Polityka ochrony danych osobowych Banku BGŻ BNP Paribas S.A.

Poziom	1
Rodzaj regulacji	Polityka
Status	
Wersja	1.0
Zakres stosowania	Bank BGŻ BNP Paribas S.A.
Właściciel Regulacji	Pion Ryzyka Operacyjnego i Przeciwdziałania Nadużyciom
Autor Regulacji	Pion Ryzyka Operacyjnego i Przeciwdziałania Nadużyciom
Kategoria regulacji	Organizacja i zarządzanie bankiem
Przedmiot regulacji	Ochrona danych osbowych
Zatwierdzający	Zarząd Banku
Data zatwierdzenia	2018-05-23
Data wejścia w życie	2018-05-25
Data ostatniej aktualizacji	
Poziom poufności	Poufne w banku
Przepisy nadrzędne (wypełnić jeśli przepis stanowi wdrożenie przepisów wyższego stopnia)	n/d
Przepis uchylany	ZA/0243/2015 Polityka ochrony danych osobowych i tajemnicy bankowej (exBNP)
Odniesienie do przepisów zewnętrznych (wypełnić jeśli przepis wprowadzany jest w celu dostosowania do przepisów prawa/wymogów organów nadzoru)	ROZPORZĄDZENIE PARLAMENTU EUROPEJSKIEGO I RADY (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
Ryzyka mitygowane przez wprowadzaną Regulację Wewnętrzną	Ryzyko niezgodności z przepisami prawa, pozostałymi regulacjami wewnętrznymi lub rekomendacjami organów nadzoru.
Czy do Regulacji Wewnętrznej został przygotowany test weryfikujący jej znajomość przez pracowników Banku	Nie
Opis wprowadzanych zmian, w porównaniu do obowiązującej Regulacji Wewnętrznej	Zmiany wprowadzone w związku z implementacją wymogów Rozporządzenia RODO.
Sygnatura/Załącznik	

Spis treści:

Wstęp

1. Wprowadzenie

Przyjęta przez Bank Polityka Ochrony Danych Osobowych (zwana dalej: „Polityką") ma na celu wprowadzenie zasad i procedur bezpieczeństwa oraz ochrony informacji.

Przyjęte zasady i procedury są zgodne z przepisami prawa oraz decyzjami i rekomendacjami Prezesa Urzędu Ochrony Danych Osobowych (zwanego dalej: „PUODO") i Komisji Nadzoru Finansowego (zwaną dalej: „KNF"), a także standardami grupy kapitałowej BNP Paribas, do której należy Bank.

2. Podstawy prawne

Niniejsza Polityka powstała w oparciu o następujące regulacje prawne:

i. 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 (zwane dalej **„RODO"**),
ii. ustawa z dnia [.] r. o ochronie danych osobowych (zwana dalej: „**Ustawą**"),
iii. ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (z późn. zm.) zwana dalej „**ustawą Prawo bankowe**".

3. Cel Polityki

Celem wdrożenia Polityki jest zapewnienie przetwarzaniu danych osobowych przez Bank, będący administratorem danych, zgodności z prawem, w szczególności w następującym zakresie:

a) przetwarzania danych wyłącznie na podstawie określonej w RODO;
b) dla zgodnych z prawem celów i w stopniu adekwatnym w stosunku do celów przetwarzania;

c) przechowywania w postaci umożliwiającej identyfikację osób, których dotyczą, nie dłużej niż jest to niezbędne do osiągnięcia celu przetwarzania lub nie dłużej niż określa to ustawa lub inne stosowne przepisy (np. ustawa o rachunkowości);
d) spełniania obowiązków informacyjnych wobec osoby, której dane dotyczą, w przypadku zbierania jej danych wprost od niej albo z innego źródła;
e) zautomatyzowanego podejmowania decyzji, w tym profilowania;
f) prowadzenia rejestrów czynności przetwarzania danych i kategorii czynności przetwarzania danych;
g) raportowania naruszeń ochrony danych osobowych do organu nadzorczego;
h) powołania i umiejscowienia w Banku Inspektora Ochrony Danych;
i) powierzania przez Bank przetwarzania danych innemu podmiotowi, w drodze umowy;
j) respektowania praw osoby, której dane dotyczą;
k) zabezpieczenia danych osobowych.

4. Definicje

Stosowane w Polityce określenia należy definiować następująco:

a) Bank – Bank BGŻ BNP Paribas S.A.; administrator danych osobowych;
b) grupa kapitałowa – grupa kapitałowa BNP Paribas do której należy Bank;
c) dane osobowe - oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą"); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej;
d) rejestr czynności przetwarzania danych – wykaz czynności przetwarzania danych osobowych prowadzonych przez Bank jako administratora danych;
e) rejestr kategorii czynności przetwarzania danych - wykaz kategorii czynności przetwarzania danych osobowych prowadzonych przez Bank jako procesora;
f) przetwarzanie danych - oznacza operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie;
g) anonimizacja – nieodwracalny proces przeprowadzony na danych osobowych, którego skutkiem jest pozbawienie danych wystarczającej liczby elementów, tak aby na ich podstawie nie było już możliwości zidentyfikowania osoby, której dane dotyczą;
h) profilowanie – 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
i) system informatyczny - zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych;

j) 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;

k) odbiorca danych – oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, któremu ujawnia się dane osobowe, niezależnie od tego, czy jest stroną trzecią1. Organy publiczne, które mogą otrzymywać dane osobowe w ramach konkretnego postępowania zgodnie z prawem Polskim lub UE, nie są uznawane za odbiorców;

l) integralność danych — właściwość zapewniająca, że dane osobowe nie zostały zmienione lub zniszczone w sposób nieautoryzowany;

m) rozliczalność — możliwość wykazania przez Bank, że podejmowane przez niego działania są zgodne z zasadami przetwarzania danych osobowych wskazanymi w art. 5 RODO.

n) Komitet ds. Ochrony Danych – komitet właściwy do omawiania oraz podejmowania decyzji w zakresie zasad ochrony oraz przetwarzania danych osobowych.

Polityka Banku w zakresie ochrony danych osobowych

Zakres Polityki ochrony danych osobowych

Polityka opisuje kwestie związane z przetwarzaniem danych osobowych w Banku, to jest:

i. podstawy przetwarzania danych osobowych;
ii. realizację i zakres obowiązku informacyjnego wobec podmiotów danych;
iii. okres retencji danych osobowych przetwarzanych przez Bank;
iv. regulacje dotyczące powierzenia przetwarzania danych przez Bank;
v. okres retencji danych osobowych przetwarzanych przez Bank;
vi. kwestie związane z zautomatyzowanym podejmowaniem decyzji i profilowaniem;
vii. realizacje praw podmiotów danych;
viii. prowadzenie rejestrów czynności przetwarzania danych i kategorii czynności przetwarzania danych;
ix. zabezpieczenia przetwarzania danych osobowych w systemach informatycznych stosowanych przez Bank.

