3. Zespół IT są zobowiązani informować IODO o zmianach w zastosowanych środkach zabezpieczeń w obszarze przetwarzania danych osobowych.
4. SOA jest odpowiedzialna za:
   1) wydawanie upoważnień do przetwarzania danych osobowych w momencie zawarcia umowy o pracę lub umowy cywilnoprawnej i prowadzenia rejestru upoważnień pracowników i osób, z którymi zawarto umowy cywilnoprawne;
   2) wprowadzanie zawartych umów powierzenia przetwarzania danych osobowych do Rejestru umów prowadzonego w systemie Intranet.BS
   3) organizowanie szkoleń z zakresu bezpieczeństwa danych osobowych we współpracy z IODO.

§ 10.

1. Kierownik jednostki lub komórki organizacyjnej odpowiedzialny jest za:
   1) współdziałanie z IODO w zakresie przestrzegania zasad ochrony danych osobowych w Banku;
   2) występowanie z wnioskiem o nadanie uprawnień w systemie informatycznym, jeżeli dane przetwarzane są w formie elektronicznej, zgodnie z procedurą nadawania uprawnień ujętą w Instrukcji Zarządzania Systemami Informatycznymi w Banku Spółdzielczym w Szczytnie;
   3) niezwłoczne występowanie z wnioskiem o odebranie uprawnienia do przetwarzania danych osobowych osobie upoważnionej do przetwarzania danych osobowych, której zakres obowiązków zmienił się lub ustała przyczyna, dla której uprawnienia takie zostały nadane;
   4) zgłoszenie do IODO zamiaru utworzenia, modyfikacji lub likwidacji zbioru danych osobowych, za który jest odpowiedzialny;
   5) nadzór nad podmiotami przetwarzającymi w obszarze zgodnym z umową przetwarzania danych, co do celów, zakresu i czasu przetwarzania;
   6) współpracę z IODO w zakresie obsługi incydentów naruszenia ochrony danych oraz wdrażania mechanizmów zabezpieczających,
   7) konsultowanie z IODO zapisów w umowach dotyczących ochrony oraz przetwarzania danych osobowych.

§ 11.

1. Każdy pracownik lub osoba, przy pomocy której Bank wykonuje swoje czynności, dopuszczona do przetwarzania danych osobowych zarządzanych przez ADO, winna posiadać upoważnienie do przetwarzania danych osobowych zawierające:
   1) imię i nazwisko osoby upoważnionej;
   2) datę nadania i okres jego obowiązywania;

3) zakres upoważnienia do przetwarzania danych osobowych.

2. Wzór upoważnienia do przetwarzania danych osobowych stanowi załącznik nr 3 do niniejszej Polityki.
3. Szczegółową procedurę nadawania, modyfikacji i anulowania uprawnień w systemach informatycznych reguluje Instrukcja Zarządzania Systemami Informatycznymi w Banku Spółdzielczym w Szczytnie.
4. Każdy pracownik, przed dopuszczeniem do pracy związanej z dostępem do danych osobowych, obowiązkowo odbywa szkolenie z zasad ochrony danych osobowych. Obowiązek ten dotyczy również osób wykonujących prace na podstawie umowy cywilnoprawnej, o ile wykonanie zlecanych czynności związane będzie z dostępem do danych osobowych.
5. Każdy pracownik lub osoba, przy pomocy której Bank wykonuje swoje czynności, przetwarzająca dane osobowe, zobowiązana jest zapewnić ich należytą ochronę, a w szczególności odpowiada za:
   1) przestrzeganie zasad bezpiecznego przetwarzania danych osobowych wynikających z Rozporządzenia, przepisów prawa i unormowań wewnętrznych, w wykonywanych zadaniach,
   2) wykonywanie operacji na danych osobowych zgodnie z nadanymi uprawnieniami i zakresem upoważnienia do przetwarzania danych osobowych,
   3) stosowanie mechanizmów zabezpieczających,
   4) zgłaszanie incydentów naruszenia bezpieczeństwa danych osobowych.

§ 12.

Naruszenie postanowień niniejszej Polityki stanowi ciężkie naruszenie obowiązków pracowniczych lub umownych w przypadku współpracowników.

Rozdział 6. **Powierzanie przetwarzania danych osobowych oraz zachowanie tajemnicy bankowej**

§ 13.

1. Bank może powierzyć przetwarzanie danych osobowych innemu podmiotowi wyłącznie w zakresie przewidzianym w umowie oraz o ile Podmiot przetwarzający daje gwarancje bezpieczeństwa powierzonych danych poprzez właściwe zarządzanie bezpieczeństwem informacji i wdrożenie środków proceduralno-organizacyjnych, technicznych i fizycznych, które zapewniają ochronę przetwarzania danych osobowych odpowiednią do ryzyka, zagrożeń oraz kategorii danych osobowych objętych ochroną i kategorii osób, których dane dotyczą.
2. Decyzję o powierzeniu przetwarzania danych osobowych podejmuje Zarząd na podstawie weryfikacji przeprowadzonej przy wsparciu IODO przez jednostkę koordynującą zgodnie z zapisami Instrukcji „Zasady outsourcingu czynności bankowych i maklerskich w Banku Spółdzielczym w Szczytnie” oraz na podstawie analizy podmiotu przetwarzającego, która przeprowadzana jest w oparciu o ankietę, której wzór stanowi załącznik nr 9 do niniejszej Polityki.

