PRZECIWDZIAŁANIE PRANIU PIENIĘDZY I FINANSOWANIU TERRORYZMU

PRZECIWDZIAŁANIE KORUPCJI

SZKOLENIE DLA PEŁNOMOCNIKÓW BANKU BNP PARIBAS BANK POLSKA S.A.

BNP PARIBAS BANK POLSKA S.A.
GRUDZIEŃ 2022

BNP PARIBAS

Bank zmieniającego się świata

CEL SZKOLENIA

- Zgodnie z Ustawą z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (Dz.U. 2018 poz. 723) wszystkie instytucje obowiązane (w tym Bank) mają obowiązek przeszkolenia osób wykonujących zadania związane z przeciwdziałaniem praniu pieniędzy oraz finansowaniem terroryzmu w zakresie związanym z realizacją tych obowiązków.
- Obowiązek wykonania szkolenia dotyczy nie tylko pracowników instytucji obowiązanej, ale również osób trzecich współpracujących z Bankiem (w szczególności dostawców lub pośredników).
- Szkolenie ma na celu przybliżenie zagadnień związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniem terroryzmu, w szczególności obowiązków dotyczących identyfikacji Klienta oraz weryfikacji jego tożsamości, identyfikacji beneficjenta rzeczywistego, identyfikacji osób zajmujących eksponowane stanowiska polityczne, identyfikacji transakcji podejrzanych oraz ich raportowania wynikających z ww. ustawy.

- Kwestie przeciwdziałania legalizacji środków finansowych pochodzących z przestępstw są w Polsce uregulowane również w:

  - **ustawie z dnia 6 czerwca 1997 r. Kodeks karny** (Dz. U. z 2016 r., poz. 1137, z późn. zm.) („Kodeks karny") – artykuły 165a i 299,
  - **ustawie z dnia 29 sierpnia 1997 r. Prawo bankowe** (Dz. U. z 2015 r., poz. 128, z późn. zm.) („Prawo bankowe") – artykuły 106, 107 i 108.

- Szkolenie ma również na celu przybliżenie:
  - podstawowych informacji z zakresu sankcji międzynarodowych,
  - podstawowych zagadnień związanych z ochroną danych osobowych.
  - Podstawowych informacji z zakresu przeciwdziałania korupcji.

AML – podstawowe informacje

AML – Anti Money Laundering
Przeciwdziałanie Praniu Pieniędzy

- **Pranie pieniędzy** polega na posiadaniu, używaniu, przekazywaniu lub wywożeniu za granicę, ukrywaniu, dokonywaniu transferu lub konwersji, pomaganiu w przenoszeniu lub posiadaniu albo podejmowaniu innych czynności, które mogą udaremnić lub znacznie utrudnić stwierdzenie przestępczego pochodzenia lub miejsca umieszczenia, wykrycia, zajęcia albo orzeczenia przepadku, środków płatniczych, instrumentów finansowych, papierów wartościowych, wartości dewizowych, praw majątkowych lub innych, mienia ruchomego lub nieruchomości, pochodzących z korzyści związanych z popełnieniem czynu zabronionego.

- **Etapy prania pieniędzy:**

CTF – podstawowe informacje

CTF – Caunter Financing of Terrorism
Przeciwdziałanie Finansowaniu Terroryzmu

- **Finansowanie terroryzmu** polega na przekazywaniu lub zbieraniu środków, aktywów lub usług, które mogą zostać użyte do ułatwiania lub dokonywania aktów terroru. Proces finansowania terroryzmu jest podobny do prania pieniędzy – w obu przypadkach usiłuje się ukryć ścieżkę przepływu pieniędzy przez system finansowy. Finansowanie terroryzmu, w przeciwieństwie do prania pieniędzy, jest trudniejsze do wykrycia, ponieważ często realizowane jest przy pomocy drobnych środków pieniężnych pochodzących z legalnych działań.

