Kodeks dobrych praktyk

w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe

WPROWADZENIE

1. Kodeks dobrych praktyk w zakresie przetwarzania danych osobowych przez banki i rejestry kredytowe (dalej „Kodeks”) stanowi zbiór zasad postępowania w zakresie ochrony danych osobowych w polskim sektorze bankowym.
2. Kodeks stanowi doprecyzowanie zasad przetwarzania i ochrony danych osobowych określonych w Rozporządzeniu 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 osobowych) z uwzględnieniem specyfiki sektora bankowego.
3. Kodeks stanowi kodeks postępowania, o którym mowa w art. 40 Rozporządzenia.

1. Kodeks ma zastosowanie do banków krajowych oraz rejestrów kredytowych działających na terytorium Rzeczpospolitej Polskiej, będących członkami Związku Banków Polskich.
2. Banki i rejestry kredytowe przetwarzają dane osobowe w związku z prowadzeniem swojej działalności zgodnie z przepisami Prawa bankowego oraz innych właściwych ustaw oraz w zakresie działalności wynikającej ze swoich statutów z uwzględnieniem wytycznych i rekomendacji Komisji Nadzoru Finansowego oraz innych właściwych regulatorów.
3. Do stosowania Kodeksu mogą przystąpić inne podmioty niż wskazane w ust. 4 niniejszego Wprowadzenia, na zasadach określonych w ust. 9 Wprowadzenia, w tym podmioty świadczące na rzecz tych instytucji usługi wymagające przetwarzania danych osobowych, jednakże wyłącznie w zakresie świadczenia takich usług na rzecz banków i rejestrów kredytowych.
4. Kodeks będzie miał zastosowanie do przetwarzania danych osobowych Klientów, w tym osób, których dane są przetwarzane przez rejestry kredytowe w związku z realizacją przez te rejestry obowiązków i uprawnień wskazanych we właściwych przepisach prawa oraz w aktach wewnętrznych.
5. Kodeks nie ma zastosowania do przetwarzania danych osobowych pracowników, współpracowników oraz kandydatów do pracy w bankach i rejestrach kredytowych.
6. Podmioty, o których mowa w ust. 6 niniejszego Wprowadzenia, przystępując do stosowania Kodeksu zobowiązują się do stosowania wszystkich zasad wyrażonych w Kodeksie. W celu przystąpienia do stosowania Kodeksu, właściwy podmiot złoży do Związku Banków Polskich pisemne oświadczenie zawierające zobowiązanie do przestrzegania jego zasad.

10. Wprowadzenie Kodeksu ma na celu:

(a) wsparcie banków i rejestrów kredytowych we właściwym stosowaniu Rozporządzenia z uwzględnieniem cech przetwarzania danych osobowych w sektorze bankowym i szczególnych potrzeb banków i rejestrów kredytowych,

(b) dopasowanie obowiązków banków i rejestrów kredytowych oraz podmiotów przetwarzających do wymogów odnoszących się do ryzyka naruszenia praw i wolności osób fizycznych, jakie może nieść przetwarzanie ich danych osobowych,

(c) ograniczanie ryzyka naruszenia praw i wolności osób fizycznych, jakie może nieść przetwarzanie danych osobowych, poprzez wskazanie obowiązków dla banków i rejestrów kredytowych oraz podmiotów przetwarzających dane osobowe w tym zakresie,

(d) ułatwienie Klientom dokonania oceny, czy dany bank lub rejestr kredytowy stosuje odpowiednie zasady ochrony przetwarzanych danych osobowych,

(e) zwiększenie zaufania Klientów do banków oraz rejestrów kredytowych, że ich dane osobowe są chronione na odpowiednim poziomie.

Spis treści

[A. DEFINICJE I SKRÓTY 4](#_Toc501116029)

[B. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH, PODSTAWY PRAWNE PRZETWARZANIA DANYCH I WARUNKI POZYSKIWANIA ZGODY 5](#_Toc501116030)

[I. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH 5](#_Toc501116031)

[II. PODSTAWY PRAWNE PRZETWARZANIA DANYCH 7](#_Toc501116032)

[III. WARUNKI POZYSKIWANIA ZGODY 8](#_Toc501116033)

[C. PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ 10](#_Toc501116034)

[I. ZASADY OGÓLNE 10](#_Toc501116035)

[II. OBOWIĄZEK INFORMACYJNY 13](#_Toc501116036)

[III. PRAWO DOSTĘPU DO DANYCH OSOBY, KTÓREJ DANE DOTYCZĄ 15](#_Toc501116037)

[IV. PRAWO DO SPROSTOWANIA DANYCH 16](#_Toc501116038)

[V. PRAWO DO USUNIĘCIA DANYCH (PRAWO DO BYCIA ZAPOMNIANYM) 17](#_Toc501116039)

[VI. PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH 18](#_Toc501116040)

[VII. OBOWIĄZEK POWIADOMIENIA O SPROSTOWANIU LUB USUNIĘCIU DANYCH OSOBOWYCH LUB O OGRANICZENIU PRZETWARZANIA 19](#_Toc501116041)

[VIII. PRAWO DO PRZENOSZENIA DANYCH 19](#_Toc501116042)

[VIII.a Zasady ogólne 19](#_Toc501116043)

[VIII.b Prawo do otrzymywania danych 21](#_Toc501116044)

[VIII.c Prawo do żądania do przesłania danych innemu administratorowi 21](#_Toc501116045)

[IX. PRAWO SPRZECIWU 22](#_Toc501116046)

[D. PRZECHOWYWANIE I USUWANIE DANYCH OSOBOWYCH 23](#_Toc501116047)

[E. PROFILOWANIE ORAZ ZAUTOMATYZOWANE PRZETWARZANIE DANYCH OSOBOWYCH OSÓB FIZYCZNYCH 24](#_Toc501116048)

[F. POWIERZENIE PRZETWARZANIA - KLAUZULE UMÓW Z DOSTAWCAMI 27](#_Toc501116049)

[G. POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH 28](#_Toc501116050)

[H. OCENA SKUTKÓW PRZETWARZANIA DANYCH 30](#_Toc501116051)

[Załączniki do Kodeksu 31](#_Toc501116052)

[Załącznik nr 1 - Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego 32](#_Toc501116053)

[Załącznik nr 2 - Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą 33](#_Toc501116054)

[Załącznik nr 3 – Opis przykładowego modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym 34](#_Toc501116055)

[Załącznik nr 4 - Zakresy informacji przekazywanych Klientowi 37](#_Toc501116056)

[Załącznik nr 5 - Przykładowe postanowienia umów zawieranych z podmiotami przetwarzającymi 47](#_Toc501116057)

[Załącznik nr 6 – Przykłady zautomatyzowanego przetwarzania danych 49](#_Toc501116058)

[Zautomatyzowane przetwarzanie danych osobowych na poziomie wybranego portfela kredytowego lub całego portfela banku w celu dostarczenia analiz statystycznych bankom i innym instytucjom odpowiedzialnym za zapewnienie stabilności finansowej 49](#_Toc501116059)

[Zautomatyzowane przetwarzanie danych osobowych w celu budowy modelu oceny punktowej (scoringowego) rejestru kredytowego 50](#_Toc501116060)

[Zautomatyzowane przetwarzanie danych osobowych w celu stosowania przez banki metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Rozporządzenie 575/2013). 51](#_Toc501116061)

# DEFINICJE I SKRÓTY

Pojęcia użyte w niniejszym Kodeksie mają następujące znaczenie:

1. **Prawo Bankowe -** ustawa z dnia 29 sierpnia 1997 r. Prawo bankowe (t.j. Dz.U. z 2016 r. poz. 1988 z późn. zm.).
2. **Rozporządzenie lub RODO** **-** Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych).
3. **Ustawa o ochronie danych osobowych –** ustawa z dnia \_\_\_\_\_\_\_\_ o ochronie danych osobowych (t.j. Dz.U. z \_\_\_\_\_\_\_ r. poz. \_\_\_ z późn. zm.).
4. **Administrator -** oznacza osobę fizyczną lub prawną, organ publiczny, jednostkę lub inny podmiot, który samodzielnie lub wspólnie z innymi ustala cele i sposoby przetwarzania danych osobowych; jeżeli cele i sposoby takiego przetwarzania są określone w prawie Unii lub w prawie państwa członkowskiego, to również w prawie Unii lub w prawie państwa członkowskiego może zostać wyznaczony administrator lub mogą zostać określone konkretne kryteria jego wyznaczania.
5. **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.
6. **Profilowanie** **-** oznacza dowolną formę zautomatyzowanego przetwarzania danych osobowych, które polega na wykorzystaniu danych osobowych do oceny niektórych czynników osobowych osoby fizycznej, w szczególności do analizy lub prognozy aspektów dotyczących efektów pracy tej osoby fizycznej, jej sytuacji ekonomicznej, zdrowia, osobistych preferencji, zainteresowań, wiarygodności, zachowania, lokalizacji lub przemieszczania się.
7. **Pseudonimizacja -** oznacza przetworzenie danych osobowych w taki sposób, by nie można ich było już przypisać konkretnej osobie, której dane dotyczą, bez użycia dodatkowych informacji, pod warunkiem że takie dodatkowe informacje są przechowywane osobno i są objęte środkami technicznymi i organizacyjnymi uniemożliwiającymi ich przypisanie zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej.
8. **Rejestr kredytowy** **-** oznacza instytucję utworzoną na podstawie art. 105 ust. 4 Prawa bankowego.
9. **Zgoda** **-** oznacza dobrowolne, konkretne, świadome i jednoznaczne okazanie woli, którym osoba, której dane dotyczą, w formie oświadczenia lub wyraźnego działania potwierdzającego, przyzwala na przetwarzanie dotyczących jej danych osobowych.
10. **Organ nadzorczy** **-** oznacza niezależny organ publiczny na terytorium Rzeczpospolitej Polskiej właściwy do wypełniania zadań i wykonywania uprawnień powierzonych mu zgodnie z Rozporządzeniem.
11. **Klient -** oznacza potencjalnego, aktualnego lub byłego:

a) klienta banku oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez banki niebędącą klientem banku lub osobę, której dane osobowe bank przetwarza w związku z prowadzeniem przez bank działalności obejmujących czynności bankowe oraz w związku z realizacją przez bank obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do banków oraz w aktach wewnętrznych banków, takich w szczególności jak statuty (Klient banku);

b) klienta rejestru kredytowego oraz jego przedstawicieli, osobę korzystającą z usług świadczonych przez rejestr kredytowy niebędącą klientem rejestru kredytowego lub osobę, której dane osobowe rejestr kredytowy przetwarza w związku z prowadzeniem przez rejestr kredytowy działalności oraz w związku z realizacją przez rejestr kredytowy obowiązków i uprawnień wskazanych we właściwych przepisach prawa, mających zastosowanie do rejestrów kredytowych (Klient rejestru kredytowego).

1. **Grupa** **-** oznacza osobę prawną lub jednostkę organizacyjną nieposiadającą osobowości prawnej powiązaną organizacyjnie lub ekonomicznie z bankiem lub rejestrem kredytowym.

Inne pojęcia użyte w niniejszym Kodeksie bez nadania im odrębnej definicji, mają znaczenie jakie zostało im nadane w przepisach Rozporządzenia.

# ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH, PODSTAWY PRAWNE PRZETWARZANIA DANYCH I WARUNKI POZYSKIWANIA ZGODY

1. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

**1. Zasada zgodności z prawem, rzetelności i przejrzystości**

Banki oraz rejestry kredytowe zapewniają realizację zasady o której mowa w art. 5 ust. 1 lit a) Rozporządzenia, dotyczącej przetwarzania danych zgodnie z prawem, rzetelnie i w sposób przejrzysty, poprzez zapewnienie podstaw prawnych przetwarzania oraz realizację praw Klientów obejmujących w szczególności informowanie Klientów o przetwarzaniu ich danych zgodnie z wymogami Rozporządzenia. W tym celu banki oraz rejestry kredytowe w oparciu o swoje wewnętrzne procesy zapewniają realizację tych zasad.

**2. Zasada ograniczenia celu przetwarzania**

Banki oraz rejestry kredytowe zapewniają realizację zasady zbierania danych wyłącznie w konkretnych, wyraźnych i prawnie uzasadnionych celach i nieprzetwarzanie ich dalej w sposób niezgodny z tymi celami, tj. zasady, o której mowa w art. 5 ust. 1 lit b) Rozporządzenia. W tym celu banki oraz rejestry kredytowe w ramach swoich wewnętrznych procesów zapewniają realizację tych zasad, zapewniając w szczególności odpowiedni nadzór w tym zakresie, uwzględniając role i zadania inspektora ochrony danych.

**3. Zasada minimalizacji danych**

Banki oraz rejestry kredytowe zapewniają realizację zasady minimalizacji danych, o której mowa w art. 5 ust. 1 lit c) Rozporządzenia, poprzez przetwarzanie danych adekwatnych, stosownych oraz ograniczonych do celów przetwarzania. W tym celu banki oraz rejestry kredytowe realizują wewnętrzne procesy zapewniające realizację tej zasady, w tym w szczególności zapewniają, że wymagania w zakresie minimalizacji danych uwzględniane są w procesach tworzenia nowych i modyfikacji już istniejących produktów, procesów i systemów w ramach dokonywania identyfikacji zagrożeń związanych z ryzykiem operacyjnym.