1. Zadania oraz obowiązki jednostek organizacyjnych Banku uczestniczących w przetwarzaniu danych osobowych

1.1. Obowiązki Inspektora Ochrony Danych:

i. Pełni funkcję punktu kontaktowego dla PUODO w kwestiach związanych z przetwarzaniem danych, w tym w związku z uprzednimi konsultacjami, o których mowa w art. 36 RODO, oraz w stosownych przypadkach prowadzi konsultacji we wszelkich innych sprawach dotyczących przetwarzania danych osobowych w Banku;

[1] „strona trzecia" oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub podmiot inny niż osoba, której dane dotyczą, administrator, podmiot przetwarzający czy osoby, które – z upoważnienia administratora lub podmiotu przetwarzającego – mogą przetwarzać dane osobowe.

ii. Współpracuje z PUODO w zakresie kwestiach związanych z przetwarzaniem danych osobowych;
iii. Odpowiada za właściwą organizację oraz koordynację procesów szkoleniowych z tematyki ochrony danych osobowych, w szczególności informuje Bank oraz jego pracowników, którzy przetwarzają dane osobowe, o obowiązkach spoczywających na nich na mocy RODO oraz innych obowiązujących przepisów o ochronie danych i i doradza im w tym zakresie;
iv. Odpowiada za właściwą organizację procesu zarzadzania incydentami ochrony danych osobowych, w szczególności uczestniczy w procesowaniu każdego incydentu skutkującego koniecznością informowania podmiotów danych lub PUODO, jak również zarządza kryteriami oceny ryzyka incydentów ochrony danych osobowych;
v. Prowadzi rejestr czynności przetwarzania danych osobowych (w sytuacjach gdzie Bank działa jako administrator danych), rejestry kategorii czynności przetwarzania danych osobowych (w sytuacjach gdzie Bank działa jako procesor danych) oraz rejestr zgód stosowanych przez Bank. Inspektor Ochrony Danych udostępnia ww. rejestry na umotywowane żadanie innych jednostek organizacyjnych oraz PUODO lub innych organów lub podmiotów trzecich;
vi. Udziela na żądanie Banku zaleceń co do oceny skutków dla ochrony danych oraz monitoruje jej wykonanie zgodnie z art. 35 RODO, w szczególności uczestniczy w procesie oceny skutków przetwarzania danych osobowych.
vii. Odpowiada, przy wsparciu innych jednostek organizacyjnych w szczególności Pionu Prawego oraz Departamentu Bezpieczeństwa oraz Zapewnienia Ciągłości Działania, za doradztwo w sprawach związanych z przetwarzaniem danych osobowych.
viii. Koordynuje prace Komitetu ds. Ochrony Danych Osobowych.
ix. Nadzoruje i monitoruje przestrzeganie RODO i innych obowiązujących przepisów o ochronie danych oraz polityk Banku w dziedzinie ochrony danych osobowych, w szczególności odpowiada za kontrole w ramach II linii obrony oraz ocenę efektywności kontroli wykonywanych w ramach I linii obrony i procesów przetwarzania realizowanych w Banku;
x. Nadzoruje implementację zasad oraz regulacji Grupy BNPP w obszarze przetwarzania danych osobowych;
xi. Nadzoruje implementację w Banku zasad Privacy by default oraz Privacy by design;
xii. Nadzoruje kontakt z podmiotami danych, w szczególności proces rozpatrywania reklamacji, o ile mają one związek z przetwarzaniem danych osobowych.

1.2. Obowiązki Dyrektora Biura Data Governance i Regulacji Zewnętrznych:

x. Nadzór oraz kontrole I poziomu w zakresie poprawności, jakości, aktualności, dostępności oraz zasad ekstrakcji, agregacji i przepływu danych osobowych.
xi. Zarządzanie właścicielstwem danych osobowych.

1.3. Obowiązki Obszarów Zarządzania:

i. Każdy Obszar Zarządzania zobowiązany jest wyznaczyć Koordynatora ds. Ochrony Danych Osobowych. Obowiązkiem Koordynatora ds. Ochrony Danych Osobowych, jest właściwa organizacja zadań oraz przepływu informacji w ramach swojego obszaru, jak również reprezentowanie swojego obszaru w ramach Komitetu ds. Ochrony Danych;
ii. Przekazywanie Inspektorowi Ochrony Danych informacji o powołaniu lub zmianie osoby Koordynatora ds. Ochrony Danych Osobowych.

1.4. Obowiązki Pionu IT:

i. Realizacja zmian o charakterze IT, zgodnie z wymogami przedstawionymi przez inne jednostki organizacyjne, w szczególności zgodnie z wytycznymi Inspektora Ochrony Danych oraz Dyrektora Biura Data Governance i Regulacji Zewnętrznych.
ii. Realizacja właściwych kontroli I poziomu, w tym zleconych przez Inspektora Ochrony Danych oraz Dyrektora Biura Data Governance i Regulacji Zewnętrznych.
iii. Właściwe zarządzanie infrastrukturą IT, w sposób zapewniający poszanowanie zasad przetwarzania danych osobowych, w szczególności wymogów Rozporządzenia RODO.
iv. Zarządzanie uprawnieniami do systemów IT, w których dochodzi do przetwarzania danych osobowych, oraz prowadzenie ewidencji przedmiotowych uprawnień.

1.5. Obowiązki Pionu Operacji:
i. Właściwa realizacja obowiązków w zakresie wymogów dotyczących sposobu, miejsca, zasad oraz okresu przechowywania danych w dokumentacji papierowej. Wytyczne w tym zakresie, na podstawie których Pion Operacji realizuje swoje obowiązki wydaje Inspektor Ochrony Danych.
ii. Przekazywanie informacji oraz wyjaśnień, niezbędnych do właściwej i terminowej realizacji wymogów w zakresie ochrony danych osobowych, w szczególności udzielanie odpowiedzi na zapytania innych jednostek organizacyjnych odnośnie informacji o podmiotach danych (innych niż pracownicy Banku).
iii. Realizacja czynności operacyjnych w zakresie procesu przetwarzania i ochrony danych osobowych, w szczególności realizacja procesu komunikacji z podmiotami danych (innymi niż pracownicy Banku).
iv. Realizacja właściwych kontroli I poziomu, w tym zleconych przez Inspektora Ochrony Danych oraz Dyrektora Biura Data Governance i Regulacji Zewnętrznych.

1.6. Obowiązki Departamentu Bezpieczeństwa oraz Zapewnienia Ciągłości Działania:
i. Projektowanie i nadzór nad właściwymi środkami bezpieczeństwa, w tym bezpieczeństwa IT, organizacyjnego oraz fizycznego, zapewniającymi ochronę danych osobowych na poziomie wskazanym w obowiązujących przepisach prawa.
ii. Zarządzanie uprawnieniami do systemów IT, w których dochodzi do przetwarzania danych osobowych, oraz prowadzenie ewidencji przedmiotowych uprawnień.
iii. Zapewnienie właściwego wsparcia Inspektorowi Ochrony Danych w czynności wymagających wiedzy merytorycznej z obszaru bezpieczeństwa informacji.
iv. Realizacja zadań w zakresie zarządzania incydentami bezpieczeństwa, zgodnie z postanowieniami innych regulacji wewnętrznych.
v. Realizacja właściwych kontroli I poziomu.

1.7. Obowiązki Pionu Prawnego:
i. Opiniowanie dokumentacji związanej z przetwarzaniem i ochroną danych osobowych, od strony wymogów formalnoprawnych.
ii. Obsługa prawna zagadnień związanych z przetwarzaniem lub ochroną danych osobowych w Banku.
iii. Zapewnienie właściwego wsparcia Inspektorowi Ochrony Danych w zakresie zagadnień natury formalnoprawnej.