- **Etapy finansowania terroryzmu:**

Moja rola w procesach AML oraz CTF

Cel –identyfikacja Klienta

- **Dane identyfikacyjne w procesie weryfikacji tożsamości klienta, osoby upoważnionej do działania w jego imieniu oraz beneficjenta rzeczywistego są potwierdzane na podstawie:**
  - **a) dokumentu stwierdzającego tożsamość osoby fizycznej,**
  - **b) dokumentu zawierającego aktualne dane z wyciągu z właściwego rejestru,**
  - **c) innych dokumentów, danych lub informacji pochodzących z wiarygodnego i niezależnego źródła.**

Identyfikacja osób prawnych lub jednostek organizacyjnych

- Forma organizacyjna
- Nazwa (firma)
- Dane identyfikacyjne reprezentantów
- Adres siedziby lub prowadzenia działalności
- NIP lub nazwa rejestru handlowego, państwo rejestracji, numer i data rejestracji

Identyfikacja osób fizycznych

- Imię i Nazwisko
- Seria i numer dokumentu tożsamości
- Obywatelstwo
- Adres zamieszkania
- **PESEL** lub data urodzenia
- Państwo urodzenia
- Dodatkowo w przypadku prowadzenia działalności gospodarczej: Nazwa firmy, NIP, adres głównego miejsca wykonywania działalności

Moja rola w procesach AML oraz CTF

Cel – identyfikacja beneficjenta rzeczywistego

- **Ustalenie (identyfikacja) Beneficjenta rzeczywistego (Beneficjentów rzeczywistych) Klienta innego niż osoba fizyczna bądź osoba fizyczna prowadząca działalność gospodarczą (w tym także jako wspólnik spółki cywilnej) powinno odbywać się w oparciu o aktualną dokumentację, obejmującą kompletną strukturę własności i kontroli Klienta. Dokumentacja ta może być uzyskana z oficjalnego rejestru lub innego niezależnego i wiarygodnego źródła (np. zewnętrzne bazy danych, wywiadownie gospodarcze itp.), jak również przedłożona przez Klienta, z tym jednak zastrzeżeniem, że nie występują wątpliwości co do ich rzetelności.**

- **Beneficjent rzeczywisty** to osoba(y) sprawująca(e) kontrolę nad Klientem poprzez posiadane uprawnienia, umożliwiające wywieranie decydującego wpływu na czynności lub działania podejmowane przez Klienta, lub takie, w imieniu których są nawiązywane stosunki gospodarcze lub przeprowadzana jest transakcja okazjonalna. W szczególności jest to każda osoba fizyczna:

  - będąca udziałowcem lub akcjonariuszem, której przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji osoby prawnej,
  - dysponująca więcej niż 25% ogólnej liczby głosów w organie stanowiącym osoby prawnej, także jako zastawnik albo użytkownik lub na podstawie porozumień z innymi uprawnionymi do głosu,
  - sprawująca kontrolę nad osobą prawną lub osobami prawnymi, którym łącznie przysługuje prawo własności więcej niż 25% ogólnej liczby udziałów lub akcji lub które łącznie dysponują więcej niż 25% ogólnej liczby głosów w organie stanowiącym tej osoby prawnej, także jako zastawnik albo użytkownik lub na podstawie porozumień z innymi uprawnionymi do głosu,
  - sprawująca kontrolę nad osobą prawną poprzez posiadanie uprawnień, o których mowa w art. 3 ust. 1 pkt 37 ustawy z dnia 29 września 1994 r. o rachunkowości (Dz. U. z 2021 r. poz.217, z późn. zm),
  - zajmująca wyższe stanowisko kierownicze w przypadku udokumentowanego braku możliwości ustalenia lub wątpliwości co do tożsamości osób fizycznych określonych w tiret pierwszym, drugim, trzecim i czwartym oraz w przypadku niestwierdzenia podejrzeń prania pieniędzy lub finansowania terroryzmu.