**4. Zasada prawidłowości**

Banki oraz rejestry kredytowe zapewniają realizację zasady, o której mowa w art. 5 ust. 1 lit. d) Rozporządzenia, zgodnie z którą dane powinny być prawidłowe i w razie potrzeby uaktualniane. Banki oraz rejestry kredytowe będą podejmować wszelkie rozsądne działania, aby dane osobowe, które są nieprawidłowe w świetle celów ich przetwarzania, zostały niezwłocznie usunięte lub sprostowane. W tym celu banki oraz rejestry kredytowe w ramach swoich wewnętrznych procedur zapewniają realizację tej zasady, w tym w szczególności zasady zarządzania danymi wykorzystywanymi w ramach prowadzonej działalności, obejmujące w szczególności zarządzanie architekturą oraz jakością danych, uwzględniających okresowe dokonywanie oceny jakości danych, dokonywanie czyszczenia danych, identyfikację przyczyn błędów występujących w danych i bieżące monitorowanie jakości danych.

**5. Zasada ograniczenia przechowywania**

Banki oraz rejestry kredytowe zapewniają realizację zasady, o której mowa w art. 5 ust. 1 lit. e) Rozporządzenia, zgodnie z którą dane powinny być 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. W tym celu banki oraz rejestry kredytowe w ramach swoich wewnętrznych procesów zapewniają realizację tej zasady oraz zapewniają, aby efektywność i poprawność działania mechanizmów kontrolnych w tym zakresie w szczególności uwzględniała role i zadania inspektora ochrony danych.

**6. Zasada integralności i poufności**

Banki oraz rejestry kredytowe zapewniają integralność i poufność danych określoną w art. 5 ust. 1 lit. f) Rozporządzenia poprzez odpowiednie zapewnienie bezpieczeństwa danych osobowych, w tym zapewnienie ochrony przed niedozwolonym lub niezgodnym z prawem przetwarzaniem oraz przypadkową utratą, zniszczeniem lub uszkodzeniem za pomocą odpowiednich środków technicznych i organizacyjnych. Banki stosują w tym zakresie zasady wynikające z rekomendacji Komisji Nadzoru Finansowego, w tym w szczególności Rekomendacji D Komisji Nadzoru Finansowego dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

**7. Zasada rozliczalności**

Banki oraz rejestry kredytowe zapewniają realizację zasady rozliczalności, o której mowa w art. 5 ust. 2 Rozporządzenia, poprzez wdrożenie odpowiednich procedur i zasad, pozwalających bankom oraz rejestrom kredytowym na wykazanie przestrzegania przepisów Rozporządzenia, ze szczególnym uwzględnieniem udziału w tych działaniach inspektora ochrony danych.

1. PODSTAWY PRAWNE PRZETWARZANIA DANYCH

Bank lub rejestr kredytowy przetwarza dane osobowe, jeśli spełniony jest co najmniej jeden z poniższych warunków:

a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów;

b) 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;

c) przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na banku lub rejestrze kredytowym;

d) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej;

e) przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej bankowi lub rejestrowi kredytowemu;

f) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez bank, rejestr kredytowy 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.

1. WARUNKI POZYSKIWANIA ZGODY
2. 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.
3. 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 lub rejestr kredytowy danych w tym celu/celach.
4. Zapytanie o zgodę musi być wyrażone w zrozumiałej, łatwo dostępnej formie, jasnym i prostym językiem, a dodatkowo w przypadku zapytań elektronicznych – w zwięzłej formie i nie może niepotrzebnie zakłócać korzystania z usługi, której dotyczy.
5. Zgoda w formie oświadczenia woli powinna być wyrażona w zrozumiałej i łatwo dostępnej formie oraz sformułowana jasnym i prostym językiem, a także stanowić odrębną deklarację. Dopuszcza się włączenie klauzuli zgody do umowy lub wniosku o zawarcie umowy, z zastrzeżeniem umożliwienia osobie złożenia odrębnego podpisu lub zaznaczenia okienek wyboru na umowie.

Oświadczenie woli może być wyrażone w dowolnej formie (ustnej, dokumentowej, pisemnej lub elektronicznej), w tym m.in. poprzez zaznaczenie okienek wyboru na formularzu lub w systemie informatycznym, przy których wskazane są klauzule zgód, złożenie przez osobę podpisu na dokumencie tradycyjnym pod oświadczeniem woli, złożeniem podpisu elektronicznego na dokumencie elektronicznym z oświadczeniem woli, oświadczenie o wyrażeniu zgody przesłane drogą elektroniczną, np. e-mailem, contact center (call center).

1. Do wyraźnych działań wskazujących na wyrażenie zgody 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 lub rejestr kredytowy 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.
2. Jedna zgoda Klienta może obejmować wiele podobnych celów, w szczególności w następujących sytuacjach:
3. przetwarzania danych osobowych w celach marketingu bezpośredniego banku oraz marketingu bezpośredniego podmiotów z Grupy w ramach oferowania danego produktu;
4. udostępnienia danych osobowych w celu sprawdzenia Klienta w zewnętrznych bazach danych innych niż rejestry kredytowe, np. u różnych podmiotów z grupy kapitałowej, biurach informacji gospodarczej.
5. Jedna zgoda Klienta może obejmować wiele podobnych celów także w sytuacji, gdy opiera się ona na podstawie różnych reżimów prawnych, jeżeli dotyczy wspólnego produktu, na przykład w sytuacji udostępnienia danych osobowych stanowiących jednocześnie udostępnienie danych objętych tajemnicą bankową.
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.
7. Zgody nie uważa się za wyrażoną świadomie lub dobrowolnie, m.in. jeśli:
8. od wyrażenia przez osobę zgody uzależnione jest wykonanie umowy, w tym świadczenie usług, a do wykonania tej umowy zgoda nie jest niezbędna;
9. 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;
10. 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.
11. Bank lub rejestr kredytowy powinien umożliwić osobie, która wyraziła zgodę, wycofanie tej zgody w dowolnym momencie oraz w sposób równie łatwy, jak jej wyrażenie. Nie oznacza to jednak, że wycofanie zgody musi nastąpić dokładnie w taki sam sposób jak jej wyrażenie. Odwołanie zgody może nastąpić m.in. poprzez ustne lub pisemne lub elektroniczne oświadczenie woli osoby, która zgodę wyraziła, wybór ustawień technicznych systemu informatycznego lub zaznaczenie albo odznaczenie odpowiednich okienek wyboru na formularzu lub w systemie informatycznym.
12. Bank lub rejestr kredytowy zbierając zgodę od osoby lub oświadczenie o wycofaniu zgody, powinien upewnić się, że osoba wyrażająca/wycofująca zgodę jest w rzeczywistości osobą, której dane dotyczą.
13. Bank lub rejestr kredytowy zapewnia rozliczalność w zakresie przetwarzania danych na podstawie zgody, w szczególności zebranie oświadczeń zgód, rejestrację rozmów telefonicznych, backup’y/zrzuty z ekranu systemu informatycznego, jak również zatwierdzone procedury wewnętrzne banku lub rejestru kredytowego lub skrypty rozmów z Klientami.

# PRAWA OSOBY, KTÓREJ DANE DOTYCZĄ

# ZASADY OGÓLNE

1. Banki i rejestry kredytowe realizują prawa osób, których dane dotyczą, w tym:
   * + 1. prawo do informacji (obowiązek informacyjny);
       2. prawo dostępu do danych lub otrzymania kopii danych;
       3. prawo do sprostowania danych;
       4. prawo do usunięcia danych;
       5. prawo do ograniczenia przetwarzania;
       6. prawo do przenoszenia danych;
       7. prawo do sprzeciwu.
2. Postanowienia niniejszego Rozdziału odnoszą się do wszystkich praw wymienionych w Rozdziałach II – IX Części C Kodeksu, o ile przepisy tychże Rozdziałów nie stanowią inaczej.
3. Klient banku lub rejestru kredytowego jest uprawniony do zgłoszenia żądania, o którym mowa w ust. 1 powyżej w formie pisemnej lub elektronicznej na formularzu udostępnionym przez bank lub rejestr kredytowy. Nie wyłącza to uprawnienia Klienta do złożenia żądania w innej akceptowalnej i możliwej do udokumentowania przez bank lub rejestr kredytowy formie. W każdym przypadku żądanie Klienta powinno wskazywać, jakich danych osobowych i czynności dotyczy. W przypadku, gdy żądanie Klienta jest nieprecyzyjne, w tym nie zawiera wskazania zakresu danych osobowych i czynności, jaka objęta jest wnioskiem, bank lub rejestr kredytowy powinien zwrócić się do Klienta o przekazanie takich informacji. W przypadku braku sprecyzowania przez Klienta jakich danych i jakich czynności żądanie dotyczy, bank lub rejestr kredytowy jest uprawniony do wstrzymania realizacji żądania do momentu uzyskania wystarczających informacji od Klienta. Bank lub rejestr kredytowy realizuje żądanie Klienta zgodnie ze swoimi wewnętrznymi procedurami.
4. Realizacja praw osoby, której dane dotyczą, przez bank lub rejestr kredytowy następuje w rozsądnym terminie uwzględniającym koszty, stopień trudności realizacji żądania oraz w oparciu o wewnętrzne procesy banków lub rejestrów kredytowych zapewniające realizację tych zasad.
5. W zakresie realizacji praw osoby, której dane dotyczą, komunikacja z tą osobą powinna odbywać się w zwięzłej, przejrzystej, zrozumiałej i łatwo dostępnej formie, jasnym i prostym językiem, oraz zgodnie z poniższym:
6. bez zbędnej zwłoki, najpóźniej w terminie miesiąca od otrzymania żądania osoby, której dane dotyczą, bank lub rejestr kredytowy udziela informacji o działaniach podjętych w związku z żądaniem osoby;
7. w przypadku konieczności wydłużenia terminu realizacji żądania osoby, której dane dotyczą, najpóźniej w terminie miesiąca od otrzymania żądania bank lub rejestr kredytowy udziela informacji o przedłużeniu terminu rozpatrzenia żądania oraz podaje przyczyny opóźnienia. Wydłużenie terminu może nastąpić z uwagi na skomplikowany charakter żądań lub liczbę żądań, lecz nie więcej niż o dwa miesiące;
8. w przypadku nieuwzględnienia żądania osoby, której dane dotyczą, najpóźniej w ciągu miesiąca od otrzymania żądania osoby, której dane dotyczą, bank lub rejestr kredytowy udziela informacji o odmowie podjęcia działań w związku z żądaniem osoby, powodach niepodjęcia działań, możliwości wniesienia skargi do organu nadzorczego oraz skorzystania ze środków ochrony prawnej przed sądem oraz o ustaniu podstawy do ograniczenia przetwarzania danych Klienta.
9. Bank lub rejestr kredytowy komunikuje się z Klientem w języku polskim. Z zastrzeżeniem ust. 7, w przypadku, jeśli inny język niż polski jest językiem standardowo używanym przez bank w komunikacji z danym Klientem, Bank udzieli odpowiedzi na wniosek Klienta w tym języku.

1. Realizacja wniosku o wydanie kopii danych lub przeniesienie danych następuje w języku, w jakim są one przetwarzane przez bank lub rejestr kredytowy.
2. Informacje mogą zostać udzielone m.in. w sposób pisemny (w formie tradycyjnej lub elektronicznej) lub ustnie, po potwierdzeniu innymi sposobami tożsamości osoby, której dane dotyczą. Jeśli żądanie osoby nastąpiło drogą elektroniczną, w miarę możliwości odpowiedź powinna być przekazana elektronicznie chyba, że osoba zażąda innej formy odpowiedzi. Informacje przekazywane drogą elektroniczną powinny być przekazywane z zastosowaniem zasad bezpieczeństwa.
3. Komunikacja z osobą, której dane dotyczą, oraz podejmowanie działań na żądanie tej osoby, są wolne od opłat, z zastrzeżeniem postanowień ust. 10.

W przypadku ewidentnie nieuzasadnionych lub nadmiernych żądań osoby, której dane dotyczą, w szczególności ze względu na swój ustawiczny charakter, bank, a także rejestr kredytowy może pobrać opłatę w rozsądnej wysokości uwzględniającej koszty sporządzenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań albo odmówić podjęcia działań w związku z żądaniem tej osoby. O wysokości opłat bank lub rejestr kredytowy informuje osobę, której dane dotyczą.

