06.04.2023
3.2.0/30289
00000165666

ZWIĄZEK BANKÓW POLSKICH

DR TADEUSZ BIAŁEK
WICEPREZES

Warszawa, 5 kwietnia 2023 r.

Państwo
Prezesi Zarządów Banków
Członków Związku Banków Polskich

Szanowni Państwo,

w nawiązaniu do prowadzonych w Związku Banków Polskich prac w obszarze ochrony danych osobowych z uwzględnieniem specyfiki sektora bankowego, w załączeniu przesyłam dokument: ***Zasady dobrych praktyk w zakresie przetwarzania i ochrony danych osobowych w sektorze bankowym („Zasady")***.

Załączone Zasady zostały wypracowane w Grupie Roboczej ZBP „Bankowy IOD" z udziałem Przedstawicieli Banków – Członków ZBP. Ideą, która przyświecała pracom było opracowanie wyczerpującego sektorowego dokumentu poświęconego uspójnieniu praktyki stosowania zasad ochrony danych osobowych w bankach.

Zasady dotyczą przetwarzania i ochrony danych osobowych w polskim sektorze bankowym przez banki i rejestry kredytowe. Celem dokumentu jest możliwie przystępne wyjaśnienie pracownikom Banków, jak również klientkom i klientom jaki sposób przetwarzane i chronione są dane osobowe. W Zasadach omówiono między innymi: podstawowe zasady dotyczące przetwarzania danych osobowych, podstawy prawne przetwarzania danych, prawa osób, których dane dotyczą oraz obowiązki administratora, zasady przechowywania i usuwania danych, profilowanie oraz zautomatyzowane podejmowanie decyzji, naruszenie ochrony danych osobowych, bezpieczeństwo danych osobowych klientów.

Wyrażam nadzieję, że przekazany dokument będzie stanowić dla Państwa pomocne narzędzie wykorzystywane w przetwarzaniu danych osobowych oraz że pomoże on zrozumieć klientom obowiązki administratorów oraz prawa, które przysługują osobom korzystającym z usług Banków i rejestrów kredytowych.

Jako Związek Banków Polskich zobowiązujemy się do podjęcia działań mających na celu rozpowszechnienie Zasad dobrych praktyk w zakresie przetwarzania i ochrony danych osobowych w sektorze bankowym. Chcemy, aby rekomendacje wynikające z tego dokumentu były powszechnie znane przedstawicielom sektora, ale również odpowiednim organom administracji publicznej oraz samym klientom Banków.

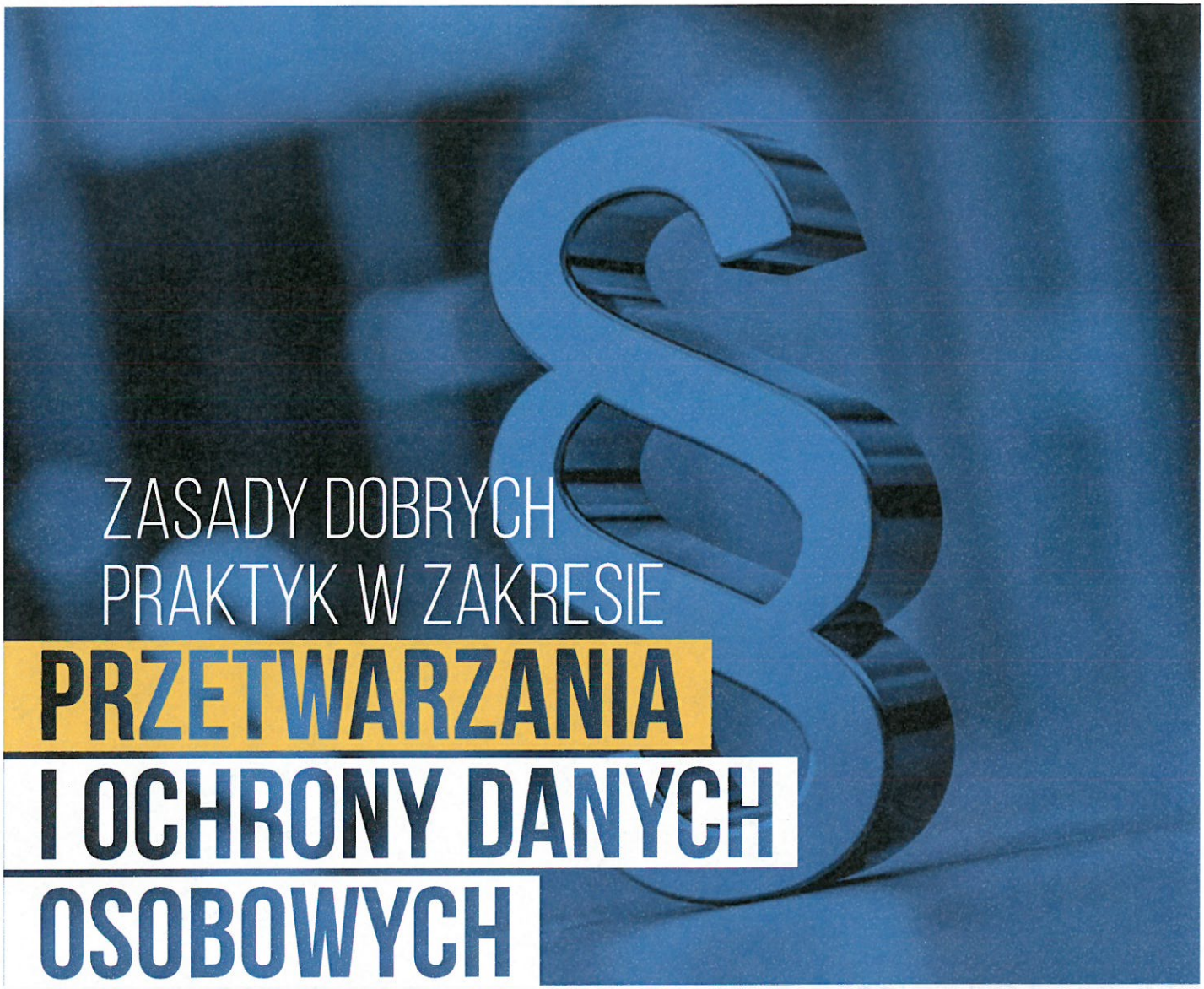
Z poważaniem

WICEPREZES ZWIĄZKU
DR TADEUSZ BIAŁEK

Załącznik:

Zasady dobrych praktyk w zakresie przetwarzania i ochrony danych osobowych w sektorze bankowym.

ul. Kruczkowskiego 8, 00-380 Warszawa, tel.: 22 48 68 113, e-mail: tadeusz.bialek@zbp.pl



ZASADY DOBRYCH PRAKTYK W ZAKRESIE PRZETWARZANIA I OCHRONY DANYCH OSOBOWYCH W SEKTORZE BANKOWYM

ZWIĄZEK BANKÓW POLSKICH

opracowane przez Grupę Roboczą
przy Związku Banków Polskich "Bankowy IOD"

ZASADY DOBRYCH PRAKTYK

w zakresie

przetwarzania i ochrony danych osobowych w sektorze bankowym

Marzec 2023 r.