- **Istnieją także szczególne przypadki, dla których przewidziano odrębne zasady ustalania beneficjenta rzeczywistego, tj. osoby fizyczne prowadzące działalność gospodarczą oraz trust.**

Moja rola w procesach AML oraz CTF

Cel – identyfikacja beneficjenta rzeczywistego

- **Nowelizacja Ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu przynosi kilka nowych wymogów w zakresie procesów KYC-AML:**
- Na etapie nawiązania relacji biznesowej wymagane jest ustalenie, czy Klient (korporacyjny lub instytucjonalny) posiada wpis w Centralnym Rejestrze Beneficjentów Rzeczywistych (CRBR). Dotyczy to jedynie pewnych konkretnych form prawnych, które wylicza Ustawa, a także niektórych podmiotów, zarejestrowanych w krajach UE;
- W przypadku ustalenia, że UBO są członkowie organu zarządzającego Klienta, wymagane jest odnotowanie okoliczności, które nie pozwoliły na wskazanie UBO z innej podstawy prawnej;
- Odnotowywać należy również wszelkie utrudnienia w weryfikacji tożsamości UBO;
- W odniesieniu do Klientów, którzy mają obowiązek posiadania wpisu w CRBR, Bank musi weryfikować treść tego wpisu z własnymi ustaleniami na temat tego, kto jest UBO Klienta oraz dane tej osoby (tych osób) w obu źródłach. W razie stwierdzenia rozbieżności, należy podjąć próbę ich wyjaśnienia, kontaktując się z Klientem. Brak wyjaśnienia przyczyn rozbieżności oznacza, że Bank musi zaraportować tę nieprawidłowość do organu administrującego CRBR.

Moja rola w procesach AML oraz CTF

Cel – identyfikacja osób zajmujących eksponowane stanowiska polityczne (PEP)

- **Przez osoby zajmujące eksponowane stanowiska polityczne (PEP) rozumie się przez to osoby fizyczne zajmujące znaczące stanowiska lub pełniące znaczące funkcje publiczne, z wyłączeniem grup stanowisk średniego i niższego szczebla, w tym:**
  - szefów państw, szefów rządów, ministrów, wiceministrów, sekretarzy stanu,
  - członków parlamentu lub podobnych organów ustawodawczych,
  - członków organów zarządzających partii politycznych,
  - członków sądów najwyższych, trybunałów konstytucyjnych oraz innych organów sądowych wysokiego szczebla, których decyzje nie podlegają zaskarżeniu, z wyjątkiem trybów nadzwyczajnych,
  - członków trybunałów obrachunkowych lub zarządów banków centralnych,
  - ambasadorów, chargés d'affaires oraz wyższych oficerów sił zbrojnych,
  - członków organów administracyjnych, zarządczych lub nadzorczych przedsiębiorstw państwowych, spółek z udziałem Skarbu Państwa, w których ponad połowa akcji albo udziałów należy do Skarbu Państwa lub innych państwowych osób prawnych ;
  - dyrektorów, zastępców dyrektorów oraz członków organów organizacji międzynarodowych lub osoby pełniące równoważne funkcje w tych organizacjach,
  - dyrektorów generalnych w urzędach naczelnych i centralnych organów państwowych, dyrektorów generalnych urzędów wojewódzkich,
  - inne osoby pełniące funkcje lub stanowiska publiczne w organach państwa lub centralnych organach administracji rządowej.
- **Status PEP przyznawany jest nie tylko osobom, które zajmują eksponowane stanowiska polityczne, ale również niektórym członkom ich rodzin oraz współpracownikom. Ich kategorie wymienia Ustawa.**
- **Szczegółowa lista tzw. krajowych stanowisk i funkcji PEP znajduje się w Rozporządzeniu Ministra Finansów, Funduszy i Polityki Regionalnej z dnia 27 lipca 2021 r. (Dz. U. 2021 poz. 1381).**