3. 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.
4. Zawarte umowy powierzenia przetwarzania danych osobowych przechowywane są przez SOA.
5. Raz w roku lub w przypadku zmian w zakresie powierzenia przetwarzania danych osobowych, jednostka koordynująca przy wsparciu IODO, przeprowadza weryfikację procesu powierzenia przetwarzania danych osobowych oraz Podmiotów przetwarzających w oparciu o ankietę, której wzór stanowi załącznik nr 9 do niniejszej Polityki.
6. Weryfikacja Podmiotów przetwarzających, do których stosuje się zapisy „Polityki zarządzania ryzykiem outsourcingu w Banku Spółdzielczym w Szczytnie" odbywa się dodatkowo zgodnie z zapisami w „Instrukcji Zasady outsourcingu czynności bankowych i maklerskich w Banku Spółdzielczym w Szczytnie".
7. 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 ADO 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 ADO 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 ADO naruszenia powierzonych danych osobowych.
8. Wzór „Umowy powierzenia przetwarzania danych osobowych oraz zachowania tajemnicy bankowej" stanowi załącznik nr 2 do niniejszej Polityki. W przypadku umowy, w której załącznik jest inny niż wzorcowy, wymagana jest pozytywna opinia IODO.
9. Każdorazowo, w przypadku konieczności zmiany lub modyfikacji obowiązujących umów, o których mowa w ust. 1 oraz w ust. 8, nowa treść wymaga akceptacji IODO.

Rozdział 7. **Współadministrowanie danymi osobowymi**

§ 14.

1. Bank może wspólnie z innym podmiotem lub podmiotami ustalać cele i sposoby przetwarzania danych osobowych niezbędny do osiągniecia celów i założeń biznesowych.
2. W przypadku współadministrowania danymi osobowymi, Bank zobowiązany jest do zawarcia umowy o współadministrowanie danymi osobowymi, w której

współadministratorzy w przejrzysty sposób określają odpowiednie zakresy swojej odpowiedzialności dotyczącej wypełniania obowiązków wynikających z RODO, w szczególności w odniesieniu do wykonywania przez osobę, której dane dotyczą, przysługujących jej praw, oraz obowiązków w odniesieniu spełnienia obowiązku informacyjnego.

3. Wzór umowy o współadministrowanie danymi osobowymi w przypadku zawierania Konsorcjum bankowego określono w załączniku nr 7 do „Regulaminu zawierania konsorcjów bankowych".
4. W przypadku konieczności zawarcia umowy, o której mowa w ust. 3, zawierającej odstępstwa od wzorca obowiązującego u Administratora danych, wymagane jest uprzednie uzyskanie akceptacji IODO dla projektu umowy.

Rozdział 8. **Środki zabezpieczenia danych osobowych**

§ 15.

Zbiory danych osobowych są chronione w sposób zapewniający zabezpieczenie przetwarzanych danych osobowych w systemach informatycznych i na nośnikach informacji przed utratą poufności, integralności, dostępności i rozliczalności tych danych, ze szczególnym uwzględnieniem postanowień dotyczących regulacji wewnętrznych z zakresu zarządzania systemami informatycznymi oraz postępowania z informacjami stanowiącymi tajemnicę w Banku.

§ 16.

Do ochrony systemów informatycznych, w których przetwarzane są dane osobowe, wykorzystuje się wszelkie adekwatne programowe i sprzętowe zabezpieczenia oraz dodatkowe, dostępne środki techniczne i organizacyjne. Wykaz zastosowanych minimalnych środków technicznych i organizacyjnych stanowi załącznik nr 1 do niniejszej Polityki.

§ 17.

1. Dane osobowe mogą być przetwarzane jedynie przez osoby, które posiadają upoważnienie nadane przez ADO oraz zostały zobowiązane do zachowania tajemnicy przetwarzanych danych i sposobu ich zabezpieczenia.
2. Osoby, które nie posiadają upoważnienia, mogą przebywać w obszarach przetwarzania danych osobowych jedynie w obecności innej osoby, która posiada stosowne upoważnienie.
3. Budynki i pomieszczenia, stanowiące obszary przetwarzania danych osobowych, są objęte systemem zabezpieczenia technicznego i są zabezpieczane po ich opuszczeniu przez osoby upoważnione do pracy w tych pomieszczeniach.
4. Okres retencji danych osobowych przetwarzanych przez Bank jest uzależniony od celu, dla jakiego przetwarzane są dane. Okresy retencji zostały określone w prowadzonym Rejestrze czynności przetwarzania.
5. Usuwanie danych osobowych oraz niszczenie nośników informacji odbywa się z zachowaniem zasad określonych w odrębnych regulacjach wewnętrznych.
6. Dane osobowe są udostępniane jedynie uprawnionym podmiotom z uwzględnieniem przepisów Rozporządzenia, regulacji wewnętrznych oraz innych przepisów powszechne obowiązujących.