WPROWADZENIE

Niniejsze Zasady dotyczą przetwarzania i ochrony danych osobowych w polskim sektorze bankowym przez banki i rejestry kredytowe.

Celem Zasad jest możliwie przystępne wyjaśnienie klientkom i klientom oraz osobom korzystającym z usług tych instytucji w innym charakterze – w jaki sposób przetwarzane i chronione są ich dane osobowe.

Zachęcamy do lektury Zasad i liczymy, że pomogą one zrozumieć obowiązki administratorów oraz prawa, które przysługują osobom korzystającym z usług rejestrów kredytowych i banków.

SPIS TREŚCI

I. PODSTAWOWE INFORMACJE O PRZETWARZANIU DANYCH OSOBOWYCH

1. SŁOWNIK POJĘĆ

ADMINISTRATOR Podmiot, który (samodzielnie lub wspólnie z innym administratorem) ustala, jak i w jakich celach będzie przetwarzać dane osobowe klientów. Administratorem danych osobowych klientów jest bank lub rejestr kredytowy. Jeśli w Rekomendacji użyte jest słowo „administrator" – oznacza ono bank lub rejestr kredytowy.

BANK Osoba prawna utworzona zgodnie z przepisami ustaw, działająca na podstawie zezwoleń uprawniających do wykonywania czynności bankowych obciążających ryzykiem środki powierzone pod jakimkolwiek tytułem zwrotnym.

DANE OSOBOWE LUB DANE Wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej, np.:

- imiona i nazwisko,
- PESEL,
- e-mail,
- numer dokumentu tożsamości.

KLIENT Osoba fizyczna, która korzystała, korzysta lub zamierza skorzystać z usług administratora lub której dane osobowe administrator przetwarza w związku ze swoją działalnością, obowiązkami oraz uprawnieniami wynikającymi z przepisów prawa i aktów wewnętrznych (np. umów lub regulaminów), jak między innymi pełnomocnik klienta, jego reprezentant, przedstawiciel, osoba uposażona, spadkobierca czy beneficjent rzeczywisty.

PROCESOR Podmiot, który przetwarza dane osobowe w imieniu i na zlecenie administratora (w przepisach RODO nazwany podmiotem przetwarzającym).

PRAWO BANKOWE Ustawa z 29 sierpnia 1997 r. Prawo bankowe.

REJESTR KREDYTOWY Instytucja utworzona na podstawie art. 105 ust. 4 Prawa bankowego, w szczególności:

- Biuro Informacji Kredytowej S.A.,
- System Bankowy Rejestr prowadzony przez Związek Banków Polskich.

RODO Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 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) (Dz. Urz. UE L 119 z 4 maja 2016 r. wraz z późniejszym sprostowaniem).

2. ZASADY DOTYCZĄCE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator przetwarza dane osobowe zgodnie z zasadami określonymi w RODO. Te zasady to:

ZASADA **LEGALNOŚCI**

dane osobowe należy przetwarzać zgodnie z prawem,

ZASADA **RZETELNOŚCI**

dane osobowe powinno się przetwarzać w sposób staranny, uczciwy i etyczny,

ZASADA **PRZEJRZYSTOŚCI**

informacje o przetwarzaniu danych oraz o jego konsekwencjach powinno się przekazywać w sposób wyczerpujący i przystępny,

ZASADA **CELOWOŚCI**

dane osobowe można zbierać tylko w konkretnych, wyraźnych i prawnie uzasadnionych celach oraz nie można przetwarzać ich niezgodnie z tymi celami,

ZASADA **ROZLICZALNOŚCI**

administrator powinien móc wykazać, że wdrożył i przestrzega wszystkich wyżej wymienionych zasad,

ZASADA **PRAWIDŁOWOŚCI**

należy dbać o to, aby dane osobowe były aktualne oraz w uzasadnionych przypadkach poprawiane lub usuwane,

ZASADA **MINIMALIZACJI DANYCH**

zakres danych osobowych powinien być adekwatny i stosowny do realizacji celów, dla których dane są przetwarzane oraz ograniczony do tego, co niezbędne do ich realizacji,

ZASADA **OGRANICZENIA PRZECHOWYWANIA DANYCH**

dane osobowe można przetwarzać tylko tak długo, jak jest to niezbędne, by zrealizować cel przetwarzania,

ZASADA **INTEGRALNOŚCI I POUFNOŚCI DANYCH**

dane osobowe powinny być odpowiednio zabezpieczone przed przypadkową utratą, bezprawnym ujawnieniem, zniszczeniem, zmianą lub uszkodzeniem.

3. PODSTAWY PRAWNE PRZETWARZANIA DANYCH

1. Administrator może przetwarzać dane klientów, jeżeli wykaże co najmniej jedną z podstaw prawnych wskazanych w RODO, tj. gdy:

- klient się na to zgodzi,
- dane są niezbędne, aby:
  - realizować umowę, której stroną jest klient,
  - podjąć działania na żądanie klienta, przed zawarciem umowy (np. rozpatrzenie wniosku kredytowego o produkt lub usługę administratora),
- dane są niezbędne, aby realizować obowiązek prawny administratora wynikający z innych przepisów, między innymi wymienionych w rozdz. III ust. 2 (np. do przeprowadzenia oceny zdolności kredytowej; zidentyfikowania osób, na rzecz których będą prowadzone rachunki bankowe; zrealizowania obowiązków związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu),
- dane są niezbędne do ochrony żywotnych interesów klienta lub innej osoby (np. w celu ratowania życia lub zdrowia klienta w związku z wypadkiem w placówce administratora),
- dane są niezbędne, aby wykonywać zadania w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi,
- dane są niezbędne, aby administrator mógł realizować swoje prawnie uzasadnione interesy, pod warunkiem, że interesy lub podstawowe prawa i wolności klienta, wymagające ochrony danych osobowych, nie mają nadrzędnego charakteru wobec tych prawnie uzasadnionych interesów administratora. Administratorzy mogą oprzeć się na tej podstawie, np. gdy chcą zabezpieczyć swoje interesy na wypadek roszczeń, które mogą wynikać ze świadczonych usług, zapewnić bezpieczeństwo informatyczne i marketing usług.

