



BYDGOSZCZ

**Polityka bezpieczeństwa danych osobowych w Banku
Spółdzielczym w Bydgoszczy**

Bydgoszcz 2019

Spis treści

Rozdział 1.	Postanowienia wstępne.....	3
Rozdział 2.	Zasady ochrony danych osobowych.....	5
Rozdział 3.	Bezpieczeństwo danych osobowych.....	5
Rozdział 4.	Informacja i dostęp do danych.....	6
Rozdział 5.	Inspektor ochrony danych osobowych	6
Rozdział 6.	Rejestrowanie czynności przetwarzania	7
Rozdział 7.	Ocena skutków dla ochrony danych	7
Rozdział 8.	Postanowienia końcowe	8

Załączniki:

- 1. Wzór Rejestru czynności przetwarzania i kategorii czynności**
- 2. Schemat oceny skutków dla ochrony danych osobowych**

Rozdział 1. Postanowienia wstępne

§ 1

Polityka ochrony danych osobowych w Banku Spółdzielczym w Bydgoszczy, zwana dalej „Polityką”, została opracowana na podstawie 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.

§ 2

1. Niniejsza Polityka jest dokumentem opisującym zasady ochrony danych osobowych stosowane przez Bank. Zakres przedmiotowy stosowania Polityki obejmuje wszystkie dane osobowe przetwarzane w Banku, zarówno w formie elektronicznej, jak i manualnie.
2. Bank zabezpiecza dane osobowe pod kątem ochrony podstawowych praw i wolności osób fizycznych, w związku z przetwarzaniem ich danych osobowych.
3. Przez bezpieczeństwo danych osobowych należy rozumieć zapewnienie ich poufności, integralności, dostępności oraz rozliczalności, na zasadach przewidzianych w niniejszej Polityce i innych regulacjach wewnętrznych, do których ona odsyła, poprzez wdrożenie i stosowanie niezbędnych do tego celu mechanizmów technicznych i organizacyjnych.
4. Bank prowadzi wykaz zbiorów danych osobowych i systemów ich przetwarzania, wg wzoru zamieszczonego w Instrukcji IT, który przechowuje IOD.

§ 3

Przez użyte w niniejszej Polityce określenia należy rozumieć:

- 1) **Administrator (danych osobowych)** – Bank Spółdzielczy w Bydgoszczy, jako podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych,
- 2) **Inspektor Ochrony Danych (IOD)** – osoba formalnie wyznaczona przez Administratora, posiadająca odpowiednie kwalifikacje, wiedzę i umiejętności w dziedzinie ochrony

danych osobowych, do której zadań należy informowanie i doradzanie Administratorowi w zakresie przestrzegania obowiązków wynikających z przetwarzania danych osobowych;

- 3) **Bank** – Bank Spółdzielczy w Bydgoszczy,
- 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) **przetwarzanie danych osobowych** – 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,
- 6) **jednostka organizacyjna** – zorganizowana część Banku tworząca odrębną placówkę, która posiada strukturę organizacyjną. W Banku jednostkami organizacyjnymi są: Centrala, Oddziały wraz z Punktami Obsługi Klienta,
- 7) **komórka organizacyjna** – wewnętrzne elementy struktury Centrali Banku: Wydziały, Komórki, Samodzielne Stanowiska Pracy,
- 8) **pracownik Banku** – osoba zatrudniona w Banku na podstawie umowy o pracę lub świadcząca usługi na podstawie umowy cywilnoprawnej,
- 9) **Instrukcja IT** – Instrukcja Zarządzania Systemami Informatycznymi w Banku Spółdzielczym w Bydgoszczy,
- 10) **Instrukcja ODO** – Instrukcja ochrony danych osobowych w Banku Spółdzielczym w Bydgoszczy,
- 11) **zbiór danych** - uporządkowany zestaw danych osobowych dostępnych według określonych kryteriów, niezależnie od tego, czy zestaw ten jest scentralizowany, zdecentralizowany czy rozproszony funkcjonalnie lub geograficznie.

Rozdział 2. Zasady ochrony danych osobowych

§ 4

1. Zapewnienie przez Bank bezpieczeństwa danych osobowych polega na zapewnieniu:
 - 1) przetwarzania zgodnego z prawem, rzetelnego i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”),
 - 2) zbierania danych osobowych w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami („ograniczenie celu”),
 - 3) adekwatności i stosowności zbieranych danych osobowych oraz ograniczenia ich do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”),
 - 4) prawidłowości i aktualności przetwarzanych danych („prawidłowość”),
 - 5) przechowywania 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 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”).

Rozdział 3. Bezpieczeństwo danych osobowych

§ 5

1. Bank zapewnia bezpieczeństwo danych przetwarzanych w systemach informatycznych i poza nimi.
2. Szczegółowy opis stosowanych środków bezpieczeństwa znajduje się w Instrukcji ochrony danych osobowych w Banku Spółdzielczym w Bydgoszczy oraz Instrukcji zarządzania systemami informatycznymi w Banku Spółdzielczym w Bydgoszczy.