1. Bank lub rejestr kredytowy będzie uprawniony do pobrania opłaty, o której mowa w ust. 9 w sytuacji, gdy żądanie:
2. zostało zgłoszone przed upływem 3 miesięcy od dnia zgłoszenia przez osobę, której dane dotyczą, żądania tego samego rodzaju, przy czym ograniczenie to nie dotyczy prawa do sprostowania danych, prawa do ograniczenia przetwarzania danych ani prawa do sprzeciwu;
3. dotyczy informacji dzielonych na kilka lub kilkanaście żądań;
4. dotyczy wniosku o szczególny nośnik lub format odpowiedzi, jeżeli nie odpowiada on standardowemu formatowi przyjętemu przez bank lub rejestr kredytowy;
5. dotyczy wniosku o udzielenie odpowiedzi w języku innym niż język, który w komunikacji z Klientem składającym wniosek jest standardowo używany przez bank lub rejestr kredytowy;
6. dotyczy wniosku, którego realizacja wymaga znacznego zaangażowania zasobów ludzkich lub środków niezbędnych do prawidłowego wykonania wniosku w stopniu zakłócającym normalną działalność banku lub rejestru kredytowego, np. wniosku o szczegółowe informacje (takie jak wielkość lokaty Klienta w konkretnych dniach, godziny udostępnienia danych osobowych odbiorcom danych, szczegółowa analiza zobowiązań zawartych w informacji pozyskanej z rejestru kredytowego albo raportach kredytowych przekazywanych bankom);
7. ma zostać zrealizowane w szczególnym trybie jak np. odpowiedź przesłana kurierem;
8. składane jest ponownie przed upływem 3 miesięcy po tym, jak uprzednie takie samo żądanie zostało wycofane.
9. Opłata, o której mowa w ust. 9 powyżej będzie uwzględniać administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań, w tym w szczególności koszty kuriera, tłumacza, zakupu i dostosowania nośnika, wykonania nagrania dźwiękowego, przełożenia odpowiedzi na język braille’a.
10. W przypadku, gdy zgodnie z ust. 9 powyżej, bank lub rejestr kredytowy będzie uprawniony do naliczenia opłaty za realizację wniosku Klienta, bank lub rejestr kredytowy rozpocznie realizację wniosku po wpłynięciu na konto banku lub rejestru kredytowego opłaty, o której mowa w ust. 9 powyżej.
11. Bank lub rejestr kredytowy będzie uprawniony do odmowy podjęcia działań w związku z żądaniem Klienta w sytuacji, gdy:
12. żądanie ma zostać zrealizowane w formacie lub na nośniku nieznanym lub niestosowanym przez bank lub rejestr kredytowy;
13. wniosek jest niejasny i Klient składający wniosek, mimo prośby banku lub rejestru kredytowego, nie wyjaśnił niejasności związanych z wnioskiem;
14. tożsamość wnioskodawcy jest nieustalona i mimo prób banku lub rejestru kredytowego, nie udało się potwierdzić tożsamości wnioskującego;
15. Klient nie uiścił opłaty, o której mowa w ust. 9 powyżej;
16. realizacja żądania mogłaby spowodować ujawnienie tajemnicy bankowej lub tajemnicy przedsiębiorstwa banku lub rejestru kredytowego (np. algorytm modelu scoringowego) lub innej tajemnicy prawnie chronionej;
17. po weryfikacji wewnętrznej możliwości technicznej realizacji wniosku, bank lub rejestr kredytowy ustali, że jego realizacja powodowałaby nałożenie na Klienta nieracjonalnie wysokich kosztów;
18. w przypadku wskazanym w ust. 7 – Klient zażąda wydania kopii danych lub przeniesienia danych w języku innym niż język, w jakim dane są przetwarzane przez bank lub rejestr kredytowy.
19. Jeśli bank lub rejestr kredytowy ma wątpliwości co do tożsamości osoby składającej żądanie, może poprosić tę osobę o dodatkowe informacje niezbędne do potwierdzenia jej tożsamości. W przypadku niedostarczenia przez osobę składającą żądanie informacji pozwalających na identyfikację, bank lub rejestr kredytowy pozostawia wniosek bez rozpoznania, pod warunkiem poinformowania osoby składającej żądanie. Jeśli bank lub rejestr kredytowy przetwarza dane osobowe niepozwalające mu na identyfikację osoby, której dane dotyczą, nie ma on obowiązku pozyskania dodatkowych informacji w tym celu z innych źródeł.
20. Czas na realizację żądania, o którym mowa w ust. 3 powyżej, biegnie ponownie od dnia ustalenia tożsamości Klienta, wniesienia opłaty lub złożenia przez Klienta wyjaśnień lub uzupełnienia żądania.
21. OBOWIĄZEK INFORMACYJNY
22. W przypadku zbierania danych osobowych, jak również w przypadku zmiany celów przetwarzania danych osobowych w stosunku do celu, dla których dane osobowe zostały zebrane, banki lub rejestry kredytowe dopełniają obowiązku informacyjnego. Zakres informacji przekazywanych Klientowi zawarty został w Załączniku nr 4 do Kodeksu.

1. W przypadku zbierania danych osobowych bezpośrednio od osoby, której dane dotyczą, informacja jest przekazywana podczas pozyskiwania danych, natomiast w przypadku zbierania danych osobowych nie od osoby, której dane dotyczą:
2. w rozsądnym terminie, nie później jednak niż w ciągu miesiąca od pozyskania danych;
3. najpóźniej przy pierwszej komunikacji z osobą, której dane dotyczą, jeżeli dane osobowe mają być stosowane do komunikacji z tą osobą;
4. najpóźniej przy pierwszym ujawnieniu danych, jeżeli bank lub rejestr kredytowy planuje ujawnić dane osobowe innemu odbiorcy danych.
5. Informacje, o których mowa w ust. 1, 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.
6. Rejestr kredytowy przetwarza dane osobowe Klientów banków, przy czym są to dane zebrane przez banki i przekazane przez banki do rejestru kredytowego (rejestr kredytowy przetwarza dane zebrane nie od osoby, której dane dotyczą). Rejestry kredytowe jako administratorzy danych, o którym mowa w art. 14 RODO nie spełniają samodzielnie i we własnym zakresie obowiązku informacyjnego, względem osób których dane dotyczą (Klientów banku), ponieważ banki umieszczają klauzule informacyjne w zakresie dotyczącym rejestrów kredytowych w dokumentach przeznaczonych dla Klienta, lub w systemie informatycznym po potwierdzeniu tożsamości osoby, której dane dotyczą, czy też poprzez przesłanie informacji drogą elektroniczną z zastosowaniem zasad bezpieczeństwa. Rejestry kredytowe w zakresie obowiązku informacyjnego korzystają z wyłączenia określonego w art. 14 ust. 5 RODO (ust. 5 a) poniżej).
7. Odstępstwa od wypełnienia obowiązku informacyjnego w stosunku do osoby, której dane dotyczą, są możliwe, jeśli m.in.:
8. Klient posiada stosowne informacje;
9. 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;
10. 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;
11. dane osobowe muszą pozostać poufne zgodnie z obowiązkiem zachowania tajemnicy bankowej oraz innych tajemnic ustawowo chronionych.
12. Bank lub rejestr kredytowy 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 Klienta zawierających klauzule informacyjne, analizy oraz procedury wewnętrzne banku, skrypty rozmów z Klientami.
13. Spełnienie obowiązku informacyjnego może nastąpić również przez wskazanie kategorii odbiorców, na przykład: organów uprawnionych do żądania dostępu do danych osobowych na podstawie art. 105 ust. 1 pkt 2 Prawa bankowego, podmiotów uprawnionych do otrzymania danych osobowych na podstawie art. 104 ust. 2 Prawa bankowego, podmiotów określonych w art. 6a Prawa bankowego (outsourcing) oraz instytucji, o których mowa w art. 105 ust. 4 Prawa bankowego (BIK S.A., Bankowy Rejestr w Związku Banków Polskich).

# PRAWO DOSTĘPU DO DANYCH OSOBY, KTÓREJ DANE DOTYCZĄ

1. Osoba, której dane dotyczą jest uprawniona do uzyskania od banku lub rejestru kredytowego potwierdzenia, czy bank lub rejestr kredytowy przetwarza jego dane osobowe, a jeżeli ma to miejsce, osoba ta jest uprawniona do uzyskania dostępu do danych oraz następujących informacji o:
   1. celu przetwarzania, który powinien być konkretny, wyraźnie określony i prawnie uzasadniony. Przykłady celów przetwarzania danych osobowych wraz ze wskazaniem podstaw prawnych zawarte zostały w Załączniku nr 4 do Kodeksu;
   2. kategorii odnośnych danych osobowych;
   3. odbiorcach lub kategoriach odbiorców, którym dane osobowe zostały lub mogą zostać ujawnione, w szczególności o odbiorcach w państwach trzecich lub organizacjach międzynarodowych. Przykłady odbiorców danych osobowych zawarte zostały w Załączniku nr 4 do Kodeksu;
   4. w miarę możliwości planowany okres przetwarzania danych osobowych, a gdy nie jest to możliwe, kryteria ustalania tego okresu, przy założeniu, iż zapewnione zostanie ograniczenie okresu przechowywania danych do ścisłego minimum. Wyjaśnienia na temat okresów przechowywania danych osobowych zawarte zostały w Załączniku nr 4 do Kodeksu;
   5. informacje 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;
   6. informacje o prawie wniesienia skargi do Organu nadzorczego, jeżeli Klient banku uważa, że przetwarzanie jego danych osobowych narusza jego prawa;
   7. jeżeli dane osobowe nie zostały zebrane od osoby, której dane dotyczą – wszelkie dostępne informacje o ich źródle. Przykłady źródeł danych osobowych zawarte zostały w Załączniku nr 4 do Kodeksu.
   8. 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, według wzoru zawartego w Załączniku nr 3 i 6 do Kodeksu.
2. Jeżeli dane osobowe są przekazywane do państwa trzeciego lub organizacji międzynarodowej, osoba, której dane dotyczą, ma prawo zostać poinformowana przez bank o odpowiednich zabezpieczeniach, o których mowa w art. 46 RODO, związanych z przekazaniem, w tym w szczególności o fakcie zatwierdzenia przez organ nadzorczy niniejszego kodeksu postępowania.
3. Bank lub rejestr kredytowy może udostępnić Klientom kanał, w którym Klient będzie mógł samodzielnie pobrać dane w przypadku żądania Klienta dostępu do danych. W przypadku złożenia przez Klienta wniosku o uzyskanie dostępu do danych lub ich otrzymania, bank lub rejestr kredytowy jest uprawniony w pierwszej kolejności do skierowania Klienta do skorzystania z takiego kanału.
4. Bank lub rejestr kredytowy dostarcza Klientowi kopię danych osobowych podlegających przetwarzaniu. Za wszelkie kolejne kopie, o które zwróci się Klient, bank lub rejestr kredytowy może pobrać opłatę w rozsądnej wysokości wynikającej z kosztów banku lub rejestru kredytowego, o których mowa w ust. 11 Rozdziału I. Ust. 12 Rozdziału I stosuje się odpowiednio.
5. Jeżeli osoba, której dane dotyczą zwraca się o kopię drogą elektroniczną i jeżeli nie zaznaczy inaczej, informacja może zostać udzielona powszechnie stosowaną drogą elektroniczną. W przypadku rejestru kredytowego udostępnienie kopii danych drogą elektroniczną może być uwarunkowane dodatkowymi wymaganiami identyfikacji osoby z uwagi na brak bezpośredniej relacji z osobą (rejestr kredytowy przetwarza dane pozyskane nie od osoby, której dane dotyczą).
6. Spełnienie obowiązku informacyjnego może nastąpić również przez wskazanie kategorii odbiorców, na przykład: organów uprawnionych do żądania dostępu do danych osobowych na podstawie art. 105 ust. 1 pkt 2 Prawa bankowego, podmiotów uprawnionych do otrzymania danych osobowych na podstawie art. 104 ust. 2 Prawa bankowego, podmiotów określonych w art. 6a Prawa bankowego (outsourcing) oraz instytucji, o których mowa w art. 105 ust. 4 Prawa bankowego (BIK S.A., Bankowy Rejestr w Związku Banków Polskich).

# PRAWO DO SPROSTOWANIA DANYCH

1. Osoba, której dane dotyczą, ma prawo żądania od banku lub rejestru kredytowego niezwłocznego sprostowania dotyczących go danych osobowych, które są nieprawidłowe. W przypadku rejestru kredytowego prawo żądania sprostowania danych może dotyczyć danych identyfikacyjnych Klienta w takim zakresie, w jakim rejestr kredytowy będzie w stanie sprawdzić zasadność żądania. Rejestr kredytowy nie realizuje prawa do sprostowania Klienta banku, gdyż poprawność tych danych może potwierdzić tylko bank.
2. Klient ma prawo żądania uzupełnienia niekompletnych danych osobowych, w tym poprzez przedstawienie dodatkowego oświadczenia.
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 terminie 7 dni od wystąpienia okoliczności uzasadniających przekazanie informacji. Rejestr kredytowy jest obowiązany wprowadzić informacje, o których mowa w zdaniu poprzedzającym, do zbioru, w którym są one przetwarzane, w terminie nie dłuższym niż 7 dni od dnia ich otrzymania.

# PRAWO DO USUNIĘCIA DANYCH (PRAWO DO BYCIA ZAPOMNIANYM)

1. W przypadku, gdy osoba, której dane dotyczą, chce zrealizować wobec banku lub rejestru kredytowego uprawnienie do żądania usunięcia danych osobowych jej dotyczących, żądanie takie powinno być wyrażone w formie wyraźnego oświadczenia wskazującego przedmiotowy zakres żądania. Rejestr kredytowy usuwa dane osobowe wykonując dyspozycję banku w wyniku realizacji żądania Klienta banku.
2. Bank lub rejestr kredytowy ustali okresy przechowywania danych, uwzględniając okres nie dłuższy, niż jest to niezbędne dla celów, w których dane są przetwarzane oraz okres dla przechowywania danych w celach archiwalnych lub statystycznych. Ustalenie to może mieć charakter opisowy, wskazujący na kryteria ustalania tego okresu.
3. Bank lub rejestr kredytowy może przechowywać dane do celów wskazanych w Części D ust. 2 Kodeksu.