2. W zależności od celów przetwarzania i rodzaju danych osobowych, administrator stosuje właściwe podstawy przetwarzania. Administrator może w określonych okolicznościach przetwarzać:

- szczególne kategorie danych (tzw. dane wrażliwe), między innymi o stanie zdrowia klienta, aby przygotować kanały jego obsługi, np. po udzieleniu przez klienta wyraźnej zgody oraz
- dane dotyczące wyroków skazujących i czynów zabronionych (np. przekazane z inicjatywy klienta o jego pobycie w areszcie lub zakładzie karnym w związku z popełnieniem konkretnego przestępstwa i wnioskiem o wstrzymanie windykacji).

4. ZGODA NA PRZETWARZANIE DANYCH

1. **Administrator pozyskuje zgodę klienta na przetwarzanie jego danych osobowych – gdy nie ma innej podstawy prawnej do przetwarzania danych.**

2. **Aby zgoda klienta była prawidłowa, powinna być:**

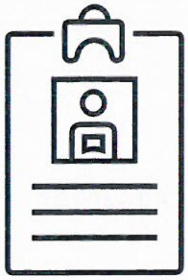
DOBROWOLNA	ŚWIADOMA	KONKRETNA	WYRAŻONA
klient powinien mieć możliwość swobodnego udzielenia zgody i możliwość jej wycofania bez niekorzystnych dla niego konsekwencji	klient powinien zostać poinformowany o tym, czego zgoda dotyczy i jakie są jej konsekwencje	treść zgody powinna określać jednoznaczny cel przetwarzania danych osobowych	przez aktywne działanie lub oświadczenie (tj. jednoznaczne okazanie swojej woli, np. kliknięcie „zgadzam się" w aplikacji mobilnej)

3. **Klient przed wyrażeniem zgody, powinien otrzymać:**

- informację, że może wycofać zgodę w dowolnym momencie (wycofanie zgody nie wpływa jednak na zgodność z prawem wcześniejszego przetwarzania na jej podstawie),
- informacje zgodnie z rozdz. II ust. 2, w tym kto jest administratorem, w jakim celu przetwarza dane klienta – mogą być przekazane w formie np. rozwijalnego tekstu.

4. **Treść oświadczenia o wyrażeniu zgody powinna być przedstawiona:**

W SPOSÓB, KTÓRY WYRAŹNIE ODRÓŻNIA SIĘ OD POZOSTAŁYCH KWESTII	W ZROZUMIAŁEJ I ŁATWO DOSTĘPNEJ FORMIE, JASNYM I PROSTYM JĘZYKIEM



II. PRAWA OSÓB, KTÓRYCH DANE DOTYCZĄ ORAZ OBOWIĄZKI ADMINISTRATORA

1. PRAWA KLIENTA

1. Każdy klient, na zasadach określonych w art. 15-22 RODO, ma przede wszystkim prawo do:

- dostępu do swoich danych, w tym otrzymania kopii swoich danych,
- sprostowania i uzupełnienia swoich danych,
- żądania usunięcia swoich danych,
- żądania ograniczenia przetwarzania swoich danych,
- przenoszenia swoich danych,
- sprzeciwienia się dalszemu przetwarzaniu swoich danych,
- niepodlegania decyzjom, które mogłyby wywołać dla klienta poważne skutki o znacznym wpływie, opartym wyłącznie na zautomatyzowanym przetwarzaniu dotyczących go danych.

2. OBOWIĄZEK INFORMACYJNY

1. Gdy administrator zbiera dane bezpośrednio od klienta, powinien mu przekazać poniższe informacje:

- **dane administratora** – nazwa i adres administratora, który przetwarza dane oraz swoje dane kontaktowe,
- **dane inspektora ochrony danych** – każdy bank lub rejestr kredytowy musi go wyznaczyć,
- **cele i podstawy przetwarzania danych** – po co administrator przetwarza dane i jaki przepis prawa na to pozwala,
- **informacje o prawnie uzasadnionych interesach przetwarzania danych** – czyli sytuacjach, w których zadania związane z działalnością banku lub rejestru kredytowego wymagają przetwarzania danych, a nie wynikają one z realizacji obowiązku prawnego lub wykonania zobowiązań umownych wynikających z umowy zawartej z klientem (np. prowadzenie działań marketingowych, dochodzenie roszczeń lub obrona przed nimi),
- **o odbiorcach danych (lub ich kategoriach)** – np. konkretny podmiot, któremu administrator przekazuje dane lub rodzaje takich podmiotów (między innymi firmy kurierskie, biura księgowe, rejestry kredytowe, firmy informatyczne),
- czy administrator zamierza przekazać lub przekazuje dane osobowe do państwa trzeciego lub organizacji międzynarodowej (np. SWIFT),
- jak długo administrator przechowuje dane (może tu być wskazany konkretny przepis prawa, który określa termin przetwarzania danych osobowych),
- jakie prawa ma klient (prawa określone są w ust. 1 niniejszego rozdziału),
- o możliwości wycofania zgody w dowolnym momencie (jeśli zgoda jest podstawą przetwarzania),
- o możliwości wniesienia skargi do organu nadzorczego zajmującego się ochroną danych (w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych),
- czy podanie danych jest obowiązkowe (np. bez nich administrator nie zawrze umowy) oraz co się stanie, jeśli klient nie poda danych,
- czy przetwarzanie danych obejmuje podejmowanie decyzji z użyciem danych klienta w sposób wyłącznie zautomatyzowany, a decyzja mogłyby wywołać dla klienta poważne skutki o znacznym wpływie (jeśli w ogóle ma to miejsce),
- o fakcie i konsekwencjach profilowania klienta.