Rozdział 4. Informacja i dostęp do danych

§ 6

1. Bank zapewnia osobom, których dane osobowe przetwarza, poszanowanie ich praw do:
 - 1) uzyskania na etapie zbierania danych osobowych informacji, dotyczących przetwarzania jej danych osobowych.
 - 2) dostępu do przetwarzanych danych,
 - 3) przenoszenia swoich danych osobowych, przetwarzanych przez Bank,
 - 4) sprzeciwu wobec przetwarzania i profilowania ich danych osobowych,
 - 5) żądania sprostowania i usuwania danych,
 - 6) otrzymywania informacji o naruszeniu ochrony ich danych osobowych,

- na zasadach i w przypadkach określonych przepisami prawa i regulacjami wewnętrznymi Banku.
2. Wzory stosowanych w Banku klauzul informacyjnych znajdują się w Instrukcji ochrony danych osobowych w Banku Spółdzielczym w Bydgoszczy.
3. Podjęcie przez Bank działania w przypadkach opisanych w ust. 1 pkt 2) - 6) wymaga uprzedniej konsultacji z IOD.
4. Udostępnienie informacji obejmujących dane osobowe osobom i organom zewnętrznym jest możliwe wyłącznie zgodnie z przepisami prawa, w tym ustawy Prawo bankowe, za uprzednią zgodą IOD.

Rozdział 5. Inspektor ochrony danych osobowych

§ 7

1. Z uwagi na główną działalność Banku, w której wykonuje się operacje przetwarzania, wymagające ze względu na swój charakter, zakres i cele regularnego i systematycznego przetwarzania danych osobowych znacznej ilości osób, Bank wyznacza Inspektora Ochrony Danych Osobowych oraz jego Zastępcę.
2. Inspektorem Ochrony Danych jest osoba posiadająca odpowiednie kwalifikacje zawodowe i wiedzę fachową oraz umiejętności do wypełniania zadań IOD/~~ABI~~, wyznaczona przez Zarząd Banku.
3. Inspektor Ochrony Danych Osobowych:
 - 1) jest właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych,

- 2) wspierany przez Administratora Danych w wypełnianiu zadań, o których mowa w Instrukcji ochrony danych osobowych w Banku Spółdzielczym w Bydgoszczy, poprzez zapewnienie mu zasobów niezbędnych do wykonania tych zadań oraz dostępu do danych osobowych i operacji przetwarzania, a także zasobów niezbędnych do utrzymania jego wiedzy fachowej,
 - 3) nie otrzymuje instrukcji dotyczących wykonywania tych zadań,
 - 4) nie jest odwoływany ani karany za wypełnianie swoich zadań,
 - 5) bezpośrednio podlega najwyższemu kierownictwu administratora lub podmiotu przetwarzającego.
4. Postanowienia dotyczące Inspektora Ochrony Danych Osobowych stosuje się odpowiednio do jego Zastępcy.
 5. Szczegółowy zakres obowiązków IOD określony został w Instrukcji ODO.

Rozdział 6. Rejestrowanie czynności przetwarzania

§ 8

1. Z uwagi na brak sporadycznego charakteru przetwarzania danych osobowych w działalności Banku oraz przetwarzanie w ramach tej działalności danych szczególnych kategorii, Bank prowadzi Rejestr czynności przetwarzania i kategorii czynności, wg wzoru z załącznika nr 1 do niniejszej Polityki.
2. Rejestr czynności przetwarzania ma formę elektroniczną.

Rozdział 7. Ocena skutków dla ochrony danych

§ 9

1. Przed rozpoczęciem nowej operacji przetwarzania danych osobowych, a także cyklicznie (wg terminów wynikających z SIZ) dla już istniejących operacji przetwarzania, Bank dokonuje oceny skutków operacji przetwarzania dla ochrony danych osobowych (analiza i ocena ryzyka). Szczegółowy schemat oceny skutków dla ochrony danych zawiera załącznik nr 2 do niniejszej Polityki.
2. Analiza zawiera poniższe elementy:
 - 1) systematyczny opis przeprowadzanych (lub planowanych) operacji i celów przetwarzania na danych osobowych, podlegających ocenie,
 - 2) ocenę, czy operacje przetwarzania są niezbędne i proporcjonalne w stosunku do celów,
 - 3) ocenę ryzyka naruszenia praw i wolności osób, których dane dotyczą,

- 4) wskazanie i dokonanie oceny środków planowanych do zastosowania w celu minimalizacji ryzyka, w tym zabezpieczeń oraz środków i mechanizmów bezpieczeństwa, mających zapewnić ochronę danych osobowych i wykazać przestrzeganie przepisów niniejszej Polityki i powszechnie obowiązujących przepisów prawa, z uwzględnieniem praw i prawnie uzasadnionych interesów osób, których dane dotyczą.
3. Niezależnie od okoliczności wymienionych w ust. 1, Bank dokonuje oceny skutków przetwarzania w sytuacjach określonych w art. 35 ust. 3 RODO.
4. Dla podobnych operacji przetwarzania danych wiążących się z podobnym ryzykiem można przeprowadzić pojedynczą ocenę.
5. Analiza ryzyka jest dokonywana przy współudziale osób odpowiedzialnych za przetwarzanie i ochronę danych osobowych w Banku Spółdzielczym w Bydgoszczy, które dokonują identyfikacji zagrożeń (ryzyk) i działań obniżających poziom ryzyka oraz Inspektora Ochrony Danych. Inspektor Ochrony Danych monitoruje wykonanie analizy zgodnie z art. 35 RODO, rekomenduje środki zapobiegawcze i przedstawia wyniki analizy Administratorowi.

Rozdział 8. Postanowienia końcowe

§ 10

1. Polityka podlega przeglądom i aktualizacji przez IOD nie rzadziej niż raz w roku.
2. 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.