1.8. Obowiązki Obszaru Zarządzania Zasobami Ludzkimi:

i. Właściwe zarządzanie dokumentacją z obszaru przetwarzania oraz ochrony danych osobowych, w przypadku gdy podmiot danych jest pracownikiem Banku.
ii. Realizacja wymogów szkoleniowych, w zakresie tematyki związanej z przetwarzaniem i ochroną danych osobowych.
iii. Właściwa realizacja obowiązków w zakresie wymogów dotyczących sposobu, miejsca, zasad oraz okresu przechowywania danych osobowych, w przypadkach gdy gdy podmiot danych jest pracownikiem Banku.

1.9. Obowiązki Właściciela Danych, Właściciela Systemu oraz Właściciela Procesu:
i. Właściwe zarządzanie dokumentacją z obszaru przetwarzania oraz ochrony danych
ii. Inicjowanie oraz realizacja zmian w dokumentacji, procesach oraz infrastrukturze IT, w sposób zapewniający zgodności z wymogami obowiązujących przepisów prawa w zakresie ochrony danych osobowych.
iii. Zapewnienie właściwych pozycji budżetowych na wdrożenie zmian w dokumentacji, procesach lub infrastrukturze IT – w obszarze swojego właścicielstwa.
iv. Współpraca z Inspektorem Ochrony Danych Osobowych oraz Dyrektorem Biura Data Governance i Regulacji Zewnętrznych, w tym terminowe wdrażanie wydanych przez nich zaleceń odnośnie zasad przetwarzania oraz ochrony danych osobowych.

1.10.

2. Zasady przetwarzania danych osobowych

2.1. Bank jako administrator danych osobowych dokłada szczególnej staranności w celu ochrony interesów osób, których dane dotyczą, a w szczególności jest zobowiązany zapewnić, aby dane osobowe były:

i. przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą;
ii. zbierane w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzane dalej w sposób niezgodny z tymi celami;
iii. adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane;
iv. prawidłowe i w razie potrzeby uaktualniane; należy podjąć wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane;
v. przechowywane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane; dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO, z zastrzeżeniem że wdrożone zostaną odpowiednie środki techniczne i organizacyjne wymagane na mocy RODO w celu ochrony praw i wolności osób, których dane dotyczą;
vi. przetwarzane w sposób zapewniający odpowiednie bezpieczeństwo danych osobowych, w tym ochronę przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem, za pomocą odpowiednich środków technicznych lub organizacyjnych.

2.2. Bank jest odpowiedzialny za przestrzeganie zasad wskazanych powyżej i jest w stanie wykazać ich przestrzeganie.

3. Podstawy przetwarzania danych osobowych.

3.1. Bank dopuszcza przetwarzanie danych osobowych, gdy został spełniony co najmniej jeden z poniższych warunków:

i. osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych przez Bank w jednym lub większej liczbie określonych celów (np. marketingu produktów i usług podmiotów z grupy kapitałowej czy marketingu własnych produktów czy usług Banku dla osób nie będących klientami Banku);
ii. 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 (np. zawarcie umowy kredytowej lub na rachunek bieżący czy umowy ze zleceniobiorcą);
iii. przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na Banku (np. FATCA czy AML oraz przepisów związanych z zatrudnieniem i ubezpieczeniami społecznymi);
iv. przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;
v. przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Bankowi;
vi. przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez Bank 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 (np. marketingu bezpośredniego własnych produktów i usług Banku wobec jego klientów czy oceny rocznej pracowników Banku).

3.2. Zgoda, o której jest mowa w 3.1 pkt. i może obejmować również przetwarzanie danych w przyszłości, jeżeli nie zmienia się cel przetwarzania.

3.3. Za prawnie uzasadniony interes, o którym mowa w 3.1 pkt vi., uważa się w szczególności:

i. marketing bezpośredni własnych produktów lub usług Banku. Przetwarzanie przez Bank danych w celu prowadzenia marketingu produktów lub usług Banku nie wymaga zgody klienta, pod warunkiem, że w chwili tego przetwarzania łączy go z Bankiem zobowiązanie.
ii. dochodzenie roszczeń z tytułu prowadzonej działalności gospodarczej.

3.4. Zgody klienta wymaga:

i. marketing po wygaśnięciu umowy Klienta z Bankiem (np. w przypadku prób nakłonienia byłego klienta do ponownego zawarcia umowy z Bankiem), a także gdy klient wystąpił o zawarcie umowy lecz nie została ona zawarta;
ii. marketing produktów lub usług podmiotów innych niż Bank (w tym również podmiotów z Grupy kapitałowej, do której należy Bank).

3.5. Przez zgodę osoby, której dane dotyczą, należy rozumieć 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. Do wyraźnych działań wskazujących na wyrażenie zgody np. przez klienta zaliczyć można w szczególności wybór przez klienta ustawień technicznych systemu informatycznego, przekazanie przez klienta ustnie, pisemnie lub za pomocą elektronicznych środków komunikacji stosowanych przez Bank swoich danych osobowych, wrzucenie przez klienta wizytówki do pojemnika w celu udziału w konkursie, pod warunkiem, że wcześniej osoba ta zostanie poinformowana o konieczności przekazania danych (np. wizytówki) w przypadku chęci wzięcia udziału w konkursie.

3.6. Za wyrażenie zgody nie uznaje się m.in. milczenia osoby, braku sprzeciwu, niepodjęcia przez nią działań oraz zaznaczenia domyślnie okienek wyboru w systemie informatycznym.

3.7. Zgody nie uważa się za wyrażoną świadomie lub dobrowolnie, m.in. jeśli:

i. od wyrażenia przez osobę zgody uzależnione jest wykonanie umowy, w tym świadczenie usług, a do wykonania tej umowy zgoda nie jest niezbędna;
ii. osoba nie ma możliwości udzielenia osobnej zgody na różne cele przetwarzania danych w przypadkach, kiedy jest to stosowne, np. osobna zgoda na przetwarzanie danych w celach marketingowych Banku a osobna na udostępnienie danych podmiotowi z grupy w celach marketingowych;
iii. zapytanie o zgodę nie zostało przedstawione w sposób pozwalający wyraźnie odróżnić go od pozostałych kwestii, w przypadku gdy treść zgody na przetwarzanie danych zawarta jest w pisemnym oświadczeniu, które zawiera również inne treści, np. klauzula zgody na przetwarzanie danych osobowych zawarta w treści umowy pomiędzy bankiem a klientem.

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

3.9. Udzielone przez klienta zgody dotyczące przetwarzania danych mogą zostać przez niego w każdym czasie odwołane ze skutkiem natychmiastowym. Odwołanie zgody nie wpływa na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej wycofaniem.

3.10. Bank zbierając zgodę od osoby lub oświadczenie o wycofaniu zgody, powinien upewnić się, że osoba wyrażająca/wycofująca zgodę jest w rzeczywistości osobą, której dane dotyczą.

3.11. Rejestr zgód stosowanych przez Bank jest dostępny do wglądu u Inspektora Ochrony Danych.

3.12. Jeżeli w związku z przetwarzaniem danych osobowych przez Bank, w szczególności w zakresie podstaw przetwarzania danych osobowych, pojawią się jakiekolwiek wątpliwości lub pytania konieczne jest skontaktowanie się z Inspektorem Ochrony Danych.