2. Administrator może przekazać informacje o przetwarzaniu danych osobowych w dowolnej formie, np.:

Niezależnie od powyższego, wszystkie wymagane informacje o przetwarzaniu danych osobowych administrator może publikować na swoich stronach internetowych.

3. **Bank przekazuje klientowi informacje o przetwarzaniu danych osobowych przez rejestr kredytowy, w sytuacji, gdy zbierane przez bank dane będą przekazywane przez bank do rejestru kredytowego.**

4. **Jeżeli klient otrzymał już wymagane informacje o sposobie i celach przetwarzania dotyczących go danych osobowych, administrator nie musi ponownie przekazywać tych samych informacji.**

5. **Jeśli administrator pozyskuje dane z innego źródła niż od klienta, poza informacjami opisanymi w pkt 1, podaje dodatkowe informacje:**

- o kategoriach danych osobowych, które przetwarza (np. dane teleadresowe, identyfikacyjne),
- o źródle, z którego pozyskał dane (np. rejestry gospodarcze, CEIDG, osoba udzielająca pełnomocnictwa).

6. **Jeśli administrator pozyskuje dane w inny sposób niż bezpośrednio od klienta (z innego źródła), informacje o przetwarzaniu danych osobowych powinien przekazać mu:**

W ROZSĄDNYM TERMINIE	NAJPÓŹNIEJ PRZY PIERWSZEJ KOMUNIKACJI	NAJPÓŹNIEJ PRZY ICH PIERWSZYM UJAWNIENIU
– nie później niż w ciągu miesiąca od pozyskania danych osobowych,	– jeśli administrator chce korzystać z danych w komunikacji z klientem,	– jeżeli planuje się ujawnić dane osobowe innemu odbiorcy.

3. WERYFIKACJA TOŻSAMOŚCI I KOMUNIKACJA Z KLIENTEM

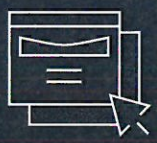
1. **Administrator, gdy ma uzasadnione wątpliwości co do tożsamości osoby, która składa żądanie dotyczące danych osobowych, może wymagać dodatkowych informacji niezbędnych do potwierdzenia jej tożsamości. Ze względu na ryzyko związane z dostępem do danych objętych tajemnicą bankową, potwierdzenie tożsamości może być bardziej wymagające niż w przypadku innych, standardowych usług.**

2. Komunikację w sprawie przetwarzania danych administrator prowadzi:

ZWIĘŹLE I PRZEJRZYŚCIE	W ZROZUMIAŁEJ I ŁATWO DOSTĘPNEJ FORMIE	JASNYM I PROSTYM JĘZYKIEM

3. Informacje o przetwarzaniu danych, w tym w zakresie obowiązku informacyjnego, administrator może podawać „warstwowo" – np. poprzez możliwość bezpośredniego przejścia kliknięciem z pierwszej warstwy informacji do dalszego tekstu, w którym zamieszczono ich pełną treść.

4. Administrator może komunikować się w sprawie przetwarzania danych różnymi kanałami. Może to robić, między innymi:

 E-MAILEM	 SMS-EM	 TELEFONICZNIE
 POPRZEZ APLIKACJE MOBILNE	 LISTOWNIE	 ZA POŚREDNICTWEM STRON INTERNETOWYCH

5. Przekazywanie klientowi informacji dotyczących przetwarzania danych osobowych oraz związana z nimi komunikacja i działania administratora są co do zasady bezpłatne. Wyjątki od tej zasady mogą wynikać z wewnętrznych aktów administratora (jak regulaminy czy cenniki) lub mieć swoje źródło bezpośrednio w przepisach prawa (np. w sytuacji określonej w ust. 4 pkt 4 niniejszego rozdziału).

4. ZASADY REALIZACJI ŻĄDAŃ OPARTYCH O PRAWA OKREŚLONE W ROZDZ. II, UST. 1

1. **Administrator – zgodnie z ust. 3 pkt 1 niniejszego rozdziału – nie zrealizuje żądania, jeżeli będzie posiadał uzasadnione wątpliwości co do tożsamości osoby, która je składa.**

2. **Administrator możliwie szybko – nie później niż w ciągu miesiąca od kiedy klient złoży żądanie oparte o prawa określone w ust. 1 niniejszego rozdziału – powinien udzielić mu informacji o działaniach podjętych w związku ze sprawą.**

3. **Termin realizacji żądania może wydłużyć się o dwa miesiące (np. jeśli żądanie ma skomplikowany charakter lub ze względu na liczbę żądań). W takiej sytuacji maksymalnie w ciągu miesiąca od dnia, w którym klient złożył żądanie, administrator powinien powiadomić go o wydłużeniu terminu oraz o przyczynie opóźnienia.**

4. **Realizacja żądań klienta złożonych przez niego w oparciu o prawa określone w ust. 1 niniejszego rozdziału – jest co do zasady wolna od opłat. Jeśli żądania klienta w zakresie, o którym mowa w zdaniu powyżej, są ewidentnie nieuzasadnione lub nadmierne (np. ciągle się powtarzają), administrator może:**

- pobrać rozsądną opłatę, której wysokość będzie uwzględniać administracyjne koszty udzielenia informacji, prowadzenia komunikacji lub podjęcia żądanych działań,
- ewentualnie – odmówić podjęcia działań w związku z żądaniem.

5. **Jeżeli administrator nie podejmuje działań w związku z żądaniem klienta, to w ciągu miesiąca, od kiedy otrzyma żądanie, powinien powiadomić klienta**

- z jakiego powodu nie podejmuje żadnych działań,
- że klient może wnieść skargę do organu nadzorczego zajmującego się ochroną danych (w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych) oraz skierować sprawę na drogę sądową.

5. PRAWO DOSTĘPU DO DANYCH

1. Klient ma prawo dostać od administratora potwierdzenie, czy przetwarzane są jego dane. Jeśli tak, ma prawo uzyskania dostępu do swoich danych.