Moja rola w procesach AML oraz CTF

Cel - wykrywanie i zgłaszanie transakcji nietypowych

- **Każdy pracownik Banku lub osoba trzecia współpracująca z Bankiem przyjmująca do realizacji dyspozycję Klienta stanowi „pierwszą linię" obrony w procesie przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i podlega obowiązkowi dochowania należytej staranności, w tym identyfikacji i zgłoszenia wszelkich nietypowych transakcji.**

- **Przykładowe cechy transakcji nietypowych:**
  - Dziwne, wzbudzające podejrzenia zachowanie klienta (klient przejawia oznaki zdenerwowania, zaniepokojenia, strachu) podczas realizacji transakcji,
  - Klient jest obserwowany lub dokonuje transakcji w towarzystwie osób trzecich, względnie realizuje transakcje wynikające z polecenia osób trzecich,
  - Nietypowa (wysoka) kwota transakcji (np. wygląd Klienta nie uzasadnia posiadania przez niego odpowiednich środków finansowych do realizacji transakcji),
  - Nietypowy poziom złożoności (np. zakup na raty wielu różnych produktów „z wyższej półki" jednocześnie),
  - Brak oczywistego celu gospodarczego (np. nieuzasadniony zakup kilku produktów tego samego rodzaju).
  - Wysoka częstotliwość korzystania z produktów kredytowych (np. Klient w bardzo krótkich odstępach czasowych zaciąga wiele kredytów).

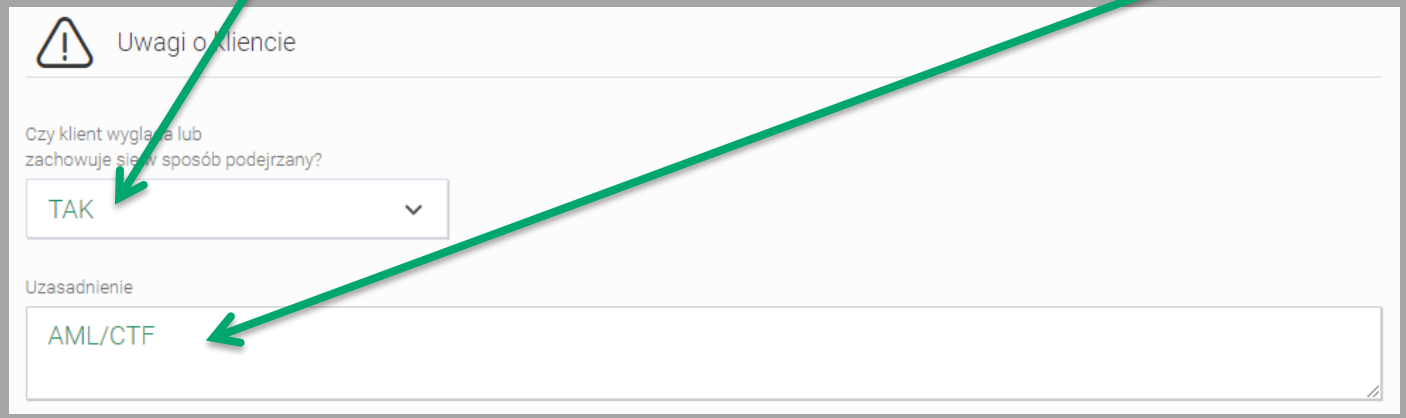
Uwaga!
Wymienione wyżej przypadki stanowią jedynie przykłady transakcji nietypowych, z którymi pracownik Banku lub osoba trzecia współpracująca z Bankiem może się zetknąć w ramach wykonywanych obowiązków.

Sposób zgłaszania transakcji nietypowych

- W przypadku wykrycia bądź podejrzenia przez dostawcę, pośrednika lub inna osobę trzecią współpracującą z Bankiem transakcji nietypowej należy **umieścić w aplikacji RATATU – we wniosku klienta - informację o podejrzanych okolicznościach transakcji**, a w przypadku gdy nie jest to możliwe, poinformować Przedstawiciela Banku BNP Paribas Bank Polska S.A., który odpowiada za współpracę z Państwem w ramach łączącej nas umowy.