1. Bank lub rejestr kredytowy może nie uwzględnić żądania usunięcia danych wynikającego z cofnięcia zgody przez osobę, której dane dotyczą na przetwarzanie jej danych, w przypadku gdy zgoda osoby, której dane dotyczą nie była jedyną przesłanką przetwarzania jej danych przez bank lub rejestr kredytowy, w szczególności, gdy celem przetwarzania danych Klienta jest nadal realizacja umowy wiążącej osobę, której dane dotyczą i bank lub rejestr kredytowy albo gdy przetwarzanie danych osoby, której dane dotyczą jest niezbędne do wypełnienia obowiązku prawnego ciążącego na banku lub rejestrze kredytowym.
2. Bank lub rejestr kredytowy ma obowiązek uwzględnienia sprzeciwu osoby, której dane dotyczą, wobec przetwarzania jej danych przez bank lub rejestr kredytowy wniesionego zgodnie z art. 21 ust. 1 RODO, gdy w ocenie banku lub rejestru kredytowego nie występują prawnie uzasadnione podstawy przetwarzania nadrzędne wobec prawa do sprzeciwu i interesów wnioskodawcy.
3. Przetwarzanie przez bank lub rejestr kredytowy danych osobowych osoby, której dane dotyczą, pomimo jej żądania usunięcia danych, jest zgodne z prawem, jeżeli jest niezbędne w szczególności do wywiązania się przez bank lub rejestr kredytowy z obowiązku prawnego, do wykonania przez bank lub rejestr kredytowy zadania realizowanego w interesie publicznym, do celów statystycznych lub do ustalenia, dochodzenia lub obrony roszczeń.
4. Po usunięciu danych zgodnie z żądaniem osoby, której dane dotyczą, bank lub rejestr kredytowy jest uprawniony do zachowania informacji o tym, czyj i jaki wniosek wykonał (w tym celu bank lub rejestr kredytowy może przetwarzać w szczególności imię i nazwisko, PESEL, adres wnioskującego, adres poczty elektronicznej, numer telefonu oraz informację o zakresie usuniętych danych i terminie ich usunięcia). Bank lub rejestr kredytowy do określania katalogu danych niezbędnych do zachowania po ich usunięciu, stosuje zasady minimalizmu danych i ochrony prywatności Klienta.
5. W związku z tym, że banki i rejestry kredytowe nie upubliczniają danych osobowych Klientów, nie stosuje się do nich art. 17 ust. 2 RODO.

# PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. Żądanie ograniczenia przetwarzania danych powinno być złożone w formie wyraźnego oświadczenia Klienta wskazującego przedmiotowy zakres swojego żądania.
2. Ograniczenie przetwarzania danych bank lub rejestr kredytowy może realizować w szczególności poprzez oznaczenie w systemie przechowywanych danych osobowych w celu ograniczenia ich przyszłego przetwarzania, przy czym w przypadku Klienta banku rejestr kredytowy realizuje ograniczenie przetwarzania na wniosek banku.
3. Bank lub rejestr kredytowy może dodatkowo, w celu ograniczenia przetwarzania danych osobowych, w szczególności:
4. czasowo przenieść wybrane dane osobowe do innego systemu przetwarzania,
5. uniemożliwić użytkownikom dostęp do wybranych danych,
6. czasowo usunąć ze strony internetowej opublikowane dane,
7. ograniczyć środkami technicznymi przetwarzanie w zautomatyzowanych zbiorach danych w taki sposób, by dane osobowe nie podlegały dalszemu przetwarzaniu ani nie mogły być zmieniane.
8. Bank lub rejestr kredytowy dokłada należytej staranności w celu wykonania ciążących na nim obowiązków związanych z ograniczeniem przetwarzania danych osobowych osoby, której dane dotyczą, a w szczególności dokonuje niezwłocznej weryfikacji prawidłowości przetwarzania danych w przypadku, złożenia żądania, o którym mowa w ust. 1.
9. Bank lub rejestr kredytowy może przechowywać dane osobowe, co do których zostało zgłoszone żądanie ograniczenia przetwarzania.
10. Realizacja żądania ograniczenia przetwarzania danych nie powoduje zaprzestania przez bank lub rejestr kredytowy przetwarzania, które jest niezbędne do wykonania przez bank lub rejestr kredytowy obowiązków wynikających z przepisów prawa, zaleceń lub rekomendacji Organu nadzorczego oraz innych organów nadzorujących bank lub rejestr kredytowy.

# OBOWIĄZEK POWIADOMIENIA O SPROSTOWANIU LUB USUNIĘCIU DANYCH OSOBOWYCH LUB O OGRANICZENIU PRZETWARZANIA

1. Bank lub rejestr kredytowy poinformuje o sprostowaniu lub usunięciu danych osobowych lub ograniczeniu przetwarzania każdego odbiorcę, któremu ujawnił dane osobowe Klienta.
2. Obowiązek o którym mowa w ust. 1 jest wyłączony, gdy zawiadomienie okaże się niemożliwe lub wymagać będzie niewspółmiernie dużego wysiłku, w szczególności gdy: a) zmiana, sprostowanie, ograniczenie lub usunięcie nie jest widoczne dla odbiorcy, w tym podmiotów przetwarzających, lecz wymaga ustanowienia odrębnego kanału komunikacji;

b) odbiorca dalej nie funkcjonuje , został zlikwidowany lub wykreślony z rejestru (zakończył działalność);

c) z okoliczności wynika, że dane nie będą dalej przetwarzane.

1. Bank lub rejestr kredytowy na żądanie osoby, której dane dotyczą, przekazuje informacje o odbiorcach, którym przekazano jego dane.
2. Jeśli obowiązek, o którym mowa w ust. 3, okaże się niewykonalny lub wymaga niewspółmiernie dużego wysiłku, bank lub rejestr kredytowy powinien udokumentować podjęcie racjonalnych działań, z uwzględnieniem dostępnych mu technologii i dostępnych mu środków, w tym technicznych, w celu wypełnienia tego obowiązku.
3. W przypadku rejestrów kredytowych obowiązek informowania, o którym mowa w ust.1 realizowany jest poprzez udostępnianie raportów kredytowych z aktualnymi danymi.

# PRAWO DO PRZENOSZENIA DANYCH

# VIII.a Zasady ogólne

1. Klientowi przysługuje prawo do otrzymania w ustrukturyzowanym, powszechnie używanym formacie nadającym się do odczytu maszynowego danych osobowych go dotyczących oraz prawo do żądania przesłania tych danych innemu Administratorowi („prawo do przenoszenia danych”) na zasadach określonych w niniejszym Kodeksie.
2. Klientowi przysługuje prawo do żądania przenoszenia danych go dotyczących, które dostarczył bankowi lub rejestrowi kredytowemu, jeżeli dane te są przetwarzane przez bank lub rejestr kredytowy na podstawie zgody Klienta lub na podstawie umowy, której Klient jest stroną.
3. Dane podlegające przenoszeniu to dane przetwarzane przez bank lub rejestr kredytowy w sposób zautomatyzowany. Przenoszeniu nie podlegają dane znajdujące się w zbiorach papierowych.
4. Dane podlegające przenoszeniu to dane, które zostały przekazane bankowi lub rejestrowi kredytowemu przez Klienta świadomie i aktywnie oraz dane wygenerowane przez działanie Klienta, w tym dane dotyczące transakcji.
5. Dane niepodlegające przenoszeniu to dane wywnioskowane i/lub dane wywiedzione przez bank lub rejestr kredytowy na podstawie danych przekazanych przez Klienta, w tym w szczególności to dane dotyczące oceny zdolności kredytowej, jak również dane pochodzące od osób trzecich (np. dane o transakcjach, w których osoba żądająca przeniesienia danych jest drugą stroną transakcji).
6. W przypadku, gdy bank lub rejestr kredytowy nie ma możliwości oddzielenia danych, o których przeniesienie wnosi wnioskodawca, od innych danych znajdujących się w systemach informatycznych banku lub rejestru kredytowego (np. w zakresie informacji o dokonanych transakcjach), bank może się powstrzymać z wykonaniem żądania osoby do czasu uzgodnienia z nią ostatecznego zakresu jej żądania i złożenia przez nią odpowiednich oświadczeń (zgód) niezbędnych do umożliwienia bankowi przekazania danych w innym zakresie niż pierwotnie wnioskowany.
7. Rejestry kredytowe nie otrzymują danych bezpośrednio od Klienta banku. Dane Klienta banku przekazywane są do rejestru kredytowego przez bank i w związku z tym Klientowi banku nie przysługuje uprawnienie do przenoszenia danych w stosunku do rejestru kredytowego.
8. Klient może złożyć wniosek w celu skorzystania z przysługującego mu prawa do przenoszenia danych osobiście lub przez osobę upoważnioną przez niego na zasadach wskazanych w Rozdziale I Części C niniejszego Kodeksu. We wniosku Klient obowiązany jest wskazać, jakie konkretnie dane osobowe objęte są żądaniem przeniesienia.
9. Banki stosują powszechnie używany format (np. xml, csv, JSON) oraz strukturę, aby zapewnić interoperacyjność, rozumianą jako: możliwość współdziałania różnych odrębnych organizacji na rzecz osiągnięcia uzgodnionych i korzystnych dla wszystkich stron celów, przy jednoczesnym dzieleniu się informacjami i wiedzą pomiędzy tymi organizacjami poprzez wspierane przez nie procesy biznesowe, za pomocą wymiany danych za pośrednictwem odpowiednich systemów.

# VIII.b Prawo do otrzymywania danych

1. Bank lub rejestr kredytowy zapewni możliwość otrzymania pliku na urządzenie prywatne osoby na przykład przez usługi bankowości elektronicznej. Jeżeli Klient nie posiada usług bankowości elektronicznej, bank może umożliwić złożenie wniosku w innej formie np. papierowej.
2. Banki lub rejestry kredytowe przyjmą rozwiązania mające na celu udzielenie Klientowi informacji mającej na celu umożliwienie Klientowi podjęcia kroków na rzecz ochrony informacji, które otrzymał. Bank lub rejestr kredytowy może również, w ramach dobrej praktyki, zalecić odpowiednie środki ochrony w osiągnięciu tego celu.

# VIII.c Prawo do żądania do przesłania danych innemu administratorowi

1. Na wniosek Klienta, bank będzie przesyłał bezpośrednio innemu bankowi pełniącemu rolę Administratora dane osobowe wskazane we wniosku Klienta. W przypadku wniosku o przesłanie danych do Administratora spoza sektora bankowego, należy korzystać z możliwości bezpośredniego przekazywania danych Klientowi, o ile bankowi nie uda się ustalić, czy istnieje możliwość bezpośredniego przeniesienia tych danych do drugiego Administratora.
2. Składając wniosek o przeniesienie danych Klient złoży oświadczenie o wyrażeniu zgody na przeniesienie danych do innego Administratora. W przypadku braku złożenia takiego oświadczenia, bank przekaże dane bezpośrednio Klientowi lub powstrzyma się z wykonaniem takiego żądania do czasu otrzymania odpowiedniego oświadczenia.
3. Przenoszenie danych nie nakłada na bank obowiązku zatrzymywania danych osobowych dłużej niż to konieczne czy też dłużej niż przez określony okres przechowywania. Jeżeli bank nie zatrzymuje części danych generowanych przez użytkownika, wówczas jego dane osobowe nie mogą być zawarte we wniosku o przeniesienie danych.
4. Bank „otrzymujący” dane osobowe zobowiązany jest do stosowania zasad określonych w RODO.
5. Dane mogą być przenoszone, o ile jest to technicznie możliwe.
6. Historia rachunku może zawierać dane osobowe osób trzecich. W sytuacji, gdy dane Klienta takie jak np. historia transakcji, zawierają dane osób trzecich, Administrator, do którego dane zostały przeniesione, nie powinien przetwarzać danych osób trzecich w żadnym celu, który by negatywnie wpłynął na prawa i wolności tych osób.
7. Prawo do przenoszenia danych nie może negatywnie wpływać na prawa i wolności innych osób, w tym osób, których dane znajdują się w historiach transakcji. Ma to na celu uniknięcie uzyskiwania i przesyłania danych obejmujących dane osobowe innych osób, których dane dotyczą (tych, które nie wyraziły zgody) do nowego Administratora w przypadkach, gdy istnieje prawdopodobieństwo, że dane te będą przetwarzane w sposób, który negatywnie wpłynie na prawa i wolności innych osób, których dane dotyczą.
8. W zakresie, w jakim bank realizuje wniosek osoby, której dane dotyczą, o przeniesienie danych, bank nie jest zobowiązany do poinformowania osób trzecich, których dane mogą być zawarte w przenoszonych danych, o wykonaniu takiego żądania i jego treści.
9. Bank przesyłający dane podejmie należyte starania w celu zapewnienia aby dane osobowe zostały bezpiecznie przesłane (np. z zastosowaniem szyfrowania) do właściwego miejsca przeznaczenia (np. przy użyciu informacji uwierzytelniających).

# PRAWO SPRZECIWU

* 1. W przypadku wniesienia przez Klienta sprzeciwu, Klient powinien wskazać, wobec jakiego konkretnego celu przetwarzania wnosi sprzeciw i wykazać, na czym polega jego szczególna sytuacja. W przypadku sprzeciwu wniesionego przez Klienta banku do rejestru kredytowego, rejestr kredytowy przekazuje ten sprzeciw celem rozpatrzenia przez bank.
  2. Banki lub rejestry kredytowe uwzględniają sprzeciw bądź odmawiają jego uwzględnienia, po dokonaniu analizy, czy szczególna sytuacja osoby, której dane dotyczą, ma charakter nadrzędny wobec prawnie uzasadnionych podstaw do przetwarzania dokonywanego przez bank. Na czas dokonania analizy, banki, na wyraźne żądanie osoby, której dane dotyczą, stosują ograniczenie przetwarzania na podstawie art. 18 ust. 1 RODO.
  3. Odmawiając uwzględnienia sprzeciwu, bank lub rejestr kredytowy w przystępny sposób wyjaśnia osobie, której dane dotyczą przyczyny, dla których uważa, że interesy, prawa i wolności tej osoby, nie mają charakteru nadrzędnego.
  4. Banki lub rejestry kredytowe mogą przetwarzać dane na potrzeby marketingu bezpośredniego (w tym profilowania) w oparciu o podstawę prawną określoną w Części B Rozdział II lit. f). W przypadku złożenia przez osobę, której dane dotyczą, sprzeciwu wobec takiego rodzaju przetwarzania, bank lub rejestr kredytowy nie przetwarza dłużej danych w tym celu.