2. W ramach prawa dostępu klient powinien dostać od administratora:

- potwierdzenie, czy jego dane są przetwarzane, czy nie,
- dostęp do informacji o przetwarzaniu, przede wszystkim:
  - w jakim celu dane są przetwarzane,
  - jakie dane są przetwarzane,
  - komu te dane mogą zostać przekazane,
  - jak długo administrator może przechowywać dane,
  - jakie prawa ma klient,
  - informację, że może wnieść skargę do organu nadzorczego zajmującego się ochroną danych (w Polsce jest nim Prezes Urzędu Ochrony Danych Osobowych),
  - jeżeli dane osobowe nie zostały zebrane od klienta – informacje o źródle ich pozyskania,
  - czy administrator stosuje zautomatyzowane podejmowanie decyzji, o którym mowa w art. 22 ust. 1 i 4 RODO (jeśli tak, administrator poda określone dodatkowe informacje z tym związane),
- jeśli administrator przekazuje dane klienta do państw trzecich lub organizacji międzynarodowych – klient dodatkowo powinien dostać informację o odpowiednich zabezpieczeniach, o których mowa w RODO, związanych z przekazaniem danych.

3. Administrator – w ramach prawa dostępu, o którym mowa w pkt 1 – nie jest zobowiązany udostępnić klientowi takich informacji i dokumentów, jak np.:

- oryginalny nośnik informacji (np. zrzut ekranu z systemów, treść maila, formularz
- kopie zawartych umów, opinii bankowych oraz zaświadczeń o niezaleganiu z płatnością zobowiązań wobec banku
- nagrania rozmów telefonicznych oraz kopii raportów udostępnionych bezpośrednio klientowi
- informacje, które są dostępne publicznie, np. w rejestrach CEIDG lub KRS

4. **Administrator dostarcza klientowi kopię danych, które przetwarza (np. poprzez sporządzenie kopii lub odpisu nośnika (np. umowy) zawierającego dane osobowe lub poprzez podanie klientowi treści jego danych osobowych, z pominięciem wykonania kopii lub odpisu nośnika). Za każdą kolejną kopię administrator może pobrać opłatę (w rozsądnej wysokości, adekwatnej do poniesionych kosztów). Kolejna kopia oznacza ten sam zakres danych udostępniany przez administratora, niezależnie od zmiany treści danych (nawet jeśli zmienią się jakieś dane, np. wysokość salda).**

5. **Administrator realizuje prawo klienta do kopii danych tak, aby nie naruszyć praw i wolności innych osób (np. poprzez ujawnienie wizerunku lub głosu innych osób).**

6. PRAWO DO SPROSTOWANIA DANYCH

1. Klient ma prawo żądać, aby administrator:

JAK NAJSZYBCIEJ SPROSTOWAŁ JEGO DANE, KTÓRE SĄ NIEPRAWIDŁOWE	**UZUPEŁNIŁ NIEKOMPLETNE DANE - NA PODSTAWIE OŚWIADCZENIA KLIENTA**

2. Jeśli rejestr kredytowy dostanie żądanie sprostowania danych klienta banku, przekazuje je do banku i informuje o tym klienta. Tylko bank może potwierdzić, czy dane jego klienta są poprawne i je zaktualizować.

3. Administrator powinien przetwarzać prawidłowe dane klienta. Jeśli klient przekazuje informację o zmianie swoich danych, (np. nazwiska, adresu, numeru dokumentu tożsamości), należy te zmiany uwzględnić.

4. Administrator aktualizuje dane jak najszybciej, w tym u współpracujących z nim procesorów. Należy przy tym uwzględnić czas potrzebny, aby wprowadzić nowe dane do wszystkich baz danych lub systemów informatycznych do obsługi klientów.

5. Administrator może odmówić sprostowania lub uzupełnienia danych klienta, jeśli:

- wykaże, że nie jest w stanie zidentyfikować klienta w systemach (np. gdy klient przekazał za mało danych lub nie zweryfikował swojej tożsamości zgodnie z przyjętymi w danym banku procedurami),
- wskazane przez klienta dane są nieprawdziwe lub nieprawidłowe,
- nie ma określonego celu lub ważnej podstawy prawnej do przetwarzania danych (np. klient przekazuje dane o stanie zdrowia).

6. **Jeśli bank przekazuje dane klienta rejestrowi kredytowemu, powinien zapewnić aktualizację w zakresie zobowiązań klienta w ciągu 7 dni od wystąpienia okoliczności uzasadniających przekazanie informacji. Rejestr kredytowy powinien zaktualizować informacje najpóźniej 7 dni od ich otrzymania od banku.**

7. **Bank nie koryguje w rejestrach kredytowych prawidłowo przekazanej historii kredytowej. Jeśli klient spłacał zadłużenie nieterminowo, bank:**

- aktualizuje informację o obecnym stanie zadłużenia,
- nie koryguje informacji o opóźnieniach w spłacie, które miały miejsce w przeszłości.

7. PRAWO DO USUNIĘCIA DANYCH (DO BYCIA ZAPOMNIANYM)

1. **Klient ma prawo żądać, aby administrator, tak szybko jak to możliwe, usunął dotyczące go dane.**

2. **W niektórych przypadkach okoliczności nie uprawniają klienta do żądania usunięcia danych lub administrator musi lub może odmówić usunięcia danych w całości lub części. Obejmuje to między innymi sytuacje, gdy:**

- administrator realizuje przepisy prawa, które określają okres, przez który dane osobowe muszą być przetwarzane,
- klient ma aktywne produkty bankowe (np. ROR, nadal spłacany kredyt) lub produkty rejestru kredytowego,
- dane (nawet po zakończeniu umowy) są dalej przetwarzane w celu realizacji przez administratora czynności wynikających z prawnie uzasadnionych interesów, np. ustalania, dochodzenia roszczeń lub obrony przed nimi, rozpatrzenia reklamacji, wniosków oraz odwołań klienta,
- wynika to z przepisów prawa.

3. **Administrator dokonuje usunięcia danych osobowych pozwalających na identyfikację danej osoby w zbiorach klientów. Usunięcie może być zrealizowane np. poprzez skasowanie danych z systemów informatycznych, zniszczenie dokumentacji papierowej czy anonimizację danych (nadpisanie danych w sposób, który uniemożliwia przywrócenie danych i identyfikację klienta).**

4. **Jeśli rejestr kredytowy przetwarza dane przekazane przez bank, powinien usunąć je:**

- na podstawie dyspozycji banku (który realizuje żądanie klienta),
- samodzielnie, gdy minie przyjęty okres przetwarzania danych.