Transakcje nietypowe oznaczamy w RATATU w procesie sporządzania wniosku dla klienta przez:

1. **Wskazanie TAK w polu „Czy klient wygląda lub zachowuje się w sposób podejrzany oraz**
2. **Wpisując z polu uzasadnienie „AML/ CTF”**



Co dalej dzieje się z moim zgłoszeniem?

- **Zgłoszenie transakcji podejrzanych do GIIF – BANK**

  Jeśli analiza po stronie Banku transakcji nietypowej nie wyjaśni wątpliwości, jednostka Compliance musi przesłać Generalnemu Inspektorowi Informacji Finansowej (GIIF) zgłoszenie dot. podejrzanych działań (SAR). Jednostka Compliance przekazuje również zgłoszenie do GIIF w przypadku otrzymania informacji o planowanej podejrzanej transakcji, a GIIF może podjąć działania zmierzające do jej wstrzymania lub do zablokowania rachunków klienta.

- Zgłoszenie transakcji podejrzanych realizowane jest niezwłocznie z zachowaniem pełnej poufności. Zabronione jest nie tylko ujawnianie faktu zgłoszenia dot. podejrzanych działań do GIIF, ale już tej okoliczności, że w odniesieniu do danego klienta/jego transakcji prowadzona jest analiza, która może (choć nie musi) zakończyć się przekazaniem zgłoszenia.

Jak zgłaszać incydenty związane z praniem pieniędzy lub finansowaniem terroryzmu oraz z naruszeniem sankcji?

- W przypadku, gdy pracownik, dostawca, pośrednik lub inna osoba współpracująca z Bankiem posiada wiedzę o naruszeniu (incydencie) przez Bank przepisów o przeciwdziałaniu praniu pieniędzy lub finansowaniu terroryzmu oraz o naruszeniu i podejrzeniu naruszenia sankcji finansowych, może dokonać anonimowego zgłoszenia takiego naruszenia za pośrednictwem odpowiednich kanałów komunikacji.
- **Incydent w zakresie naruszenia przepisów o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu** - szczególny typ naruszenia, stanowiący wyodrębnione zdarzenie lub ciąg zdarzeń, zachowanie lub postawę osoby/kilku osób, prowadzące do wystąpienia lub możliwości wystąpienia ryzyka nieprawidłowej realizacji przez Bank obowiązków wynikających z ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

- Dostępne kanały komunikacji:

  a) korespondencyjnie, na adres: **BNP Paribas Bank Polska S.A. ul. Kasprzaka 2, 01-211 Warszawa**

  (z dopiskiem: „Prezes Zarządu- Whistle-blowing", gdy zgłoszenie nie dotyczy bezpośrednio Członka Zarządu Banku lub z dopiskiem: „Rada Nadzorcza-Whistle-blowing", gdy zgłoszenie dotyczy co najmniej jednego z Członków Zarządu Banku),

  b) listownie za pośrednictwem skrzynki listowej umieszczonej w budynku Centrali Banku (koło Biura Podawczego)

  c) za pośrednictwem poczty elektronicznej, na adres: anonimowe.zgloszenia@bnpparibas.pl

  d) osobiście - ustnie na spotkaniu z Prezesem Zarządu Banku, gdy zgłoszenie nie dotyczy bezpośrednio Członka Zarządu Banku.

Sankcje międzynarodowe

CZYM SĄ SANKCJE?

Sankcje stosuje się w celu ograniczenia i powstrzymania dostrzeżonych zagrożeń dla bezpieczeństwa lub dostosowania międzynarodowych działań do uznanych norm międzynarodowych.

- **SANKCJE HANDLOWE -** mogą zakazywać eksportu (lub importu) określonych towarów, usług lub technologii do (lub z) określonych krajów i regionów, zwykle dotyczą broni i artykułów takich jak: ropa, drewno, złoto i diamenty lub sprzęt do użytku w sektorze jądrowym.