§ 18.

Zastosowane środki techniczne i organizacyjne stanowiące zabezpieczenie danych osobowych, podlegają okresowemu monitorowaniu ze względu na ich skuteczność i dostosowanie do aktualnego poziomu wiedzy i rozwoju technologicznego oraz wyników szacowania ryzyka.

Rozdział 9. **Zasady analizy ryzyka i ocena skutków dla ochrony danych**

1. 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.
2. 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.
3. Wzorcowy arkusz analizy ryzyka stanowi załącznik nr 7 do niniejszej Polityki.
4. Bank dokonuje oceny skutków planowanych operacji przetwarzania dla ochrony danych osobowych, jeżeli dany rodzaj przetwarzania, ze względu na swój charakter, zakres, kontekst i cele, z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia prawa lub wolności osoby lub osób fizycznych,
5. Kryteria, po spełnieniu, których ocena skutków planowanych operacji przetwarzania danych dla ochrony danych jest obligatoryjna, jak i sposób jej wykonania, zostały określone w „Procedurze oceny skutków przetwarzania dla ochrony danych (DPIA)", która stanowi załącznik nr 6 do niniejszej Polityki.

Rozdział 10. **Naruszenia ochrony danych osobowych**

1. Naruszenie ochrony danych osobowych oznacza naruszenie ich 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.
2. Zasady postępowania z incydentami bezpieczeństwa danych osobowych reguluje „Instrukcja zarządzania incydentem bezpieczeństwa w Banku Spółdzielczym w Szczytnie".

Rozdział 11. **Realizacja praw osób, których dane dotyczą**

Zasady informowania i przejrzystej komunikacji związanej z przetwarzaniem danych osobowych oraz tryb wykonywania praw przez osobę, której dane dotyczą zostały określone w „Instrukcji obsługi praw klienta w zakresie danych osobowych w Banku Spółdzielczym w Szczytnie".

Rozdział 12. **Uwzględnienie ochrony danych osobowych w fazie projektowania i ochrona domyślna**

1. Właściciel biznesowy i administrator systemu (w ramach systemu teleinformatycznego, na bazie, którego będzie realizowana usługa) podczas projektowania każdej z nowych usług, produktów, narzędzi lub rozwiązań, a przed wdrożeniem projektu, uwzględnia ochronę danych osobowych, jeżeli w projekcie zakłada się ich przetwarzanie, w tym przeprowadza konsultacje z IODO. Niniejszy obowiązek dotyczy każdej osoby odpowiedzialnej za wdrażanie (projektowanie) nowych usług, produktów, narzędzi lub rozwiązań.
2. Zgodnie z wymogami RODO, każda komórka organizacyjna działająca w imieniu Administratora danych wdraża odpowiednie środki techniczne i organizacyjne tak, aby domyślnie przetwarzane były wyłącznie te dane osobowe, które są niezbędne dla osiągnięcia konkretnego celu ich przetwarzania. Obowiązek ten odnosi się do ilości zbieranych danych osobowych, zakresu ich przetwarzania, okresu ich przechowywania oraz ich dostępności.
3. W celu realizacji wymogu wdrażania mechanizmów domyślnej ochrony danych, domyślnie dane osobowe można przetwarzać tylko w zakresie, w jakim przetwarzanie jest niezbędne i proporcjonalne do realizacji celu przetwarzania.

Rozdział 13. **Aktualizacja Polityki**

§ 19.

1. Polityka podlega przeglądom i aktualizacji przez IODO nie rzadziej niż raz w roku.
2. Załącznik nr 1 stanowi opis minimalnych zabezpieczeń i środków technicznych zastosowanych w Banku w celu ochrony przetwarzanych danych osobowych. Prowadzony i utrzymywany jest w aktualności przez IODO po uzyskaniu informacji od Zespołu IT oraz Zarządu Banku.
3. Poza planowymi przeglądami, niniejsza Polityka podlega obowiązkowej aktualizacji w przypadku zmian przepisów dotyczących ochrony danych osobowych lub zmian w funkcjonowaniu Banku, mających wpływ na system zabezpieczenia danych osobowych.

Rozdział 14. **Postanowienia końcowe**

§ 20.

Załączniki do niniejszej Polityki po wypełnieniu nie podlegają publikacji.

§ 21.

Załączniki do Polityki prowadzone są w formie elektronicznej.