4. Obowiązek informacyjny z art. 13 i art. 14 RODO

4.1. Jednym z podstawowych obowiązków towarzyszących zbieraniu danych osobowych jest obowiązek informacyjny, wynikający z art. 13 RODO (zbieranie danych bezpośrednio od osoby, której dane dotyczą) oraz art. 14 RODO (zbieranie danych nie bezpośrednio od osoby, której one dotyczą).

4.2. Jeżeli dane osobowe osoby, której dane dotyczą, zbierane są od tej osoby, Bank podczas pozyskiwania danych osobowych podaje jej wszystkie następujące informacje:

i. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
ii. dane kontaktowe inspektora ochrony danych;
iii. cele przetwarzania danych osobowych, oraz podstawę prawną przetwarzania;
iv. jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu Banku lub strony trzeciej – prawnie uzasadnione interesy realizowane przez Bank lub przez stronę trzecią;
v. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
vi. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych do państwa trzeciego lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych.
vii. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
viii. informacje o prawie do żądania od Banku dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania lub o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
ix. jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych (art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
x. informacje o prawie wniesienia skargi do organu nadzorczego;
xi. informację, czy podanie danych osobowych jest wymogiem ustawowym lub umownym lub warunkiem zawarcia umowy oraz czy osoba, której dane dotyczą, jest zobowiązana do ich podania i jakie są ewentualne konsekwencje niepodania danych;
xii. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

4.3. Jeżeli Bank planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym dane osobowe zostały zebrane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w 4.2 pkt. vii - xii.

4.4. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, Bank przekazuje informacje jest przekazywana podczas pozyskiwania danych.

4.5. Jeżeli danych osobowych nie pozyskano od osoby, której dane dotyczą, Bank podaje osobie, której dane dotyczą, następujące informacje:

i. swoją tożsamość i dane kontaktowe oraz, gdy ma to zastosowanie, tożsamość i dane kontaktowe swojego przedstawiciela;
ii. dane kontaktowe inspektora ochrony danych;
iii. cele przetwarzania, do których mają posłużyć dane osobowe, oraz podstawę prawną przetwarzania;
iv. kategorie odnośnych danych osobowych;
v. informacje o odbiorcach danych osobowych lub o kategoriach odbiorców, jeżeli istnieją;
vi. gdy ma to zastosowanie – informacje o zamiarze przekazania danych osobowych odbiorcy w państwie trzecim lub organizacji międzynarodowej oraz o stwierdzeniu lub braku stwierdzenia przez Komisję odpowiedniego stopnia ochrony lub w przypadku przekazania, o którym mowa w art. 46, art. 47 lub art. 49 ust. 1 akapit drugi RODO, wzmiankę o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych;
vii. okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe, kryteria ustalania tego okresu;
viii. jeżeli przetwarzanie odbywa się na podstawie prawnie uzasadnionego interesu Banku lub strony trzeciej – prawnie uzasadnione interesy realizowane przez Bank lub przez stronę trzecią;
ix. informacje o prawie do żądania od Banku dostępu do danych osobowych dotyczących osoby, której dane dotyczą, ich sprostowania, usunięcia lub ograniczenia przetwarzania oraz o prawie do wniesienia sprzeciwu wobec przetwarzania, a także o prawie do przenoszenia danych;
x. jeżeli przetwarzanie odbywa się na podstawie zgody podmiotu danych (art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) RODO) – informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem;
xi. informacje o prawie wniesienia skargi do organu nadzorczego;
xii. źródło pochodzenia danych osobowych, a gdy ma to zastosowanie – czy pochodzą one ze źródeł publicznie dostępnych;
xiii. informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

4.6. Informacje, o których mowa w 4.5, Bank podaje:

i. w rozsądnym terminie po pozyskaniu danych osobowych – najpóźniej w ciągu miesiąca – mając na uwadze konkretne okoliczności przetwarzania danych osobowych;
ii. jeżeli dane osobowe mają być stosowane do komunikacji z osobą, której dane dotyczą – najpóźniej przy pierwszej takiej komunikacji z osobą, której dane dotyczą; lub
iii. jeżeli planuje się ujawnić dane osobowe innemu odbiorcy – najpóźniej przy ich pierwszym ujawnieniu.

4.7. Jeżeli Bank planuje dalej przetwarzać dane osobowe w celu innym niż cel, w którym te dane zostały pozyskane, przed takim dalszym przetwarzaniem informuje on osobę, której dane dotyczą, o tym innym celu oraz udziela jej wszelkich innych stosownych informacji, o których mowa w 4.4 pkt. vii - xiii.

4.8. Informacje, o których mowa w 4.2 oraz 4.54.4, mogą być przekazywane m.in. jako klauzule informacyjne zawarte w dokumentach przeznaczonych dla osoby, której dane dotyczą, klauzule informacyjne w systemie informatycznym, ustna informacja przekazana przez konsultanta, po potwierdzeniu tożsamości osoby, której dane dotyczą, czy też informacja przekazana drogą elektroniczną z zastosowaniem zasad bezpieczeństwa. Informacje mogą być opatrzone standardowymi znakami graficznymi.

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

i. podmiot danych posiada stosowne informacje;
ii. 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. Do takich sytuacji zaliczyć należy m.in. przetwarzanie danych Klientów w celach archiwalnych w przypadku fuzji banków, danych odbiorców lub nadawców przelewów wpisanych podczas składania dyspozycji przelewu, danych członków zarządu i reprezentantów zawartych w wyciągach z Krajowego Rejestru Sądowego. W sytuacji nie udzielenia osobie informacji ze względu na powyższe, Bank podejmuje odpowiednie środki organizacyjne i techniczne w celu ochrony praw i wolności oraz prawnie uzasadnionych interesów osoby, której dane dotyczą, w tym udostępnia informacje publicznie, np. poprzez opublikowanie stosownego komunikatu na stronie internetowej banku lub wywieszenie informacji w punktach obsługi Klientów;
iii. pozyskanie lub ujawnienie danych osoby, której dane są zebrane nie bezpośrednio od niej, uregulowane jest w przepisach prawa przewidujących ochronę prawnie uzasadnionych interesów osoby, której dane dotyczą;
iv. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy bankowej oraz innych tajemnic ustawowo chronionych.

4.10. Bank zapewnia rozliczalność w zakresie realizacji lub braku realizacji obowiązków informacyjnych w szczególności poprzez zbieranie dokumentów przekazywanych osobom zawierające klauzule informacyjne, rejestrację rozmów telefonicznych, backup'y/zrzuty z ekranu systemu informatycznego, kopie listów lub wiadomości wysyłanych drogą elektroniczną do podmiotu danych zawierających klauzule informacyjne, analizy oraz procedury wewnętrzne banku, skrypty rozmów z klientami.

4.11. Jeżeli w związku z realizacją obowiązku informacyjnego przez Bank lub jego pracowników pojawią się jakiekolwiek pytania lub wątpliwości, konieczne jest skontaktowanie się z Inspektorem Ochrony Danych.

5. Inspektor Ochrony Danych

5.1. Bank, z uwagi na zrealizowanie przesłanek wskazanych w art. 37 ust. 1 pkt. b RODO, powołał Inspektora Ochrony Danych.

5.2. Inspektor Ochrony Danych podlega wyłącznie Zarządowi Banku i jest umiejscowiony w Pionie Ryzyka.

5.3. Bank zapewnia, by Inspektor Ochrony Danych był właściwie i niezwłocznie włączany we wszystkie sprawy dotyczące ochrony danych osobowych.