* 1. Banki lub rejestry kredytowe mogą przetwarzać dane osobowe dla celów statystycznych, w tym na podstawie obowiązujących przepisów dotyczących sektora bankowego. W przypadku złożenia przez osobę sprzeciwu wobec przetwarzania danych osobowych w tym celu, osoba, której dane dotyczą powinna wykazać, na czym polega szczególny charakter jej sytuacji i jakie prawa osoby są zagrożone.
  2. Po dokonaniu analizy szczególnej sytuacji tej osoby, banki lub rejestry kredytowe w zakresie dotyczącym ich Klientów odmawiają uwzględnienia sprzeciwu, w przypadku gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym, w jasny i przystępny sposób wyjaśniając przyczyny odmowy.
  3. W ramach realizacji prawa do sprzeciwu, banki lub rejestry kredytowe w zakresie dotyczącym ich Klientów umożliwiają złożenie sprzeciwu drogą elektroniczną, przy zachowaniu procedur bezpieczeństwa i identyfikacji osoby składającej żądanie. Za złożenie sprzeciwu banki lub rejestry kredytowe nie pobierają opłat.

# PRZECHOWYWANIE I USUWANIE DANYCH OSOBOWYCH

1. Dane osobowe Klientów lub potencjalnych Klientów nie mogą być przechowywane w formie umożliwiającej ich identyfikację przez okres dłuższy, niż jest to niezbędne do celów, w których dane te są przetwarzane.
2. Po osiągnięciu zamierzonych (pierwotnych) celów przetwarzania, o których mowa w ust. 1, dane osobowe osób, których dane dotyczą, powinny zostać usunięte, chyba, że ich dalsze przechowywanie znajduje podstawę prawną (np. ustawa z dnia 29 września 1994 r. o rachunkowości, ustawa z dnia 29 sierpnia 1997 r. - Ordynacja podatkowa, ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, ustawa z dnia 24 listopada 2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystywaniu sektora finansowego do wyłudzeń skarbowych).
3. Dalsze przetwarzanie danych osobowych jest dopuszczalne w przypadku ich przetwarzania dla prawnie uzasadnionego interesu, o którym mowa w Części B Rozdział II lit. f), tj. m.in. w celu:

a) realizacji działań zmierzających do zapewnienia ochrony i odporności systemów informatycznych banków oraz rejestrów kredytowych na przypadkowe zdarzenia albo niezgodne z prawem lub nieprzyjazne działania naruszające dostępność, autentyczność, integralność i poufność przechowywanych lub przesyłanych danych osobowych oraz zapewnienia bezpieczeństwa związanych z nimi usług oferowanych lub udostępnianych przez banki i rejestry kredytowe poprzez te systemy informatyczne;

b) ciągłego i niezakłóconego prowadzenia działalności przez banki oraz rejestry kredytowe poprzez zapewnienie integralności kopii zarchiwizowanych/zapasowych/awaryjnych od momentu ich utworzenia aż do likwidacji;

c) archiwizacyjnym (dowodowym) dla zabezpieczenia się przed różnymi rodzajami twierdzeń i roszczeń (zarzutów), dotyczy to zwłaszcza danych osobowych znajdujących się we wnioskach kredytowych niezakończonych zawarciem umowy kredytu;

d) realizacji zadań przez rejestry kredytowe oraz banki związanych z zapobieganiem przestępstwom dokonywanym na szkodę banku lub rejestru kredytowego, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, w tym w szczególności w celu zapobiegania oszustwom, a także zarządzania ryzykiem operacyjnym w działalności banków;

e) wypełnienia zaleceń i rekomendacji Organu nadzorczego, jak również innych nadzorców, w tym Komisji Nadzoru Finansowego;

f) analityki biznesowej, celów naukowych lub do celów wewnętrznych analiz statystycznych;

g) marketingu bezpośredniego (motyw 47 RODO).

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

# PROFILOWANIE ORAZ ZAUTOMATYZOWANE PRZETWARZANIE DANYCH OSOBOWYCH OSÓB FIZYCZNYCH

1. Profilowanie jest metodą (sposobem) przetwarzania danych osobowych. Może być ono oparte o różne modele i algorytmy.
2. Profilowanie opiera się na odpowiednich matematycznych lub statystycznych procedurach profilowania, z zachowaniem środków technicznych i organizacyjnych zapewniających zmniejszenie ryzyka błędów w procedurach profilowania.
3. Banki i rejestry kredytowe profilują Klientów między innymi w celach:
   1. przeprowadzenia analizy lub prognozy aspektów dotyczących oceny zdolności i wiarygodności kredytowej osoby fizycznej m.in. poprzez przypisanie jej określonej oceny punktowej (tzw. scoring);
   2. realizacji Rekomendacji T Komisji Nadzoru Finansowego 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;
   3. 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;
   4. przeciwdziałania praniu pieniędzy, w tym w celu budowania modeli umożliwiających identyfikację działań przestępczych;
   5. 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;
   6. 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;
   7. 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;
   8. 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;
   9. 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;
   10. 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;
   11. 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;
   12. 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.);
   13. badania poziomu wiedzy Klientów o inwestowaniu w instrumenty finansowe oraz doświadczenie inwestycyjne niezbędne do oceny, czy dana usługa maklerska jest odpowiednia dla Klienta.
4. Ocena punktowa Klienta lub inny profil udostępniony przez rejestr kredytowy, czy też będący wynikiem profilowania przez bank w oparciu o modele własne banku, może być wykorzystywana przez banki do podjęcia w stosunku do Klienta określonych działań, w których istotnym elementem jest proces oceny zdolności i wiarygodności kredytowej Klienta, przykładowo:
5. podjęcie decyzji kredytowej;
6. monitorowanie spłaty przez Klienta zobowiązania kredytowego;
7. dokonanie przez bank wstępnej weryfikacji potencjalnych Klientów pod kątem możliwości zaproszenia ich do negocjacji w zakresie nabycia określonych produktów banku;
8. 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.
9. Banki jak i rejestry kredytowe stosują dobre praktyki rynku bankowego odnośnie konstrukcji i zarządzania modelami statystycznymi, którego ramy wyznaczone są przez m.in. Rekomendację W Komisji Nadzoru Finansowego dotyczącą zarządzania ryzykiem modeli w bankach.
10. Rejestr kredytowy przeprowadza operacje na danych osobowych Klienta, których wynikiem jest ocena punktowa lub inny profil (np. segmentacja). Rejestr kredytowy nie wykorzystuje jej do podejmowania działań w stosunku do osoby, dla której ta ocena została wyliczona.
11. Do profilowania banki i rejestry kredytowe wykorzystują dane osobowe osoby, której dane dotyczą i dane o jego zobowiązaniach (w tym historię kredytową Klienta) w takim zakresie, w jakim przetwarzanie tych danych jest niezbędne i adekwatne do celu przetwarzania.
12. Procedury profilowania nie są udostępniane Klientom w zakresie objętym tajemnicą przedsiębiorcy, prawami własności intelektualnej  lub prawami autorskimi chroniącymi oprogramowanie banku lub rejestru kredytowego.
13. Opis modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym stanowi Załącznik nr 3 do niniejszego Kodeksu. Przykłady zautomatyzowanego przetwarzania danych zawiera Załącznik nr 6 do niniejszego Kodeksu.
14. Zindywidualizowane oferty marketingowe kierowane do Klientów 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. Zindywidualizowana oferta w istotny sposób wpływa na Klienta, jeśli prowadzi do dyskryminacji lub nierównego traktowania opartego na nieobiektywnych kryteriach).
15. Procesy:
16. segmentacji Klientów;
17. marketingu bezpośredniego produktów i usług własnych;
18. marketingu podmiotów z grupy;
19. marketingu podmiotów trzecich;
20. dostosowania komunikacji kierowanej do Klientów;

oparte na profilowaniu mogą stanowić prawnie uzasadniony interes banków i rejestrów kredytowych. Powinno to się odbywać w sposób, który nie powoduje nadmiernej ingerencji w prawo do prywatności i którego podmiot danych może się racjonalnie spodziewać.

1. Zawarcie umowy, a tym samym przyjęcie regulaminu korzystania z systemu bankowości elektronicznej lub aplikacji mobilnej wykorzystującej profilowanie będzie stanowić podstawę prawną profilowania danych Klientów w celu świadczenia im usług/funkcjonalności opartych na profilowaniu danych oraz w celu przygotowywania oraz prezentowania im dopasowanych/zindywidualizowanych ofert marketingowych.
2. W przypadku, gdy Klient złoży sprzeciw wobec profilowania na podstawie dotyczących go danych w serwisie transakcyjnym lub aplikacji mobilnej, których funkcjonalność jest oparta na tego typu przetwarzaniu, wówczas bank zaprzestanie udostępniania tej funkcjonalności Klientowi, adekwatnie do treści złożonego sprzeciwu.
3. Adekwatnie do możliwości technicznych i organizacyjnych danego banku będzie istniała możliwość, aby w przypadku złożenia przez Klienta sprzeciwu, o którym mowa w ust. 13, bank oferował możliwość korzystania z serwisu transakcyjnego lub aplikacji mobilnej bez funkcjonalności opartych na profilowaniu danych.

# POWIERZENIE PRZETWARZANIA - KLAUZULE UMÓW Z DOSTAWCAMI

1. Banki jako administratorzy mogą stosować zapisy do umów zawieranych z podmiotami przetwarzającymi stanowiące Załącznik nr 5 do niniejszego Kodeksu. W przypadku wydania przez Komisję Europejską lub Organ nadzoru standardowych klauzul umownych mają one pierwszeństwo przed postanowieniami niniejszego Kodeksu.

1. Ustanowione w niniejszym Kodeksie standardowe klauzule umowne mają charakter przykładowy i nie wyłączają prawa banku do zastosowania we własnych umowach z podmiotami przetwarzającymi dane odmiennych klauzul, w szczególności, gdy bank działa w ramach Grupy.
2. Banki i rejestry kredytowe powierzając przetwarzanie danych osobowych korzystają z usług takich dostawców, którzy zapewniają wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dotyczą. Administratorzy 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).
3. 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.
4. W przypadku podmiotów świadczących na rzecz banków usługi obejmujące czynności bankowe, przyjmuje się, że wystarczające gwarancje wdrożenia odpowiednich środków technicznych i organizacyjnych, aby przetwarzanie spełniało wymogi Rozporządzenia i chroniło prawa osób, których dotyczą, są spełnione przez takie podmioty, którym będą powierzone dane osobowe, które:
   1. przystąpiły do stosowania niniejszego Kodeksu; lub
   2. świadczą na rzecz banku usługi, na które zgody udzieliła Komisja Nadzoru Finansowego oraz przedstawiły bankowi opis rozwiązań technicznych i organizacyjnych, zapewniających bezpieczne i prawidłowe wykonywanie powierzonych czynności, w szczególności ochronę tajemnicy prawnie chronionej; lub
   3. posiadają certyfikaty potwierdzające wdrożenie przez te podmioty odpowiednich środków technicznych i organizacyjnych.
5. Ust. 5 lit. a) i c) stosuje się odpowiednio do rejestrów kredytowych.

# POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH

1. Naruszenie ochrony danych osobowych w bankach i rejestrach kredytowych rozpatrywane jest jako zdarzenie występujące w ramach ryzyka operacyjnego, które należy rozumieć jako możliwość wystąpienia straty wynikającej z niedostosowania lub zawodności procesów wewnętrznych, ludzi i systemów lub ze zdarzeń zewnętrznych.
2. Naruszeniem ochrony danych osobowych 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 w ramach prowadzonej przez administratora danych działalności.
3. Za naruszenie ochrony danych osobowych podlegające obowiązkowi zgłoszenia:
4. organowi nadzorczemu - uznać należy sytuację, w której prawdopodobieństwo wystąpienia ryzyka naruszenia praw lub wolności osób fizycznych zostało oszacowane przez bank lub rejestr kredytowy na poziomie wyższym niż niski;
5. osobie, której dane dotyczą - uznać należy sytuację, w której bank lub rejestr kredytowy oszacował ryzyko naruszenia praw i wolności tej osoby jako wysokie.
6. W szczególności do naruszenia mogą prowadzić następujące sytuacje:
7. utraty danych osobowych uniemożliwiającej wykonanie zobowiązania;
8. naruszenia integralności danych osobowych niosącego ryzyko błędnego wykonania zobowiązania;
9. utraty poufności danych osobowych;

a będące następstwem:

1. skompromitowania lub błędnego działania systemu informatycznego;
2. zdarzeń losowych/środowiskowych;
3. niepożądanych (sabotażowych/dezorganizacyjnych) działań osób, w tym osób trzecich (kradzież, zniszczenie, uniemożliwienie dostępu, modyfikacja, ujawnienie danych);
4. błędu ludzkiego, w tym w ramach niewłaściwego postępowania personelu w zakresie zabezpieczenia danych osobowych.
5. Z zastrzeżeniem dokonania oceny ryzyka naruszenia, za naruszenie ochrony danych osobowych podlegające zgłoszeniu do osoby, której dane dotyczą, może być uznany w szczególności: wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych z numerami kart kredytowych wraz z informacjami pozwalającymi na wykonanie transakcji przez osobę trzecią, wyciek bazy zawierającej tylko pojedynczą daną, ale pozwalającą jednocześnie nawiązać kontakt z osobą fizyczną np. numer telefonu, adres email (naruszeniem podlegającym zgłoszeniu nie będzie zatem wyciek pliku zawierającego same nazwy ulic wraz z numerami, same kody pocztowe bądź nazwy miast), wysłanie pocztą elektroniczną/tradycyjną dokumentów zawierających dane stanowiące tajemnicę bankową do osoby nieupoważnionej (np. błędne wysłanie karty kredytowej, błędne wysłanie dokumentacji kredytowej), przechwycenie oraz wyciek danych/narzędzi służących do logowania i identyfikacji Klientów w bankowości elektronicznej, zagubienie/kradzież dokumentów z danymi Klientów, zerwanie plomb założonych na pojemnikach służących do archiwizacji dokumentów, wygenerowanie i użycie błędnej bazy danych do wysyłki Klientom informacji marketingowych/chronionych wysłanie maili do odkrytych odbiorców, informacja uzyskana w trybie dostępu do danych osobowych przez osobę nieuprawnioną (tzw. informacja ustawowa).
6. Za naruszenie ochrony danych osobowych nie podlegające zgłoszeniu ani do regulatora, ani do organu może być uznane w szczególności: wyciek (tj. niekontrolowane ujawnienie) informacji z bazy danych z numerami kart kredytowych lub numerami rachunków lub numerami umów (bądź fragmentów tych numerów) nie pozwalających na identyfikację konkretnej osoby, zagubienie nośnika danych z plikiem zaszyfrowanym, przy czym klucz używany do odszyfrowania tych danych nie został złamany w wyniku naruszenia, błędne wprowadzenie danych kontaktowych Klienta do systemu banku lub rejestru kredytowego, jeżeli w wyniku tego błędu nie doszło do ujawnienia tajemnicy bankowej ani naruszenia interesów konsumenta, ujawnienie informacji prawnie chronionych osobie trzeciej, jeżeli do ich ujawnienia doszło w z winy Klienta (np. dane do logowania, dane do identyfikacji podawane na infolinii, umożliwienie zapoznania się z pocztą elektroniczną, udostępnienie treści wiadomości SMS).
7. Obowiązek notyfikacji powinien zostać wykonany bez zbędnej zwłoki – w miarę możliwości, nie później niż w terminie 72 godzin po stwierdzeniu naruszenia. Przez stwierdzenie naruszenia uznaje się moment, w którym bank/rejestr kredytowy po zakończeniu postępowania wyjaśniającego w ramach swoich wewnętrznych procedur uzna, że prawdopodobieństwo wystąpienia ryzyka naruszenia prawa i wolności osoby fizycznej zostało ocenione jako wyższe niż niskie. To, czy zawiadomienia dokonano bez zbędnej zwłoki, należy ustalić z uwzględnieniem w szczególności konieczności ustalenia przyczyn i skutków naruszenia oraz minimalizacji tych skutków, charakteru i wagi naruszenia ochrony danych osobowych, jego konsekwencji oraz niekorzystnych skutków dla osoby, której dane dotyczą.

W przypadku niedotrzymania powyższego terminu do zgłoszenia należy dołączyć wyjaśnienie przyczyny opóźnienia.

1. W sytuacji, w której naruszenie ochrony danych osobowych powodowałoby wysokie ryzyko naruszenia praw lub wolności osób fizycznych, o naruszeniu tym należy bezzwłocznie powiadomić osoby, których dane dotyczą, a jeśli powiadomienie takie wymagałoby niewspółmiernie dużego wysiłku należy wydać publiczny komunikat o naruszeniu.
2. W przypadku obowiązku zawiadomienia osoby fizycznej, takie zawiadomienie powinno uwzględniać również zalecenia dla takiej osoby co do minimalizacji potencjalnie niekorzystnych skutków naruszenia ochrony jej danych osobowych. Administrator przekazuje takie zawiadomienie uwzględniając wskazówki Organu nadzorczego lub innych uprawnionych organów udzielone w tym zakresie.
3. Zawiadomienie osoby fizycznej nie jest konieczne, jeśli wdrożono adekwatne środki ochrony obejmując nimi dane osobowe, których dotyczy naruszenie oraz zastosowano środki eliminujące prawdopodobieństwo wysokiego ryzyka naruszenia praw lub wolności osób, których dane dotyczą.
4. Z każdego naruszenia ochrony danych osobowych sporządza się dokumentację opisującą w szczególności:
5. okoliczności naruszenia, tj. przykładowo:

- datę i godzinę stwierdzenia naruszenia ochrony danych osobowych,

- opis charakteru naruszenia,

- przyczynę naruszenia;

1. zaistniałe oraz prawdopodobne skutki naruszenia;
2. podjęte działania zaradcze.

# OCENA SKUTKÓW PRZETWARZANIA DANYCH

1. Banki i rejestry kredytowe powinny rozważyć przeprowadzenie oceny skutków dla ochrony danych osobowych w sytuacji gdy przykładowo:
2. przed wdrożeniem lub użyciem nowych technologii, takich jak np. nowych systemów informatycznych, nowych procesów, nowych funkcjonalności istniejących systemów lub dokonywania w nich zmian, w których przeprowadzane są operacje w zakresie przetwarzania danych Klientów banku czy też innych danych osobowych;
3. przed rozpoczęciem profilowania danych osobowych Klientów niezależnie od celu, dla którego będzie to robione, które jest podstawą do decyzji wywołującej skutki prawne wobec osoby fizycznej lub w podobny sposób znacząco wpływające na osobę fizyczną;
4. nabycie zbiorów danych od innych administratorów danych, np. w związku fuzją z innym bankiem, połączeniem się banków, etc.;
5. w przypadku naruszenia ochrony danych osobowych, o którym mowa w art. 4 pkt 12 RODO;
6. w przypadku zmiany przepisów prawa w zakresie ochrony danych osobowych;
7. przed przetwarzaniem przez bank danych biometrycznych lub innych szczególnych kategorii danych Klientów w celu podjęcia decyzji wobec Klienta (motyw 91 RODO);
8. przed wprowadzeniem nowej usługi lub produktu;

pod warunkiem, że dany rodzaj przetwarzania ze względu na swój charakter, zakres, kontekst i cele z dużym prawdopodobieństwem może powodować wysokie ryzyko naruszenia praw lub wolności osób fizycznych.

1. Niezależnie od okoliczności wymienionych w ust. 1, bank lub rejestr kredytowy dokonuje oceny skutków przetwarzania w sytuacjach określonych w art. 35 ust. 3 RODO.
2. Jeśli profilowanie odbywa się na przykład:

- na potrzeby różnych kampanii reklamowych prowadzonych przez bank lub rejestr kredytowy,

- na potrzeby zarządzania portfelem Klienta,

- na potrzeby oferowania spersonalizowanych ofert dla określonych grup Klientów,

wówczas nie ma konieczności przeprowadzania oceny skutków przed rozpoczęciem profilowania na potrzeby każdej z tych kampanii, ale możliwe jest przeprowadzenie pojedynczej oceny.

1. Dla podobnych operacji przetwarzania danych wiążących się z podobnym ryzykiem można przeprowadzić pojedynczą ocenę.

# Załączniki do Kodeksu

## Załącznik nr 1 - Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie organu nadzorczego

**WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH – ZAWIADOMIENIE ORGANU NADZORCZEGO**

**Zgłoszenie naruszenia ochrony danych osobowych**

Działając na podstawie art. 33 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych), ………………[*wskazać pełną nazwę prawną oraz adres siedziby administratora*] [„**Administrator**”] zgłasza niniejszym przypadek naruszenia ochrony danych osobowych.

W związku ze stwierdzeniem naruszenia ochrony danych osobowych Administrator przekazuje następujące informacje: w dniu …………Administrator stwierdził przypadek naruszenia ochrony danych osobowych polegający na …………[*wskazać charakter naruszenia*].

W wyniku incydentu naruszone zostały następujące dane osobowe: ……………..[ *wskazać kategorię i przybliżoną liczbę osób, których dane zostały naruszone oraz przybliżona liczbę wpisów danych osobowych których dotyczy naruszenie].* Przedmiotowy incydent bezpieczeństwa może mieć wpływ na ………………[*opisać możliwe konsekwencje naruszenia].*

Administrator informuje, że niezwłocznie po zidentyfikowaniu naruszenia zastosował następujące środki bezpieczeństwa w celu usunięcia/zminimalizowania negatywnych skutków naruszenia ……………….[*opisać zastosowane lub proponowane środki bezpieczeństwa].*

Jednocześnie administrator wyjaśnia, że przyczyną opóźnienia przekazania niniejszego zgłoszenia jest ………………………\*

Więcej informacji na temat naruszenia ochrony danych osobowych można uzyskać od ……….[*wskazać dane kontaktowe inspektora danych osobowych lub innego punktu kontaktowego – imię, nazwisko, adres email / nr telefoniczny*].

Z poważaniem

……………………………….

Podpis

*\* do wypełnienia w przypadku, gdy zgłoszenie jest przekazywane po upływie 72 godzin od stwierdzeniu naruszenia*

## Załącznik nr 2 - Wzór powiadomienia o naruszeniu ochrony danych osobowych – zawiadomienie osoby, której dane dotyczą

**WZÓR POWIADOMIENIA O NARUSZENIU OCHRONY DANYCH OSOBOWYCH – ZAWIADOMIENIE OSOBY, KTÓREJ DANE DOTYCZĄ**

**Zawiadomienie o naruszeniu ochrony danych osobowych**

**Szanowny Panie/Szanowna Pani,**

Bank/Rejestr kredytowy …………………... [*wskazać pełną nazwę prawną*] z siedzibą w ………..ul. ……………[*wskazać adres siedziby banku*] („**Bank**” / Rejestr kredytowy) uprzejmie informuje o stwierdzeniu naruszenia ochrony Pana/Pani danych osobowych przetwarzanych przez Bank/Rejestr kredytowy w związku z ………….[*opisać w związku z jakimi usługami/produktami przetwarzane są dane osobowe – np. rachunek bankowy/karta kredytowa*].

Naruszenie ochrony danych osobowych polega na ……………………[*wskazać charakter naruszenia*] i może mieć następujące skutki dla Pana/Pani ………………..

Niezwłocznie po stwierdzeniu naruszenia, Bank / Rejestr kredytowy podjął następujące środki w celu usunięcia/zminimalizowania ewentualnych skutków……………….[*opisać zastosowane lub proponowane środki bezpieczeństwa].*

Bank / Rejestr kredytowy zapewnia, że podjął niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości. W razie dodatkowych pytań lub wątpliwości prośba o kontakt z ……….[*wskazać dane kontaktowe inspektora danych osobowych lub innego punktu kontaktowego – imię, nazwisko, adres email / nr telefoniczny*].

Niniejsze zawiadomienie zostało przygotowane przez Bank/ Rejestr kredytowy zgodnie z wymogami unijnego Rozporządzenia o ochronie danych osobowych mającego zastosowanie od dnia 25 maja 2018 r. Dodatkowo, zgodnie z tymi wymogami, Bank / Rejestr kredytowy przekazał zawiadomienie o przedmiotowym naruszeniu do Prezesa Urzędu Ochrony Danych Osobowych.

Z poważaniem,

……………………………….

Podpis

## Załącznik nr 3 – Opis przykładowego modelu oceny punktowej (scoringowego) wykorzystywanego w procesie zarządzania ryzykiem kredytowym

Wyliczenie punktacji na podstawie modelu scoringowego wygląda następująco:

Model scoringowy ma najczęściej postać tablicy scoringowej, jednej albo wielu w zależności od stopnia złożoności i skali wykorzystania danego modelu. Najprostsze modele składają się z jednej tablicy scoringowej. Natomiast modele charakteryzujące się wysokim poziomem złożoności mogą składać się z wielu tablic. Każda z tablic scoringowych ocenia jednorodny segment Klientów pod względem ryzyka kredytowego. Segmentacja modeli ma na celu uzyskanie optymalnej efektywności modelu dla danego procesu biznesowego. Tak więc kryteria podziału Klientów na segmenty mogą wynikać zarówno z przesłanek biznesowych, jak i statystycznych.

Tablica scoringowa składa się z cech, czyli m.in. informacji opisujących Klienta ,przy czym w przypadku oceny ryzyka kredytowego mogą to być zarówno cechy socjo-demograficzne Klienta, jak i jego cechy behawioralne lub jego zachowania kredytowe przykładowo ilość posiadanych czynnych kredytów na moment naliczania tej oceny, największa liczba dni opóźnienia w spłacie jakiegokolwiek kredytu w ostatnich 3 miesiącach, maksymalny procent wykorzystania limitu kredytowego w ostatnich 6 miesiącach.

Z kolei cechy mają swoje warianty, czyli pewne przedziały wartości jakie może przyjąć dana cecha np. cecha „*Maksymalny procent wykorzystania limitu kredytowego w ostatnich 6 miesiącach”* może mieć poniższe warianty:

* <0-5>%
* (5-10%>
* (10-50>
* (50% i więcej)

Do każdego wariantu cechy przypisana jest punktacja. W powyższym przykładzie może to wyglądać tak:

**Cecha:** „*Maksymalny procent wykorzystania limitu kredytowego w ostatnich 6 miesiącach”*

**Wariant cechy Punktacja**

<0-5>% 63 pkt.

(5-10%> 46 pkt.

(10-50> 21 pkt.

(50% i więcej) 10 pkt.

Punktacja przypisana do danej cechy Klienta banku wskazuje na ryzyko kredytowe tej osoby, które jest związane z jej zachowaniem w określonym obszarze funkcjonowania kredytowego. Ten obszar jest opisany tą cechą. W naszym przykładzie jest to maksymalne wykorzystywanie dostępnego limitu kredytowego. Z analiz statystycznych wiadomo, że ryzyko kredytowe rośnie wraz ze wzrostem wykorzystania limitu i wiemy też, jak ono wzrasta. Warianty każdej cechy są wyznaczane poprzez grupowanie statystyczne w taki sposób, by odzwierciedlić rzeczywistą zależności pomiędzy poziomem ryzyka a wykorzystaniem limitu. Przy czym oczekuje się, że poszczególne warianty cechy będą różnicowały poziom ryzyka tak, by zachowana była logika biznesowa danej cechy.