8. PRAWO DO OGRANICZENIA PRZETWARZANIA DANYCH OSOBOWYCH

1. **Klient ma prawo żądać, aby administrator ograniczył przetwarzanie jego danych osobowych. W praktyce oznacza to, że co do zasady administrator może te dane wyłącznie przechowywać.**

2. **Klient ma prawo skorzystać z prawa do ograniczenia przetwarzania danych, jeśli:**

- uważa, że przetwarzane dane są nieprawidłowe (na czas sprawdzenia prawidłowości danych przez administratora),
- sprzeciwia się usunięciu swoich danych, przetwarzanych bez właściwej podstawy prawnej (np. gdy okazało się, że przetwarzanie wynika z kradzieży tożsamości),
- wniósł sprzeciw wobec przetwarzania jego danych i czeka na decyzję administratora w tej sprawie,
- administrator nie potrzebuje już tych danych, ale potrzebuje ich klient, aby ustalić, dochodzić roszczeń lub się przed nimi bronić. Dotyczy to zwłaszcza sytuacji, gdy:
  - osoba trzecia wykorzystała je w nieuprawniony sposób (np. fraudy kredytowe),
  - są przedmiotem postępowania wyjaśniającego, które prowadzi administrator (wyłudzenia tożsamościowe).

9. PRAWO DO PRZENOSZENIA DANYCH

1. Klient ma prawo żądać przeniesienia swoich danych, które dostarczył administratorowi. Prawo to umożliwia przenoszenie danych osobowych klienta w formie elektronicznej do innego podmiotu.

2. Z prawa do przenoszenia danych klient może skorzystać, jeśli administrator przetwarza te dane na podstawie:

WYRAŻONEJ PRZEZ NIEGO ZGODY	**UMOWY, KTÓREJ KLIENT JEST STRONĄ LUB W ZWIĄZKU Z DZIAŁANIAMI PODEJMOWANYMI NA ŻĄDANIE KLIENTA, PRZED ZAWARCIEM UMOWY** (NP. ROZPATRZENIEM WNIOSKU KREDYTOWEGO)

3. Dane podlegające przenoszeniu to dane przetwarzane przez administratora w sposób zautomatyzowany (tzn. w formie elektronicznej, czyli znajdują się w systemach banku – klient nie może żądać przeniesienia danych znajdujących się w dokumentacji papierowej). Są to ponadto tylko te dane, które zostały przekazane administratorowi przez klienta – świadomie i aktywnie (np. imię i nazwisko) oraz dane wygenerowane przez działanie klienta (np. zdefiniowane operacje cykliczne w banku).

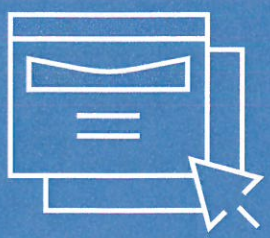
4. Za dane, które zostały przekazane administratorowi przez klienta „świadomie i aktywnie" nie uznaje się danych wytworzonych lub wywnioskowanych przez administratora, w szczególności stworzonego profilu klienta lub dotyczących go analiz.

5. Administrator może zwrócić się do klienta, aby doprecyzował zakres danych, które klient chce przenieść.

6. Administrator przeniesie dane objęte tajemnicą bankową, pod warunkiem wyrażenia zgody przez klienta na ujawnienie tych danych.

7. Administrator udostępnia dane klientowi w formie elektronicznej (np. e-mailem w dokumencie w formacie xlsx, zabezpieczonym hasłem).

8. Może dojść do sytuacji, w której administrator nie może oddzielić danych, które klient chce przenieść, od innych danych znajdujących się w systemach informatycznych (np. gdy część danych znajduje się na trwałych nośnikach, na których zapisane są również dane osób trzecich). W takiej sytuacji administrator może się powstrzymać z wykonaniem żądania klienta do czasu uzgodnienia z nim ostatecznego zakresu jego żądania i złożenia przez niego odpowiednich oświadczeń (zgód) niezbędnych do umożliwienia bankowi przekazania danych w innym zakresie niż pierwotnie wnioskowany. W przypadku braku uzgodnienia administrator przekaże informacje o powodzie odmowy.



10. PRAWO DO SPRZECIWU

1. **Klient ma prawo w określonych sytuacjach wnieść sprzeciw wobec przetwarzania jego danych osobowych. Administrator nie może już przetwarzać tych danych, jeśli sprzeciw jest uzasadniony.**

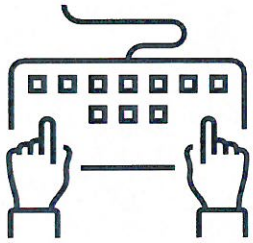
2. **Klient może wnieść sprzeciw wobec przetwarzania jego danych osobowych, jeśli administrator:**

PRZETWARZA DANE NA PODSTAWIE SWOJEGO PRAWNIE UZASADNIONEGO INTERESU

(albo gdy przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi), w tym za pomocą profilowania. Administrator może wciąż przetwarzać dane, jeśli wykaże, że posiada prawnie uzasadnione podstawy do dalszego przetwarzania tych danych, które są nadrzędne wobec interesów, praw i wolności podmiotu danych lub wykaże istnienie podstaw do ustalenia, dochodzenia lub obrony roszczeń

PRZETWARZA DANE NA POTRZEBY MARKETINGU BEZPOŚREDNIEGO

w tym profilowania. Po sprzeciwie administrator nie będzie już mógł przetwarzać danych w celach marketingowych



III. PRZECHOWYWANIE I USUWANIE DANYCH OSOBOWYCH

1. **Administrator może przechowywać dane osobowe nie dłużej niż jest to niezbędne, aby realizować cele przetwarzania.**

2. **Gdy administrator osiągnie zamierzone (pierwotne) cele przetwarzania, powinien zaprzestać przetwarzania danych osobowych, np. usunąć je lub zanonimizować, za wyjątkiem sytuacji kiedy określone przepisy prawa wymagają dalszego przechowywania danych, w szczególności:**

- **ustawa z 29 sierpnia 1997 r.** Prawo bankowe,
- **ustawa z 1 marca 2018 r.** o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu,
- **ustawa z 29 września 1994 r.** o rachunkowości,
- **ustawa z 29 sierpnia 1997 r.** Ordynacja podatkowa,
- **ustawa z 23 kwietnia 1964 r.** Kodeks cywilny,
- **ustawa z 29 lipca 2005 r.** o obrocie instrumentami finansowymi,
- **ustawa z 5 sierpnia 2015 r.** o rozpatrywaniu reklamacji przez podmioty rynku finansowego i o Rzeczniku Finansowym,
- **ustawa z 19 sierpnia 2011 r.** o usługach płatniczych,
- **ustawa z 9 października 2015 r.** o wykonywaniu Umowy między Rządem Rzeczypospolitej Polskiej a Rządem Stanów Zjednoczonych Ameryki w sprawie poprawy wypełniania międzynarodowych obowiązków podatkowych oraz wdrożenia ustawodawstwa FATCA,
- **ustawa z 9 marca 2017 r.** o wymianie informacji podatkowych z innymi państwami,
- **rozporządzenie Parlamentu Europejskiego i Rady (UE)** nr 575/2013 z 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych oraz zmieniającego rozporządzenie (UE) nr 648/2012.