5.4. Bank zapewnia Inspektorowi Ochrony Danych zasoby niezbędne do wykonania tych zadań oraz dostęp do danych osobowych i operacji przetwarzania, a także zasoby niezbędne do utrzymania jego fachowej wiedzy.

5.5. Inspektor Ochrony Danych jest punktem kontaktowym dla podmiotów danych we wszystkich sprawach związanych z przetwarzaniem ich danych osobowych oraz z wykonywaniem praw przysługujących im na mocy RODO.

5.6. Zadania realizowane przez Inspektora Ochrony Danych wskazane zostały w pkt 1.1. Polityki.

5.7. Inspektor Ochrony Danych nie otrzymuje instrukcji dotyczących wykonywania swoich zadań. Nie może być on również odwoływany ani karany przez Bank za wypełnianie swoich zadań.

5.8. Inspektor Ochrony Danych jest zobowiązany do zachowania tajemnicy lub poufności co do wykonywania swoich zadań.

6. Prawa osoby fizycznej (klienta, pracownika etc.) w zakresie ochrony danych osobowych

6.1. Każda osoba, której dane przetwarza Bank, w ramach przysługującego jej praw wskazanych w rozdziale III RODO, jest uprawniona do skorzystania z praw wskazanych w rozdziale III RODO i opisanych poniżej w 6.7 – 6.12.

6.2. Podmiot danych jest uprawniony do zgłoszenia żądania, o którym mowa w punktach poniżej w formie pisemnej lub elektronicznej na formularzu udostępnionym przez Bank. Nie wyłącza to uprawnienia Klienta do złożenia żądania w innej akceptowalnej i możliwej do udokumentowania przez Bank.

6.3. W każdym przypadku żądanie podmiotu danych powinno wskazywać, jakich danych osobowych i czynności dotyczy. W przypadku, gdy żądanie jest nieprecyzyjne, w tym nie zawiera wskazania zakresu danych osobowych i czynności, jaka objęta jest wnioskiem, Bank zwraca się do Klienta o przekazanie takich informacji.

6.4. W przypadku braku sprecyzowania przez podmiot danych jakich danych i jakich czynności żądanie dotyczy, Bank jest uprawniony do wstrzymania realizacji żądania do momentu uzyskania wystarczających informacji od Klienta. Bank realizuje żądanie podmiotu danych zgodnie ze swoimi wewnętrznymi procedurami. Odpowiednie procedury postepowania w przypadku skorzystania przez podmiot danych z przysługujących mu praw zostały wskazane w następnych punktach.

6.5. Realizacja praw osoby, której dane dotyczą, przez Bank następuje w rozsądnym terminie uwzględniającym koszty, stopień trudności realizacji żądania oraz w oparciu o wewnętrzne procesy funkcjonujące w Banku.

6.6. Bank poinformuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe osoby, której dane dotyczą.

6.7. **Prawa dostępu do jej danych osobowych**

6.7.1. Osoba, której dane dotyczą, jest uprawniona do uzyskania od Banku potwierdzenia, czy przetwarzane są dane osobowe jej dotyczące, a jeżeli ma to miejsce, jest uprawniona do uzyskania dostępu do nich oraz następujących informacji w zakresie:

i. celów przetwarzania;
ii. kategorii danych osobowych;
iii. informacji o odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub zostaną ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych;
iv. w miarę możliwości, informacji o planowanym okres przechowywania danych osobowych, a gdy nie jest to możliwe, kryteriów ustalania tego okresu;
v. informacji o prawie do żądania od Banku sprostowania, usunięcia lub ograniczenia przetwarzania danych osobowych dotyczącego osoby, której dane dotyczą, oraz do wniesienia sprzeciwu wobec takiego przetwarzania;
vi. informacji o prawie wniesienia skargi do organu nadzorczego;
vii. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkich dostępnych informacji o ich źródle;
viii. informacji o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 RODO, oraz – przynajmniej w tych przypadkach – istotne informacje o zasadach ich podejmowania, a także o znaczeniu i przewidywanych konsekwencjach takiego przetwarzania dla osoby, której dane dotyczą.

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

6.7.3. Bank dostarczy osobie, której dane dotyczą, kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się osoba, której dane dotyczą, Bank pobiera opłatę w rozsądnej wysokości wynikającej z kosztów administracyjnych. Więcej na ten temat w procedurze wskazanej w 6.7.6.

6.7.4. Jeżeli osoba, której dane dotyczą, zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, Bank udziela informacji drogą elektroniczną.

6.7.5. Prawo do uzyskania kopii, o której mowa w 6.7.3 , nie może niekorzystnie wpływać na prawa i wolności innych.

6.7.6. Szczegółowe kwestie związane z uregulowaniem realizacji procesu prawa dostępu do danych znajdują się w innych regulacjach wewnętrznych Banku.

6.8. **Prawa do sprostowania danych**

6.8.1. Osoba, której dane dotyczą, ma prawo żądania od Banku sprostowania dotyczących go danych osobowych, które są nieprawidłowe.

6.8.2. Osoba, której dane dotyczą ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.

6.8.3. Prawo do sprostowania danych realizowane jest z uwzględnieniem art. 105 ust. 4i Prawa bankowego, który obowiązuje banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje kredytowe do informowania rejestrów kredytowych o całkowitej spłacie zobowiązań, ich wygaśnięciu, stwierdzeniu nieistnienia zobowiązania, korekcie jego wysokości oraz o nowo powstałych zobowiązaniach i ich aktualizacji, w odpowiednim terminie od wystąpienia okoliczności uzasadniających przekazanie informacji.

6.9. **Prawa do usunięcia danych („prawo do bycia zapomnianym")**

6.9.1. Osoba, której dane dotyczą, ma prawo żądania od Banku niezwłocznego usunięcia dotyczących jej danych osobowych, a Bank ma obowiązek bez zbędnej zwłoki usunąć dane osobowe, jeżeli zachodzi jedna z następujących okoliczności:

i. dane osobowe nie są już niezbędne do celów, w których zostały zebrane lub w inny sposób przetwarzane;
ii. 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), i nie ma innej podstawy prawnej przetwarzania;
iii. osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 1 RODO wobec przetwarzania i nie występują nadrzędne prawnie uzasadnione podstawy przetwarzania lub osoba, której dane dotyczą, wnosi sprzeciw na mocy art. 21 ust. 2 RODO (marketing bezpośredni) wobec przetwarzania;
iv. dane osobowe były przetwarzane niezgodnie z prawem;
v. dane osobowe muszą zostać usunięte w celu wywiązania się z obowiązku prawnego przewidzianego w prawie Polskim lub UE;
vi. dane osobowe zostały zebrane w związku z oferowaniem usług społeczeństwa informacyjnego, o których mowa w art. 8 ust. 1 RODO.

6.9.2. Jeżeli Bank upublicznił dane osobowe, a ma obowiązek usunąć te dane osobowe, to – biorąc pod uwagę dostępną technologię i koszt realizacji – podejmuje rozsądne działania, w tym środki techniczne, by poinformować administratorów przetwarzających te dane osobowe, że osoba, której dane dotyczą, żąda, by administratorzy ci usunęli wszelkie łącza do tych danych, kopie tych danych osobowych lub ich replikacje.