Gdy model jest zbudowany poszczególnym cechom i ich wariantom można przypisać odpowiednie punkty. Ponadto punkty przypisuje się statystycznie zgodnie z zasadą, że wraz ze wzrostem ryzyka maleje liczba przyznanych punktów. Przedstawione zasady znajdują odzwierciedlenie w wysokości punktacji przypisanej do danego wariantu cechy.

W ten sposób punktację dla Klienta ustala się dla każdej cechy jaka jest w modelu. Suma punktów przyznanych Klientowi za każdą z cech stanowi jego ocenę scoringową, która **profiluje** tego Klienta z punktu widzenia ryzyka kredytowego.

Tablica scoringowa składa się zazwyczaj z kilku – kilkunastu cech. Przy czym modele scoringowe złożone z kilku tablic scoringowych (nazywamy modelami wielotablicowymi) mogą składać się nawet z kilkudziesięciu cech.

Niezależnie od złożoności modelu każdy model scoringowy ma swój zakres punktacji np. od 200 do 700 punktów. Im niższą ocenę punktową z danego modelu uzyska osoba, tym ma wyższe ryzyko kredytowe.

Zatem do stworzenia profilu konkretnej osoby fizycznej wykorzystujemy już gotowy model scoringowy, dane o kliencie lub jego historii kredytowej. Jednak zanim wykorzystamy ten model musimy go zbudować i ocenić jego jakość. Proces budowy modelu jest procesem związanym z licznymi analizami statystycznymi, które wykonuje się na zbiorach, w których znajdują się informacje opisujące Klientów, w szczególności dotyczące historii kredytowej.

Zgodnie ze standardami zarządzania ryzykiem modeli w bankach, w tym modeli oceny ryzyka kredytowego, wskazanymi przez Komisję Nadzoru Finansowego w *Rekomendacji W dotyczącej zarządzania ryzykiem modeli w bankach* na proces przygotowania danych do budowy modelu składa się:

* określenie celu i założeń budowy modelu oraz wskazanie zakresu jego stosowania wraz z oceną istotności modelu[[1]](#footnote-2),
* analiza rodzaju i zakresu źródeł danych wykorzystanych do budowy modelu, ocena ich jakości (w tym ocena błędnych, odstających lub braków danych) i mechanizmy połączenie danych pochodzących z różnych źródeł,
* weryfikacja czy możliwe jest zapewnienie dostępu do właściwych danych na etapie budowy, stosowania i weryfikacji jakości działania modelu.

Zanim powstanie taki finalny zbiór do analiz statystycznych związanych z budową modelu, wykorzystuje się dane opisane danymi identyfikacyjnymi Klienta, ponieważ niejednokrotnie łączy się dane konkretnej osoby przechowywane w różnych tabelach, zbiorach danych (np. jeśli w tabeli A przechowujemy dane o wieku Klienta, w tabeli B - informacje o jego kredytach, a w tabeli C – informacje o spłacaniu kredytów, to musimy mieć jednoznaczny, unikatowy identyfikator pozwalający na połączenie tabel A, B i C, a w efekcie przypisanie informacji o historii kredytowej właściwej osobie).

Po procesie przygotowania danych do analiz, zbiór taki można zanonimizować, bo do dalszych analiz nie jest ważne, do kogo należą dane. Zatem na etapie budowy modelu nie następuje tutaj ocena wiarygodności kredytowej konkretnej, możliwej do zidentyfikowania osoby. W procesie budowy modelu wykonywane są tylko analizy statystyczne służące do wytworzenia odpowiednich matematycznych, statystycznych lub innych procedur profilowania m. in. eksperckich, ekspercko – statystycznych, które mają zapewnić rzetelność i przejrzystość przetwarzania danych osobowych. Jednocześnie proces budowy modelu ma zapewnić wysoką jakość jego działania. Tak wyliczona ocena punktowa z modelu jest stosowana w procesach bankowych lub udostępniana np. na raportach BIK .

Takie tradycyjne podejście do tworzenia modeli scoringowych w postaci tablicy scoringowej ma m.in. na celu ułatwienie:

* zrozumienia działania modelu również dla osób, które nie były związane z procesem jego budowy, walidacji czy implementacji,
* wyjaśnienia powodów otrzymania przez Klienta niskiej lub wysokiej oceny punktowej w procesie audytu, przed nadzorem czy wyższą kadrą zarządzającą,
* zrozumienia przebiegu procesu budowy takiego modelu, gdyż nie ma on postaci tzw. czarnej skrzynki („black box”),
* procesu badania jakości funkcjonowania modelu,
* ocenę intuicyjności zwracanych przez model oszacowań.

Jednocześnie zarówno banki jak i rejestry kredytowe stosują dobre praktyki rynku bankowego odnośnie konstrukcji i zarządzania modelami statystycznymi, którego ramy wyznaczone są przez m.in. Rekomendację W dotyczącą zarządzania ryzykiem modeli w bankach.

## Załącznik nr 4 - Zakresy informacji przekazywanych Klientowi

Rozporządzenie – Rozporządzenie Parlamentu 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)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Zakres informacji | Pozyskiwanie danych | | Zmiana celu przetwarzania | | Wyjaśnienia / Przykłady |
| Bezpośrednio od osoby, której dane dotyczą | Nie bezpośrednio od osoby, której dane dotyczą | Dane pozyskiwane bezpośrednio od osoby, której dane dotyczą | Dane pozyskiwane nie bezpośrednio od osoby, której dane dotyczą |
| Nazwa, adres, dane kontaktowe banku oraz, gdy ma to zastosowanie – tożsamość i dane kontaktowe swojego przedstawiciela | tak | tak | nie | nie | Jako dane kontaktowe banku można wskazać nr telefonu oraz adres e-mail banku. |
| Dane kontaktowe inspektora ochrony danych | tak | tak | nie | nie | Jako dane kontaktowe inspektora ochrony danych można wskazać nazwę skrzynki mailowej oraz odesłanie do strony internetowej banku (do uznania banku), na której będzie opublikowana informacja dot. imienia, nazwiska, nr telefonu oraz adresu e-mail inspektora ochrony danych. |
| Cele przetwarzania danych, podstawa prawna przetwarzania danych | tak | tak | tak – informacja o celu przetwarzania danych | tak – informacja o celu przetwarzania danych | Przykłady celów przetwarzania danych osobowych wraz ze wskazaniem podstaw prawnych:  - marketing bezpośredni banku oraz podmiotów z grupy kapitałowej (art. 6 ust. 1 lit. a) albo art. 6 ust. 1 lit. f) Rozporządzenia)  - badanie zdolności kredytowej i analizy ryzyka kredytowego (art. 6 ust. 1 lit. b) Rozporządzenia lub art. 6 ust. 1 lit a) Rozporządzenia w przypadku przetwarzania danych po wygaśnięciu zobowiązania)  - zawarcie i wykonanie umowy (art. 6 ust. 1 lit. c) Rozporządzenia)  - statystyka/raportowanie wewnętrzne banku (art. 6 ust. 1 lit. f) Rozporządzenia)  - rozpatrywanie reklamacji (art. 6 ust. 1 lit. b) Rozporządzenia)  - wypełnienie obowiązków wynikających z przepisów prawa, np. Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu, Prawa bankowego) (art. 6 ust. 1 lit. b) Rozporządzenia)  - dochodzenie roszczeń (art. 6 ust. 1 lit. f) Rozporządzenia)  - archiwizacja (art. 6 ust. 1 lit. b) Rozporządzenia) |
| Kategorie odnośnych danych osobowych | tak | tak | nie | nie | - Dane osobiste (imię, nazwisko);  - Dane teleadresowe (adres);  - Dane kontaktowe;  - Dane finansowe;  - Dane dotyczące posiadanych produktów i usług. |
| Prawnie uzasadnione interesy realizowane przez bank / rejestr kredytowy lub stronę trzecią, jeśli przetwarzanie danych odbywa się na podstawie art. 6 ust. 1 lit. f) Rozporządzenia | tak | tak | nie | nie | Przykłady prawnie uzasadnionych interesów realizowanych przez banki / rejestry kredytowe: - przetwarzanie danych z wniosków / zapytań kredytowych w celu oceny zdolności kredytowej:  - ustalenia, dochodzenia roszczeń lub obrony przed roszczeniami  - statystyka/raportowanie wewnętrzne  - budowa i weryfikacja poprawności działania modeli statystycznych  - badanie satysfakcji Klientów  - zapewnienie bezpieczeństwa obrotu gospodarczego  - marketing bezpośredni banku i podmiotów z grupy kapitałowej.  W przypadku przetwarzania danych w celach marketingowych, w tym profilowania, jako prawnie uzasadnionego interesu realizowanego przez bank, informacja ta powinna być podana oddzielnie od wszystkich innych informacji. |
| Odbiorcy danych lub kategorie odbiorców danych, jeśli istnieją | tak | tak | nie | nie | Przykłady kategorii odbiorców danych osobowych:  - organy uprawnione do żądania dostępu do danych osobowych na podstawie art. 105 ust. 1 pkt 2 Prawa bankowego;  - podmioty uprawnione do otrzymania danych osobowych na podstawie art. 104 ust. 2 Prawa bankowego;  - podmioty określone w art. 6a Prawa bankowego (outsourcing);  - instytucje, o których mowa w art. 105 ust. 4 Prawa bankowego (BIK S.A., Bankowy Rejestr w Związku Banków Polskich). |
| Jeśli ma to zastosowanie, informacja 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 Rozporządzenia, o odpowiednich lub właściwych zabezpieczeniach oraz o możliwościach uzyskania kopii danych lub o miejscu udostępnienia danych | tak | tak | nie | nie |  |
| Okres, przez który dane osobowe będą przechowywane, a gdy nie jest to możliwe – kryteriach ustalania tego okresu | tak | tak | tak | tak | Bank może wskazać/odesłać, gdzie znajduje się szczegółowa informacja na temat okresów przechowywania danych osobowych (np. odpowiednia zakładka na stronie internetowej banku lub inny wewnętrzny dokument banku do udostępnienia Klientowi). |
| Informacje o prawie osoby do żądania od banku:  - dostępu do danych osobowych dotyczących osoby, której dane dotyczą  - sprostowania danych  - usunięcia danych  - ograniczenia przetwarzania danych | tak | tak | tak | tak | Bank może wskazać/odesłać, gdzie znajduje się szczegółowa informacja na temat okresów przechowywania danych osobowych (np. odpowiednia zakładka na stronie internetowej banku lub inny wewnętrzny dokument banku do udostępnienia Klientowi). |
| Informacje o prawie do:  - wniesienia sprzeciwu wobec przetwarzania danych  - przenoszenia danych | tak | tak | tak | tak | Bank może wskazać/odesłać, gdzie znajduje się szczegółowa informacja na temat okresów przechowywania danych osobowych (np. odpowiednia zakładka na stronie internetowej banku lub inny wewnętrzny dokument banku do udostępnienia Klientowi). |
| Informacje o prawie do cofnięcia zgody w dowolnym momencie bez wpływu na zgodność z prawem przetwarzania, którego dokonano na podstawie zgody przed jej cofnięciem, jeżeli przetwarzanie odbywa się na podstawie art. 6 ust. 1 lit. a) lub art. 9 ust. 2 lit. a) Rozporządzenia | tak | tak | tak | tak | O prawie do cofnięcia zgody w dowolnym momencie osoba powinna zostać poinformowana przed faktycznym wyrażeniem zgody. |
| Informacje o prawie wniesienia skargi do organu nadzorczego | tak | tak | tak | tak | Bank powinien wskazać nazwę organu nadzorczego ze wskazaniem informacji o prawie wniesienia skargi bądź innego środka w zależności od procedury danego organu nadzorczego. Bank może wskazać dodatkowo dane kontaktowe organu nadzorczego. |
| Informacje, 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 | tak | nie | tak | nie |  |
| Informacje o zautomatyzowanym podejmowaniu decyzji, w tym o profilowaniu, o którym mowa w art. 22 ust. 1 i 4 Rozporządzenia, 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 | tak | tak | tak | tak |  |
| Źródło pochodzenia danych osobowych, a gdy ma to zastosowanie, czy pochodzą one ze źródeł publicznie dostępnych | nie | tak | nie | tak | Przykłady źródeł danych osobowych:  - Biuro Informacji Kredytowej  - biura informacji gospodarczej  - inne banki  - osoba ustanawiająca dyspozycję na wypadek śmierci  - Minister Cyfryzacji (rejestr PESEL)  - podmioty powiązane /zależne  - Krajowy Rejestr Sądowy  - Centralna Ewidencja i Informacja o Działalności Gospodarczej  - MSiG,  - KRS |

## Załącznik nr 5 - Przykładowe postanowienia umów zawieranych z podmiotami przetwarzającymi

Umowa jest umową powierzenia przetwarzania danych osobowych w rozumieniu art. 28 Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) zwanej dalej RODO.

Zamawiający oświadcza, że jest administratorem danych osobowych w postaci……………………… powierzonych do przetwarzania Wykonawcy. Wykonawca będzie przetwarzał dane osobowe powierzone do przetwarzania wyłącznie w celu wykonania Umowy, w niezbędnym do tego zakresie (umowa nie narusza obowiązków wynikających z przepisów prawa Unii lub prawa państwa członkowskiego, któremu podlega Wykonawca). Udokumentowane polecenie może stanowić umowa, a w przypadku gdy przetwarzanie odbywa się w cyklu ciągłym każdorazowe polecenie musi zostać zarejestrowane i może być przekazane w formie pisemnej, w tym elektronicznej.