- **SANKCJE FINANSOWE -** generalnie obejmują działania zmierzające do zamrożenia aktywów w celu zablokowania dostępu do funduszy i zasobów gospodarczych określonym osobom i podmiotom. Sankcje finansowe mogą również obejmować zakaz przeprowadzania transakcji finansowych, takich jak przelewy, finansowanie (*), gwarancje i akredytywy dokumentowe, operacje na papierach wartościowych, wymiana zagraniczna itp.

SANKCJE MOGĄ DOTYCZYĆ:

- kraju lub regionu,
- towaru/usługi/technologii,
- osoby fizycznej,
- podmiotu prawnego,
- organizacji,
- statku.

Sankcje międzynarodowe

Sankcje są zazwyczaj nakładane przez międzynarodowe organy, takie jak Rada Bezpieczeństwa Organizacji Narodów Zjednoczonych, lub są inicjowane za pomocą lokalnego prawa lub regulacji.

- Programy sankcyjne mogą być wymierzone przeciw:
  - **CAŁEMU KRAJOWI LUB REGIONOWI (Iran, Syria, Kuba, Korea Północna oraz Krym/Sewastopol) -** polegają na zablokowaniu/zamrożeniu aktywów oraz odrzucaniu wszystkich transakcji handlowych. **Sankcjami objęty jest rząd danego kraju.**
  - **PODMIOTOM Z LISTY LUB PODMIOTOM O DANYM RODZAJU AKTYWNOŚCI -** obejmują środki przeznaczone dla wskazanych osób lub podmiotów i odnoszą się do embarg związanych z finansowaniem produktów podwójnego zastosowania związanych z obronnością lub do broni, które naruszają procesy demokratyczne itp. Wspólny grupowy wykaz składa się z list ONZ, Francji, Unii Europejskiej (UE), Stanów Zjednoczonych (USA) i BNP Paribas. **Sankcjami nie jest objęty rząd danego kraju.**

BNP Paribas i wszyscy pracownicy BNP Paribas mają obowiązek stosować się do sankcji nałożonych przez Organizację Narodów Zjednoczonych (ONZ), Unię Europejską (UE), Polskę (PL), Francję (FR) oraz Stany Zjednoczone (USA).

W dniu 16 kwietnia 2022 r. weszła w życie ustawa o szczególnych rozwiązaniach w zakresie przeciwdziałania wspieraniu agresji na Ukrainę oraz służących ochronie bezpieczeństwa narodowego, dająca możliwość stworzenia polskim władzom lokalnej listy sankcyjnej. Pierwszą polską listę sankcyjną ogłoszono w dniu 26 kwietnia 2022 r. - https://www.gov.pl/web/mswia/lista-osob-i-podmiotow-objetych-sankcjami

Dane osobowe – podstawowe informacje

- **Przetwarzanie i ochrona danych osobowych to istotne zadania realizowane przez Bank, również w procesach AML/CTF.**

- **Dane osobowe to wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej** (nazywa się ją „osobą, której dane dotyczą").

- **Możliwa do zidentyfikowania osoba fizyczna** to osoba, którą można bezpośrednio lub pośrednio zidentyfikować na podstawie identyfikatora takiego, jak np.: 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.
  - O danych osobowych nie mówimy zatem, gdy mamy na myśli spółkę z o.o., spółkę akcyjną, spółkę jawną, organizację, urząd. Jeśli natomiast będziemy mówić o osobach tworzących daną spółkę (członkach zarządu, prokurentach, wspólnikach) lub konkretnej osobie pełniącej funkcję w organizacji lub urzędzie – będziemy korzystać z ich danych osobowych.

- O jakie dane osobowe chodzi? W szczególności są to:
  imię i nazwisko, adres e-mail, numer telefonu, adres zamieszkania/zameldowania/korespondencyjny, numer PESEL, numer dowodu osobistego/skan lub kserokopia dowodu osobistego, miejsce pracy, adres IP itp.