6.9.3. Prawo do bycia zapomnianym nie ma zastosowania, w zakresie w jakim przetwarzanie jest niezbędne m.in.:

i. do korzystania z prawa do wolności wypowiedzi i informacji;
ii. do wywiązania się z prawnego obowiązku wymagającego przetwarzania na mocy prawa Polskiego lub Unii Europejskiej lub do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Bankowi;

iii. do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych zgodnie z art. 89 ust. 1 RODO, o ile prawdopodobne jest, że prawo do bycia zapomnianym uniemożliwi lub poważnie utrudni realizację celów takiego przetwarzania; lub
iv. do ustalenia, dochodzenia lub obrony roszczeń.

6.9.4. Szczegółowe kwestie związane z uregulowaniem realizacji procesu prawa do bycia zapomnianym znajdują się w innych regulacjach wewnętrznych Banku.

6.10. **Prawa do ograniczenia przetwarzania danych**

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

i. osoba, której dane dotyczą, kwestionuje prawidłowość danych osobowych – na okres pozwalający administratorowi sprawdzić prawidłowość tych danych;
ii. przetwarzanie jest niezgodne z prawem, a osoba, której dane dotyczą, sprzeciwia się usunięciu danych osobowych, żądając w zamian ograniczenia ich wykorzystywania;
iii. administrator nie potrzebuje już danych osobowych do celów przetwarzania, ale są one potrzebne osobie, której dane dotyczą, do ustalenia, dochodzenia lub obrony roszczeń;
iv. osoba, której dane dotyczą, wniosła sprzeciw na mocy art. 21 ust. 1 wobec przetwarzania – do czasu stwierdzenia, czy prawnie uzasadnione podstawy po stronie administratora są nadrzędne wobec podstaw sprzeciwu osoby, której dane dotyczą.

6.10.2. Jeżeli przetwarzanie danych 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 Polskiego lub unijnego interesu publicznego.

6.10.3. Przed uchyleniem ograniczenia przetwarzania administrator informuje o tym osobę, której dane dotyczą.

6.10.4. Szczegółowe kwestie związane z uregulowaniem realizacji procesu prawa do ograniczenia przetwarzania znajdują się w innych regulacjach wewnętrznych Banku.

6.11. **Prawa do przenoszenia danych**

6.11.1. Osoba, której dane dotyczą, ma prawo otrzymać w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego dane osobowe jej dotyczące, które dostarczyła Bankowi, oraz ma prawo przesłać te dane osobowe innemu administratorowi bez przeszkód ze strony Banku, któremu dostarczono te dane osobowe, jeżeli:

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

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

6.11.3. Wykonanie prawa do przenoszenia danych pozostaje bez uszczerbku dla prawa wskazanego w 6.8 (prawa do usunięcia danych).

6.11.4. Szczegółowe kwestie związane z uregulowaniem procesu realizacji prawa do przenoszenia danych znajdują się w innych regulacjach wewnętrznych Banku.

6.12. **Prawa do sprzeciwu**

6.12.1. Osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw – z przyczyn związanych z jej szczególną sytuacją – wobec przetwarzania dotyczących jej danych osobowych opartego na uzasadnionym interesie prawnym administratora danych lub gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej Bankowie, w tym profilowania na podstawie tych przepisów. Administratorowi nie wolno już przetwarzać tych danych osobowych, chyba że wykaże on istnienie ważnych prawnie uzasadnionych podstaw do przetwarzania, nadrzędnych wobec interesów, praw i wolności osoby, której dane dotyczą, lub podstaw do ustalenia, dochodzenia lub obrony roszczeń.

6.12.2. Jeżeli dane osobowe są przetwarzane na potrzeby marketingu bezpośredniego, osoba, której dane dotyczą, ma prawo w dowolnym momencie wnieść sprzeciw wobec przetwarzania dotyczących jej danych osobowych na potrzeby takiego marketingu, w tym profilowania, w zakresie, w jakim przetwarzanie jest związane z takim marketingiem bezpośrednim.

6.12.3. Jeżeli osoba, której dane dotyczą, wniesie sprzeciw wobec przetwarzania do celów marketingu bezpośredniego, danych osobowych Bankowi nie wolno już przetwarzać danych do takich celów.

6.12.4. Najpóźniej przy okazji pierwszej komunikacji z osobą, której dane dotyczą, wyraźnie informuje się ją o prawie do sprzeciwu oraz przedstawia się je jasno i odrębnie od wszelkich innych informacji.

6.12.5. Szczegółowe kwestie związane z uregulowaniem procesu realizacji prawa do sprzeciwu znajdują się w innych regulacjach wewnętrznych Banku.

6.12.6. Jeżeli w związku z realizacją procesów w zakresie praw podmiotów danych przez Bank pojawią się jakiekolwiek pytania lub wątpliwości konieczne jest skontaktowanie się z Inspektorem Ochrony Danych.

7. Okres retencji danych osobowych przetwarzanych przez Bank

7.1.1. Bank działając zgodnie z art. 5 ust. 1 pkt. e RODO przechowuje dane w formie umożliwiającej identyfikację osoby, której dane dotyczą, przez okres nie dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.

7.1.2. Dane osobowe można przechowywać przez okres dłuższy, o ile będą one przetwarzane wyłącznie do celów archiwalnych w interesie publicznym, do celów badań naukowych lub historycznych lub do celów statystycznych na mocy art. 89 ust. 1 RODO.

7.1.3. Po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, o których mowa w 7.1.1, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba, że ich dalsze przechowywanie znajduje podstawę prawną (np. w ustawie z dnia 29 września 1994 r. o rachunkowości, ustawie z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, ustawie z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawie z dnia 24 listopada 2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystywaniu sektora finansowego do wyłudzeń skarbowych).

7.1.4. Usunięcie danych osobowych osób, których dane dotyczą następuje np. poprzez ich zniszczenie lub anonimizację.

7.1.5. Procedura w zakresie okresu retencji dla danych osobowych przetwarzanych w procesach Banku znajduje się do wglądu u Inspektora Ochrony Danych.

8. Zautomatyzowane podejmowanie decyzji i profilowanie

8.1.1. Profilowanie jest metodą (sposobem) przetwarzania danych osobowych. Może być ono oparte o różne modele i algorytmy.

8.1.2. Profilowanie opiera się na odpowiednich matematycznych lub statystycznych procedurach profilowania, z zachowaniem środków technicznych i organizacyjnych zapewniających zmniejszenie ryzyka błędów w procedurach profilowania.