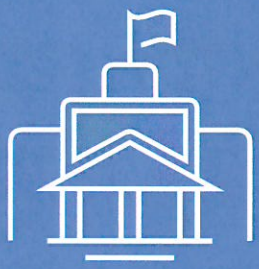
3. **Administrator może odmówić usunięcia danych osobowych w zakresie, w którym musi przetwarzać dane, aby ustalić, dochodzić roszczeń lub bronić się przed nimi. Dotyczy to również roszczeń jeszcze niezgłoszonych. Podstawa prawna odmowy wynika z:**

KODEKS CYWILNY

ustawy z 23 kwietnia 1964 r.

O ROZPATRYWANIU REKLAMACJI PRZEZ PODMIOTY RYNKU FINANSOWEGO I O RZECZNIKU FINANSOWYM

ustawy z 5 sierpnia 2015 r.



IV. PROFILOWANIE ORAZ ZAUTOMATYZOWANE PODEJMOWANIE DECYZJI

1. **Administrator może w określonych okolicznościach profilować klientów, tj. oceniać lub prognozować ich zachowania lub cechy na podstawie danych osobowych różnych osób, np.:**

- w celu oceny zdolności kredytowej klienta, od której zależy udzielenie kredytu, również z użyciem scoringu,
- zaoferowania mu spersonalizowanej oferty produktowej,
- przeciwdziałania praniu brudnych pieniędzy,
- identyfikacji działalności przestępczej.

2. **Scoring jest to metoda statystyczna, która pomaga ocenić szansę na to, że klient banku będzie spłacał swoje kredyty bez opóźnień. Metoda ta uwzględnia dane osób, które będą spłacały kredyt i informacje o ich dotychczasowych zachowaniach, które mają wpływ na ryzyko spłaty kredytów z opóźnieniami, jak np.:**

- czy spłata dotychczasowych kredytów miała miejsce z opóźnieniami,
- od jak dawna korzystają z kredytów,
- jak intensywnie wykorzystują limity kredytowe,
- czy mają stabilną sytuację ekonomiczno-finansową związaną m.in. z zatrudnieniem czy zamieszkaniem.

3. **Zasady badania zdolności kredytowej, którą przeprowadzają banki, w tym scoringu, wynikają z rekomendacji Urzędu Komisji Nadzoru Finansowego i są objęte jego nadzorem.**

4. Bank w celu oceny zdolności kredytowej i analizy ryzyka kredytowego może podejmować decyzje, opierając się wyłącznie na zautomatyzowanym przetwarzaniu, w tym profilowaniu. Dotyczy to również danych objętych tajemnicą bankową.

5. Bank może podejmować decyzje, o których mowa w ust. 4 powyżej, jedynie pod warunkiem zapewnienia osobie, której dotyczy decyzja, prawa do:

↓	↓	↓
trzymania stosownych wyjaśnień co do jej podstaw	do uzyskania interwencji ludzkiej w celu podjęcia ponownej decyzji (np. weryfikacji przez pracownika banku)	do wyrażenia własnego stanowiska

6. Przykładem decyzji podejmowanej w zautomatyzowany sposób może być udzielanie kredytów on-line. W tych procesach scoring może stanowić wyłączny element decyzji kredytowej i wówczas możemy mówić o zautomatyzowanej decyzji z użyciem scoringu. Może też być tak, że w pełni zautomatyzowana decyzja jest podejmowana bez użycia scoringu, tylko w oparciu o automatyczny proces (oparty o reguły polityki kredytowej), w którym scoringu nie ma. W większości przypadków scoring jest tylko jednym z elementów wpływających na ostateczną decyzję kredytową, nie jest więc czynnikiem decydującym samodzielnie.

7. Bank na wniosek osoby, która ubiega się o kredyt, ma obowiązek przekazać jej – w formie pisemnej – wyjaśnienie dotyczące oceny zdolności kredytowej. Wyjaśnienie musi obejmować informacje na temat czynników (w tym danych osobowych), które miały wpływ na ocenę zdolności kredytowej.

8. Bank może wykorzystywać w procesach zautomatyzowanego podejmowania decyzji, w tym profilowania, dane niezbędne z uwagi na cel i rodzaj kredytu. W szczególności są to dane określone w przepisach prawa (art. 105a ust. 1b Prawa bankowego), np.:

DANE KLIENTA	DANE DOTYCZĄCE ZOBOWIĄZANIA
(np. imię i nazwisko, miejsce pracy, forma zatrudnienia),	(np. kwota i waluta, warunki spłaty).

V. POWIERZENIE PRZETWARZANIA DANYCH OSOBOWYCH

1. Administrator może powierzyć przetwarzanie danych osobowych procesorowi. Procesor będzie przetwarzał dane w imieniu administratora i realizował wskazane przez niego cele.

2. Powierzenie przetwarzania danych osobowych przez administratora nie wymaga zgody klienta.

3. Administrator nie musi każdorazowo zawiadamiać klientów, gdy powierza przetwarzanie ich danych innemu procesorowi. Wystarczająca będzie ogólna informacja o odbiorcach danych lub ich kategoriach, przekazywana w ramach realizacji obowiązku określonego w rozdz. II, ust. 2.

4. Każde powierzenie przetwarzania danych administrator powinien uregulować umową (lub innym instrumentem prawnym, np. na podstawie decyzji organu administracji), w formie pisemnej lub elektronicznej.