Wykonawca zastosuje środki organizacyjne i techniczne zabezpieczające powierzone dane osobowe przed niepożądanym ujawnieniem, zniszczeniem lub modyfikacją w zakresie przewidzianym w art. 32 RODO. Wykonawca oświadcza że stosuje kodeks postępowania lub mechanizmy certyfikacji opisane w art. 40 i 42 RODO, lub w inny sposób może udokumentować gwarancje wdrożenia tych środków.

Wykonawca będzie prowadził rejestr wszystkich kategorii czynności przetwarzania dokonywanych w imieniu Zamawiającego, zawierający informacje wskazane w art. 30 RODO i na zasadach tam określonych. Wykonawca zobowiązuje się do udostępniania rejestru na żądanie organu nadzorczego.

Wykonawca zobowiązuje się zachować w tajemnicy wszelkie informacje i dane osobowe, do których będzie miał dostęp w związku z wykonywaniem Umowy.

W przypadku stwierdzenia jakiejkolwiek sytuacji stanowiącej naruszenie bezpieczeństwa danych osobowych powierzonych do przetwarzania Wykonawca po stwierdzeniu naruszenia ochrony danych osobowych zobowiązany jest niezwłocznie, nie później jednak niż w ciągu 24 godzin:

- poinformować o tym Zamawiającego, podając wszelkie informacje dotyczące takiego naruszenia,

- ustalić przyczynę naruszenia,

- podjąć niezwłocznie wszelkie czynności mające na celu usunięcia naruszenia i zabezpieczenie danych osobowych w sposób należyty przed dalszymi naruszeniami,

- zebrać wszystkie możliwe dane i dokumenty, które mogą pomóc w ustaleniu okoliczności naruszenia i przeciwdziałaniu podobnym naruszeniom w przyszłości i w tym celu współpracuje z Zamawiającym na każdym etapie wyjaśniania sprawy.

Zamawiającemu przysługuje prawo kontrolowania sposobu przetwarzania powierzonych danych po uprzednim poinformowaniu o kontroli co najmniej 7 dni roboczych przed jej rozpoczęciem lub niezwłocznie w przypadku wystąpienia naruszenia. Kontrola może być wykonywana przez osoby imiennie wyznaczone przez Zamawiającego w dni robocze w miejscach przetwarzania danych. Osoby wyznaczone przez Zamawiającego są uprawnione do wstępu do pomieszczeń, w których przetwarzane są dane oraz do wglądu do danych powierzonych do przetwarzania, jak również do żądania od Wykonawcy udzielania informacji dotyczących przebiegu przetwarzania danych osobowych, oraz udostępnienia rejestrów przetwarzania.

W przypadku rozwiązania Umowy Wykonawca nie ma prawa przetwarzać powierzonych danych osobowych na podstawie Umowy i jest zobowiązany zgodnie z żądaniem banku lub rejestru kredytowego zwrócić te dane bankowi lub rejestrowi kredytowemu lub usunąć dane wraz z istniejącymi kopiami pod rygorem naprawienia wszelkich szkód związanych z ich naruszeniem. Protokół ze zniszczenia lub usunięcia danych osobowych Wykonawca zobowiązany jest dostarczyć Zamawiającemu w ciągu 10 dni roboczych od daty rozwiązania Umowy.

Wykonawca nie może powierzyć czynności przetwarzania danych osobowych określonych niniejszą umową innym osobom lub podmiotom, bez uprzedniej pisemnej lub elektronicznej zgody Zamawiającego.

Wykonawca służy pomocą Zamawiającemu w wywiązywaniu się z obowiązku odpowiadania na żądania osoby, której dane dotyczą, oraz z obowiązków określonych w art. 32-36 RODO.

**Dodatkowe, przykładowe postanowienia niewymagane przez art. 28 RODO:**

Wykonawca będzie prowadził ewidencję osób zatrudnionych przez Wykonawcę przy przetwarzaniu danych. Osoby zatrudnione przez Wykonawcę zostaną zobowiązane przez Wykonawcę do zachowania w tajemnicy wszelkich informacji uzyskanych w związku z przetwarzaniem danych osobowych. Na żądanie Zamawiającego Wykonawca potwierdzi w formie pisemnej lub innej wskazanej wykonanie powyższych obowiązków.

W przypadku nałożenia na Zamawiającego prawomocnej kary, za niezgodne z prawem przetwarzanie danych osobowych zawinione przez Wykonawcę, poniesie on wobec Zamawiającego odpowiedzialność w pełnej wysokości.

# **Załącznik nr 6 – Przykłady zautomatyzowanego przetwarzania danych**

### Zautomatyzowane przetwarzanie danych osobowych na poziomie wybranego portfela kredytowego lub całego portfela banku w celu dostarczenia analiz statystycznych bankom i innym instytucjom odpowiedzialnym za zapewnienie stabilności finansowej

1. Jednym z istotnych elementów ustalania przez banki zasad zarządzania ryzykiem kredytowym (niezbędnych do obniżania ryzyka kredytowego) jest uwzględnianie informacji dostarczanych przez rejestry kredytowe.
2. Zarządzanie ryzykiem kredytowym przez banki może być realizowane na kilku poziomach:
3. poziomie Klienta,
4. poziomie wybranego portfela kredytowego lub całego portfela banku również w odniesieniu do całego sektora,
5. poziomie całego rynku lub sektora.
6. Banki wykorzystują informacje z rejestrów kredytowych w postaci zagregowanych analiz statystycznych w celu określenia pozycji banku na tle całego sektora:
7. na poziomie wybranych portfeli, lub
8. na poziomie całego portfela kredytowego banku.
9. Zapewnienie wysokiej jakości i skuteczności procesów kredytowych wymaga przez banki przetwarzania informacji uwzględniających cykliczność procesów ekonomicznych i zmiany zachodzące w portfelach. W tym celu konieczne jest by banki i rejestry kredytowe dysponowały dostępem do danych o adekwatnej długości szeregów czasowych.

1. Analizy statystyczne dostarczane bankom przez rejestry kredytowe obejmują m. in. takie informacje jak:
   1. jakość udzielonych kredytów w banku w określonym czasie vs jakość kredytów udzielonych na całym rynku w tym okresie,
   2. jakość portfela kredytowego banku ogółem oraz w podziale na różne kryteria np. obszar geograficzny, typ produktu, cechy produktu – kwota, waluta, okres kredytowania,
   3. jakość obsługi zadłużenia przez Klientów banku w tym banku oraz na całym rynku,
   4. łączne zadłużenie Klientów banku w tym banku vs ich zadłużenie w pozostałych bankach,
   5. prognozowane ryzyko kredytowe wskazanych portfeli kredytowych,
   6. jakość portfela kredytowego w zależności od kwoty zaciągniętego zobowiązania.

### Zautomatyzowane przetwarzanie danych osobowych w celu budowy modelu oceny punktowej (scoringowego) rejestru kredytowego

1. W procesie oceny ryzyka kredytowego banki wykorzystują modele scoringowe, które zostały zbudowane w sposób zapewniający wysoką jakość tych modeli. Jeśli modele nie spełniają odpowiednich wymagań jakościowych (m.in. wymagań zawartych w Rekomendacji W Komisji Nadzoru Finansowego dotyczącej zarządzania ryzykiem modeli w bankach), nie są stosowane do oceny ryzyka kredytowego konkretnej osoby. W procesie budowy modelu nie ma miejsca ocena zdolności kredytowej konkretnej, możliwej do zidentyfikowania osoby, ani nie następuje jakakolwiek analiza lub prognoza aspektów dotyczących sytuacji (ekonomicznej, zdrowia, preferencji, zachowań, wiarygodności) konkretnej osoby fizycznej. Wykonywane są wyłącznie analizy statystyczne będące wynikiem zautomatyzowanego przetwarzania danych, które mają doprowadzić w finalnym efekcie do stworzenia modelu, a więc mechanizmu, który może (nie musi) być wykorzystany do naliczania ocen scoringowych.
2. Proces budowy modelu scoringowego jest procesem wieloetapowym i związanym z licznymi analizami statystycznymi wykonywanymi na zbiorach danych, w których znajdują się m.in. dane osobowe Klientów i informacje opisujące ich zachowania kredytowe, w szczególności informacje dotyczące historii spłat czy zmian w poziomie zadłużenia. Przed przystąpieniem do modelowania określany jest obszar, zakres oraz cel modelowania.
3. Pierwszym etapem budowy modelu jest przygotowanie finalnego zbioru danych do analizy, który ma zapewnić, że model budowany jest na podstawie danych o wysokiej jakości. Zanim powstanie taki finalny zbiór do analiz statystycznych związanych z budową modelu, wykorzystuje się dane opisane danymi identyfikacyjnymi Klienta, ponieważ niejednokrotnie łączy się dane konkretnej osoby przechowywane w różnych tabelach.
4. Na etapie przygotowania zbioru danych do budowy modelu badana jest w szczególności jakość i zakres danych oraz określana długość szeregów czasowych danych niezbędnych do tego, by model uwzględniał istotne czynniki wpływające na kształtowanie modelowanego zjawiska.
5. Po przygotowaniu zbioru danych osobowych do analiz, zbiór taki może zostać pozbawiony cech umożliwiających zidentyfikowanie osoby, do której dane należą, ponieważ z punktu widzenia dalszych analiz nie jest istotne do jakiej osoby należą dane poddawane analizie. W czasie budowy modelu dokonywana jest również ocena modeli, kalibracja, ocena istotności modelu.

### 

### Zautomatyzowane przetwarzanie danych osobowych w celu stosowania przez banki metod wewnętrznych oraz innych metod i modeli, o których mowa w części trzeciej [Rozporządzenia](https://sip.lex.pl/#/dokument/68336066) Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Rozporządzenie 575/2013).

1. Z Rozporządzenia 575/2013 wynika, że zasady oceny ryzyka kredytowego Klienta w procesie udzielania finansowania, jak i zasady ustalenia wymogu kapitałowego banku powinny być tożsame.
2. Ocena zdolności kredytowej i analizy ryzyka kredytowego w oparciu o model statystyczny pozwala następnie sklasyfikować kredytobiorców do jednorodnych portfeli ze względu na charakter i poziom ryzyka oraz rodzaj zabezpieczenia, co w konsekwencji przekłada się na możliwość zbudowania modelu dla banku stosującego metody wewnętrzne, o których mowa w Rozdziale 3 Rozporządzenia 575/2013. Jeżeli bank stosuje model statystyczny (scoringowy) to ten sam model powinien być wykorzystywany w procesie udzielania kredytów (naliczanie oceny punktowej Klientom ubiegającym się o kredyt) oraz w procesie ustalania wymogu kapitałowego.
3. Banki wybierają modele statystyczne do kwantyfikacji ryzyka kredytowego, gdyż są obiektywne, spójne dla wszystkich procesów i spełniają wymogi ścisłej kontroli w banku, zgodnie z Rozporządzeniem 575/2013.
4. Jednym z podstawowych wymogów uzyskania przez bank zgody nadzoru bankowego na stosowanie metod wewnętrznych jest zapewnienie, że dane przetwarzane, również w sposób zautomatyzowany, na potrzeby modeli statystycznych są odpowiednie, aby zapewnić skuteczne wsparcie procesów pomiaru ryzyka kredytowego oraz zarządzania ryzykiem kredytowym.
5. W przypadku budowy modeli statystycznych odpowiedniość danych oznacza, że bank gromadzi i przetwarza dane w szerokim zakresie z uwzględnieniem m.in.:
   * długich horyzontów czasowych obejmujących zmiany w procesach biznesowych oraz otoczeniu ekonomicznym i prawnym banku,
   * reprezentatywności danych dla poszczególnych portfeli banku, tak by dane były spójne w długim okresie,
   * wystarczającej liczebności i zakresie danych zapewniających skuteczne wsparcie procesów pomiaru ryzyka kredytowego oraz zarządzania ryzykiem kredytowym, w szczególności w odniesieniu do przypadków niewykonania zobowiązania przez Klientów.
6. Jednakże należy podkreślić, że nie wszystkie banki posiadają odpowiedni – co do liczebności i zakresu oraz jakości – zbiór poprawnych, kompletnych i reprezentatywnych dla danego portfela Klientów danych, w szczególności w odniesieniu do danych historycznych dotyczących osoby fizycznej i jej zobowiązania (w tym danych po wygaśnięciu zobowiązania), tak by zapewnić, że stosowane modele statystyczne charakteryzują się wysoką precyzją, dokładnością i stabilnością działania w długim horyzoncie czasowym.
7. Ponadto rejestry kredytowe wspierają banki, jako zewnętrzni dostawcy produktów, m.in. budując indeksy i modele statystyczne oceniające ryzyko kredytowe z punktu widzenia całego polskiego sektora bankowego. Modele te wykorzystują dane dotyczące wszystkich kredytobiorców zgromadzonych w bazach banków, bo tylko w oparciu o takie zbiorcze informacje model oceny statystycznej może być zbudowany poprawnie i osiągać optymalną efektywność. Ponieważ modele budowane przez rejestry kredytowe oceniają szerszą populację Klientów niż modele zbudowane z perspektywy pojedynczego banku, dlatego stanowią istotną wartość stabilizującą działanie wewnętrznych modeli banku.

1. Istotność modelu – cecha modelu, która jest określana przez bank z uwzględnieniem co najmniej istotności procesu, w ramach którego używany jest modeli roli modelu w tym procesie oraz wielkości ekspozycji objętej działaniem modelu (Rekomendacja W). [↑](#footnote-ref-2)