8.1.3. Bank profiluje Klientów między innymi w celach:

i. przeprowadzenia analizy lub prognozy aspektów dotyczących oceny zdolności i wiarygodności kredytowej osoby fizycznej m.in. poprzez przypisanie jej określonej oceny punktowej (tzw. scoring);
ii. realizacji Rekomendacji T KNF dotyczącej dobrych praktyk w zakresie zarządzania ryzykiem detalicznych ekspozycji kredytowych (w szczególności rekomendacji 6, 10 i 12) poprzez korzystanie z modeli statystycznych, m.in. z modeli scoringowych opracowanych i oferowanych przez rejestry kredytowe, w celu oceny zdolności oceny kredytowej wnioskującej osoby fizycznej;
iii. podjęcia decyzji kredytowej, w tym przygotowania oceny zdolności kredytowej, w celu: ustalenia kwoty kredytu/limitu kredytowego dla których Klient, przy uwzględnieniu uzyskiwanych dochodów oraz obsłudze dotychczasowych zobowiązań, posiada możliwość spłaty;
iv. przeciwdziałania praniu pieniędzy, w tym w celu budowania modeli umożliwiających identyfikację działań przestępczych;
v. zapobiegania przestępstwom dokonywanym na szkodę banków, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w ustawie o

kredycie konsumenckim, i ich Klientów - czyli tzw. „fraudom", w tym w celu budowania modeli umożliwiających identyfikację działań przestępczych;

vi. przeciwdziałania nieuczciwej sprzedaży produktów finansowych tzw. missellingowi (w rozumieniu art. 24 ust. 2 pkt 4 ustawy z dnia 16 lutego 2007 r. o ochronie konkurencji i konsumentów), gdyż zakaz misselingu odnosi się do wszystkich produktów i usług bankowych;

vii. segmentacji klientów, w celu przypisania ich do określonych grup dochodowych, marketingowych; jak również tworzenia grup klientów, aby na ich podstawie dopasowywać do nich działania banku np. w zakresie: usług, kosztów, kanałów obsługi, procesów komunikacyjno-sprzedażowych;

viii. świadczenia marketingu bezpośredniego produktów i usług własnych, w celu przygotowywania i rozsyłania spersonalizowanych ofert bankowych np. zdarzeniowych; eksperckich, real time marketing (RTM); ustalania skłonności do zakupów produktów lub usług – w tym budowa i wykorzystanie w komunikacji modeli propensity to buy;

ix. świadczenia marketingu podmiotów z Grupy w celu przygotowania i rozsyłania spersonalizowanych ofert zdarzeniowych; eksperckich, RTM; ustalania skłonności do zakupu produktu i/lub usługi – w tym budowanie i wykorzystanie w komunikacji modeli propensity to buy;

x. świadczenia marketingu podmiotów trzecich, w celu przygotowania i rozsyłania spersonalizowanych ofert: zdarzeniowych; eksperckich, RTM; ustalanie skłonności do zakupu produktu i/lub usługi– w tym budowa i wykorzystanie w komunikacji modeli propensity to buy;

xi. dostosowania komunikacji kierowanej do klientów, w celu ustalania preferowanego kanału kontaktu; treści komunikatów, godziny kontaktu, potencjału dla danej akcji komunikacyjnej; wykorzystanie w komunikacji spersonalizowanej informacji uzyskanych w wyniku wymaganych prawem profilowań – jak np. MIFID II;

xii. świadczenia usługi serwisu bankowości elektronicznej i aplikacji mobilnej, których działanie w znaczącej funkcjonalności oparte jest o profilowanie danych (m.in. kategoryzacja płatności klienta; wysyłanie podpowiedzi do klienta w zakresie przewidywanych przyszłych płatności na podstawie dotychczas wykonywanych operacji na rachunku – w tym wykorzystanie algorytmów detekcji; podpowiedzi i sugestie dotyczące zarządzania majątkiem, korzystania z usług itd.);

xiii. badania poziomu wiedzy klientów o inwestowaniu w instrumenty finansowe oraz doświadczenie inwestycyjne niezbędne do oceny, czy dana usługa maklerska jest odpowiednia dla klienta.

8.1.4. Ocena punktowa klienta lub inny profil będący wynikiem profilowania przez Bank w oparciu o modele własne Banku, może być wykorzystywana przez Bank do podjęcia w stosunku do klienta określonych działań, w których istotnym elementem jest proces oceny zdolności i wiarygodności kredytowej klienta, przykładowo:

i. podjęcie decyzji kredytowej;

ii. monitorowanie spłaty przez klienta zobowiązania kredytowego;

iii. dokonanie przez Bank wstępnej weryfikacji potencjalnych klientów pod kątem możliwości zaproszenia ich do negocjacji w zakresie nabycia określonych produktów Banku;

iv. przygotowanie przez Bank z własnej inicjatywy oferty określonego produktu dla klienta lub warunków przedłużenia produktu, z którego klient korzysta, np. bank dokonuje weryfikacji przyznanego klientowi limitu zadłużenia w karcie kredytowej, przed wydaniem nowej karty kredytowej na kolejny okres.

8.1.5. Bank stosuje dobre praktyki rynku bankowego odnośnie konstrukcji i zarządzania modelami statystycznymi, którego ramy wyznaczone są przez m.in. Rekomendację W KNF dotyczącą zarządzania ryzykiem modeli w bankach.

8.1.6. Bank w ramach swojej działalności podejmuje zautomatyzowane decyzję w związku z:

I. oceną zdolności kredytowej klienta

II. oceną ryzyka kredytowego klienta

8.1.7. Zindywidualizowane oferty marketingowe kierowane do klientów Banku będące wynikiem profilowania, co do zasady nie są zautomatyzowanymi decyzjami, w zakresie w jakim nie wywołują wobec klienta skutków prawnych lub w inny istotny sposób nie wpływają na sytuację klienta.

9. Powierzenie przez Bank przetwarzania danych osobowych.

9.1. Bank może powierzyć innemu podmiotowi, w drodze umowy zawartej na piśmie, przetwarzanie danych oraz przetwarzać dane na zlecenie innego podmiotu.

9.2. Powierzenie przetwarzania danych przez Bank następuje w szczególności w przypadkach umów outsourcingowych, których wykonanie wymaga przetwarzania przez insourcera danych osobowych w imieniu i na rzecz Banku, a także w przypadkach udostępniania przez Bank danych osobowych osób zatrudnionych w Banku podmiotom trzecim, takim jak centra medyczne świadczące usługi zdrowotne na rzecz pracowników i firmy oferujące pozapłacowe świadczenia pracownicze.

9.3. Bank powierzając przetwarzanie danych osobowych korzysta z usług takich dostawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi RODO i chroniło prawa osób, których dotyczą. Bank wybierając podmiot przetwarzający dane zwracają uwagę na standardy bezpieczeństwa przez niego stosowane lub też wyznaczają wymagany przez siebie standard (np. za pomocą audytów czy innych form sprawdzenia).

9.4. Powierzenie przetwarzania odbywa się na podstawie umowy lub innego instrumentu prawnego, które podlegają prawu Unii Europejskiej lub prawu państwa członkowskiego, a zasady, na których podstawie następuje powierzenie wyczerpują wymagania zawarte w art. 28 RODO.

9.5. Bank stosuje jednolity wzór postanowień o powierzeniu przetwarzania danych osobowych, według wzoru znajdującego się do wglądu u Inspektora Ochrony Danych Banku.

9.6. Osoby zatrudnione przez podmiot wykonujący umowę na rzecz Banku i osoby, za których pośrednictwem podmiot ten wykonuje czynności w ramach tej umowy, mogą zostać zobowiązane przez komórkę organizacyjną Banku odpowiedzialną za zawarcie umowy, do złożenia oświadczenia o zachowaniu poufności.

9.7. Treść oświadczenia o zachowaniu poufności jest dostępna do wglądu u Inspektora Ochrony Danych Banku.

9.8. Jeżeli pojawią się jakiekolwiek pytania lub wątpliwości dotyczące powierzenia przetwarzania danych konieczne jest skontaktowanie się z Inspektorem Ochrony Danych.