5. Administrator powinien sprawdzić, czy podmiot, któremu planuje powierzyć przetwarzanie danych osobowych, zapewnia odpowiednie środki techniczne i organizacyjne, aby bezpiecznie przetwarzać dane osobowe, w tym:

CZY SPEŁNIA WYMOGI RODO

CZY ODPOWIEDNIO CHRONI PRAWA KLIENTÓW

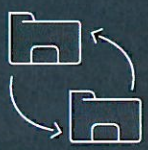
VI. NARUSZENIE OCHRONY DANYCH OSOBOWYCH

1. **Naruszenie ochrony danych osobowych to sytuacja, w której dane osobowe klienta przypadkowo lub niezgodnie z prawem będą:**

ZNISZCZONE

UTRACONE

ZMODYFIKOWANE



UJAWNIONE LUB UDOSTĘPNIONE
nieuprawnionemu odbiorcy

2. **Do naruszenia ochrony danych osobowych może dojść np. w wyniku:**

- działań lub zaniechań administratora lub podmiotu, któremu administrator powierzył przetwarzanie danych osobowych w swoim imieniu,
- nieuprawnionych działań innych podmiotów np. ataków hakerskich, phishingowych, vishingowych, smishingowych czy kradzieży tożsamości.

3. **Gdy wystąpi tego typu zdarzenie, administrator powinien:**

ODNOTOWAĆ JE W REJESTRZE NARUSZEŃ

JAK NAJSZYBCIEJ PRZEANALIZOWAĆ
czy w związku z nim mogło wystąpić istotne ryzyko naruszenia praw i wolności klienta

4. **Administrator ma obowiązek zgłosić naruszenie ochrony danych osobowych do Prezesa Urzędu Ochrony Danych Osobowych, chyba że jest mało prawdopodobne, że naruszenie skutkowało ryzykiem naruszenia praw i wolności osób fizycznych (np. prawa do prywatności). Powinien to zrobić w ciągu 72 h od momentu stwierdzenia naruszenia ochrony danych osobowych.**

5. **W sytuacji, gdy naruszenie może powodować wysokie ryzyko naruszenia praw lub wolności klienta, administrator powinien go o nim zawiadomić.**

6. **W zawiadomieniu o naruszeniu klient powinien dostać przede wszystkim poniższe informacje:**

- co się stało z jego danymi,
- na czym polegało naruszenie,
- jakie negatywne skutki może mieć dla niego to naruszenie,
- co zrobił lub proponuje zrobić administrator, żeby zaradzić naruszeniu oraz jego negatywnym skutkom,
- co klient może zrobić, aby ograniczyć te negatywne skutki,
- dane inspektora ochrony danych administratora lub innej osoby, od której może uzyskać więcej informacji.

7. **Administrator może powiadomić klienta o naruszeniu między innymi:**

- pocztą tradycyjną, e-mailem, SMS-em, telefonicznie – zarejestrowanych w banku lub innych wskazanych przez klienta, gdy naruszenie wynikało z nieaktualnych danych kontaktowych,
- w serwisie transakcyjnym lub aplikacji mobilnej, z których klient korzysta.

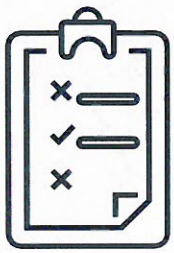
8. **W szczególnych przypadkach, np. gdy nie będzie możliwości, aby powiadomić indywidualnie klientów, których może dotyczyć naruszenie, administrator może opublikować w tej sprawie komunikat na swojej stronie internetowej lub w ogólnodostępnych mediach.**

9. W zależności od okoliczności, naruszenia ochrony danych osobowych mogą skutkować dla klienta negatywnymi skutkami, np.:

- kradzieżą lub sfałszowaniem jego tożsamości,
- stratą finansową (np. osoby trzecie mogą próbować uzyskać pożyczkę w instytucjach pozabankowych),
- naruszeniem dobrego imienia klienta lub utratą poufności danych osobowych,
- dostępem przez osobę nieupoważnioną do korzystania ze świadczeń opieki zdrowotnej,
- dostępem przez osobę nieupoważnioną do korzystania z praw obywatelskich,
- wyłudzeniem ubezpieczenia lub środków z ubezpieczenia na podstawie danych klienta,
- zarejestrowaniem na dane klienta przedpłaconej karty telefonicznej (tzw. prepaid),
- zawarciem na podstawie danych klienta umowy o świadczenie usług,
- przetwarzaniem danych osobowych klienta w celach marketingowych.

10. Aby klient mógł samodzielnie przeciwdziałać negatywnym skutkom naruszenia ochrony danych osobowych, administrator może zalecić, aby klient np.:

- zastrzegł lub wymienił dokument tożsamości
- założył konto w systemie informacji kredytowej lub gospodarczej, co pozwoli klientowi monitorować aktywność kredytową (np. alerty BIK)
- skorzystał z narzędzi do ochrony PESEL



VII. BEZPIECZEŃSTWO DANYCH OSOBOWYCH KLIENTÓW

1. **Administrator powinien zapewnić odpowiedni poziom bezpieczeństwa danych osobowych klientów oraz wdrożyć rozwiązania gwarantujące ochronę danych osobowych. Stosuje do tego odpowiednie środki techniczne i organizacyjne. Uwzględnia przy tym:**

- ogólny stan wiedzy technicznej,
- koszt wdrażania tych środków,
- charakter, zakres, kontekst i cele przetwarzania danych osobowych,
- ryzyko naruszenia praw lub wolności osób fizycznych o różnym prawdopodobieństwie wystąpienia i wadze zagrożenia.

2. **Wszystkie osoby zatrudnione w banku oraz osoby, za pośrednictwem których bank wykonuje czynności bankowe, mają obowiązek zachować tajemnicę bankową. Tajemnica bankowa obejmuje wszystkie informacje dotyczące czynności bankowej, uzyskane w czasie negocjacji, w trakcie zawierania i realizacji umowy, na podstawie której bank tę czynność wykonuje. Przypadki, w których nie obowiązuje tajemnica bankowa określa Prawo bankowe (w szczególności Rozdział 8 tej ustawy).**

***

ZWIĄZEK
BANKÓW
POLSKICH

Związek Banków Polskich,
ul. Kruczkowskiego 8, 00–380 Warszawa
mail: sekretariat@zbp.pl

Opracowanie graficzne: Polska Grupa Infograficzna (infograficy.pl)