10. Postępowanie w przypadku naruszenia ochrony danych osobowych

10.1. Zgodnie z RODO naruszeniem ochrony danych osobowych, wymagającym zawiadomienia PUODO jest 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.

10.2. W przypadku naruszenia ochrony danych osobowych, Bank bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia – zgłasza je PUODO, chyba że jest mało prawdopodobne, by naruszenie to skutkowało ryzykiem naruszenia praw lub wolności osób fizycznych.

10.3. Do zgłoszenia przekazanego organowi nadzorczemu po upływie 72 godzin dołącza się wyjaśnienie przyczyn opóźnienia.

10.4. Zgłoszenie, o którym mowa powyżej, musi co najmniej:

i. opisywać charakter naruszenia ochrony danych osobowych, w tym w miarę możliwości wskazywać kategorie i przybliżoną liczbę osób, których dane dotyczą, oraz kategorie i przybliżoną liczbę wpisów danych osobowych, których dotyczy naruszenie;
ii. zawierać imię i nazwisko oraz dane kontaktowe inspektora ochrony danych lub oznaczenie innego punktu kontaktowego, od którego można uzyskać więcej informacji;
iii. opisywać możliwe konsekwencje naruszenia ochrony danych osobowych;
iv. opisywać środki zastosowane lub proponowane przez administratora w celu zaradzenia naruszeniu ochrony danych osobowych, w tym w stosownych przypadkach środki w celu zminimalizowania jego ewentualnych negatywnych skutków.

10.5. Jeżeli – i w zakresie, w jakim – informacji nie da się udzielić w tym samym czasie, można je udzielać sukcesywnie bez zbędnej zwłoki.

10.6. Bank dokumentuje wszelkie naruszenia ochrony danych osobowych, w tym okoliczności naruszenia ochrony danych osobowych, jego skutki oraz podjęte działania zaradcze. Dokumentacja ta musi pozwolić PUODO weryfikowanie przestrzegania artykułu 33 RODO.

10.7. Dokumentacja naruszeń ochrony danych osobowych jest prowadzona przez Inspektora Ochrony Danych.

10.8. Szczegółowe regulacje dotyczące postępowania w razie stwierdzenia naruszenia bezpieczeństwa danych osobowych zawarte są w innych regulacjach wewnętrznych Banku dostępnych u Inspektora Ochrony Danych.

11. Przetwarzanie danych osobowych osób zatrudnionych w Banku

11.1. Przetwarzanie danych osobowych pracowników Banku opiera się na ogólnych zasadach wskazanych w RODO i niniejszej Polityce.

11.2. Z uwagi na specyfikę przetwarzania danych osobowych pracowników Bank przygotował i wdrożył następujące procedury regulujące kwestie przetwarzania danych osobowych pracowników:

i. Zasady przechowywania danych osobowych w Obszarze Zarządzania Zasobami Ludzkimi Banku BGŻ BNP Paribas S.A.;

ii. Zasady obsługi praw podmiotów, których dane osobowe są przetwarzane w Obszarze Zarządzania Zasobami Ludzkimi Banku BGŻ BNP Paribas S.A.

12. Wymogi wobec systemu informatycznego / aplikacji służących do przetwarzania danych osobowych w Banku

12.1. Bank przetwarza dane osobowe w systemie informatycznym rozumianym jako zespół współpracujących ze sobą urządzeń, programów, procedur przetwarzania informacji i narzędzi programowych zastosowanych w celu przetwarzania danych. W szczególności są to:

i. urządzenia bezpośrednio przetwarzające dane (komputery, serwery);
ii. urządzenia służące zapewnieniu komunikacji (sieci teleinformatyczne);
iii. urządzenia magazynujące dane (macierze, biblioteki taśmowe);
iv. oprogramowanie (aplikacje, systemy operacyjne).

12.2. Zgodnie z art. 32 RODO uwzględniając stan wiedzy technicznej, koszt wdrażania oraz charakter, zakres, kontekst i cele przetwarzania oraz ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia, Bank wdrożył odpowiednie środki techniczne i organizacyjne, aby zapewnić stopień bezpieczeństwa odpowiadający temu ryzyku, w tym między innymi:

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

12.3. Przy wprowadzaniu środków technicznych i organizacyjnych Bank uwzględnił/uwzględnia w szczególności ryzyko wiążące się z przetwarzaniem danych osobowych, w szczególności wynikające z przypadkowego lub niezgodnego z prawem zniszczenia, utraty, modyfikacji, nieuprawnionego ujawnienia lub nieuprawnionego dostępu do danych osobowych przesyłanych, przechowywanych lub w inny sposób przetwarzanych.

12.4. System informatyczny stosowany w Banku posiada funkcjonalności umożliwiające mu realizację praw podmiotów danych wskazanych w rozdziale III RODO.

12.5. System informatyczny musi zapewniać możliwość odnotowania zgody (a także jej odwołania) osoby której dane dotyczą.

12.6. System informatyczny służący do przetwarzania danych osobowych musi być zabezpieczony:

i. przed działaniem oprogramowania, którego celem jest uzyskanie nieuprawnionego dostępu do systemu informatycznego oraz przed utratą danych spowodowaną awarią zasilania lub zakłóceniami w sieci zasilającej;
ii. przed zagrożeniami pochodzącymi z sieci publicznej poprzez wdrożenie fizycznych lub logicznych (kontrolę przepływu informacji pomiędzy systemem informatycznym administratora danych a siecią publiczną oraz kontrolę działań inicjowanych z sieci publicznej i systemu informatycznego administratora danych) zabezpieczeń chroniących przed nieuprawnionym dostępem.

12.7. Ocenie, w kontekście przepisów RODO, podlegają wyłącznie systemy i aplikacje, w których przetwarzane są dane osób fizycznych oraz osób prowadzących jednoosobową działalność gospodarczą. Przepisów RODO nie stosuje się bowiem do:

i. aplikacji służących wyłącznie do przetwarzania danych osób prawnych i jednostek organizacyjnych nieposiadających osobowości prawnej;
ii. aplikacji, w których nie przetwarza się danych identyfikujących osoby.

12.8. Każdy użytkownik systemu informatycznego służącego do przetwarzania danych musi posiadać odrębny identyfikator, a dostęp do danych musi być uzależniony od wprowadzenia identyfikatora i dokonania uwierzytelnienia za pomocą hasła, które musi składać się co najmniej z 8 znaków, zawierać małe i wielkie litery oraz cyfry lub znaki specjalne, a ponadto podlega zmianie nie rzadziej niż co 30 dni.

12.9. Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie. W systemie informatycznym należy stosować środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej.

12.10. Dane osobowe przetwarzane w systemie informatycznym muszą być zabezpieczone przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych. Kopie zapasowe muszą być przechowywane w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem oraz podlegają usunięciu niezwłocznie po ustaniu ich użyteczności.

12.11. Zgodnie z wytycznymi grupy kapitałowej Bank wdrożył proces mający na celu ocenę zgodności wszelkich systemów informatycznych w ramach, których dochodzi do przetwarzania danych osobowych z wymogami ochrony danych osobowych. Ocena zgodności przeprowadzana jest za pomocą dedykowanego formularza przeznaczonego do oceny narzędzia.

12.12. Więcej informacji na temat odpowiednich środków technicznych i organizacyjnych znajduje się w innych regulacjach wewnętrznych Banku dostępnych do wglądu u Inspektora Ochrony Danych.