- Bank przetwarza bardzo wiele danych osobowych dotyczących swoich pracowników oraz klientów. Te **dane zapisywane są na różnych nośnikach i w różnej postaci**:
  - jako dokumenty papierowe,
  - w pamięci komputerów służbowych,
  - na służbowych nośnikach zewnętrznych (pendrive, płyta CD, dysk zewnętrzny, itp.),
  - w skanach dokumentów,
  - na SharePoint, dyskach wspólnych oraz na platformach służących gromadzeniu dokumentów.

Ochrona danych osobowych

- **Bank podejmuje szereg działań służących zapewnieniu bezpieczeństwa tych danych i zminimalizowaniu ryzyka ich nieuprawnionego ujawnienia, zmiany lub skasowania**. Te działania to tzw. ochrona danych osobowych.

- W każdej chwili istnieje jednak ryzyko, że - z rozmaitych przyczyn - może dojść do sytuacji, gdy przetwarzane przez Bank dane konkretnej osoby zostaną w sposób nieuprawniony lub niepożądany usunięte, zmienione lub ujawnione osobom do tego niepowołanym.

- **Naruszenie ochrony danych to 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**.

- Do incydentu ochrony danych może dojść zarówno z winy lub błędu Banku bądź jego pracownika, jak również nieumyślnie lub w wyniku działania osoby trzeciej.

- Zgodnie z RODO* Bank ma obowiązek zapobiegać naruszeniom ochrony danych osobowych, co czyni, wprowadzając odpowiednie rozwiązania systemowe, techniczne i organizacyjne oraz poprzez szkolenia dla pracowników. Dodatkowo Bank jest zobowiązany podjąć określone działania w razie zaistnienia naruszenia ochrony danych osobowych: analiza, zgłoszenie do Urzędu Ochrony Danych Osobowych, powiadomienie podmiotów danych, wdrożenie działań naprawczych.

- **Każda osoba uczestnicząca w przetwarzaniu danych osobowych klientów Banku ma obowiązek przestrzegania zasad przetwarzania danych osobowych w celu zminimalizowania ryzyka naruszenia ich ochrony, a w razie zidentyfikowania potencjalnego naruszenia – niezwłocznie zgłosić to do Inspektora Ochrony Danych** – iodo@bnpparibas.pl. Jeśli masz wątpliwości, czy doszło do naruszenia, zgłoś je – Inspektor Ochrony Danych przeanalizuje sprawę i podejmie właściwe kroki.

** 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 - RODO*

Naruszenia ochrony danych osobowych - przykłady

Incydent danych osobowych może polegać na:

Naruszeniu poufności:

- ujawnisz hasło dostępu do komputera, aplikacji, platformy, narzędzia itp.
- zgubisz lub zostanie Ci skradziony dokument zawierający dane klienta (wniosek, umowa, notatka, itp.),
- wyślesz maila z danymi dotyczącymi klienta (np. z treścią umowy) przypadkowo na nieprawidłowy adres mailowy lub na nieprawidłowy adres korespondencyjny,
- wyślesz maila do kilku odbiorców będących klientami lub potencjalnymi klientami bez użycia funkcji UDW (ukryte do wiadomości),
- błędnie wprowadzisz adres e-mail, adres korespondencyjny lub numer telefonu klienta (w konsekwencji komunikacja adresowana do klienta może trafić do osoby trzeciej)

Naruszeniu dostępności:

- skasujesz dane na dysku lokalnym,
- w wyniku aktualizacji część danych na dysku lokalnym zostanie trwale usunięta lub dostęp do nich zostanie zablokowany,
- zgubisz, zostanie Ci skradziony lub zniszczony nośnik danych, w tym służbowy telefon komórkowy lub służbowy laptop,
- spłonie archiwum z dokumentami papierowymi,
- zignorujesz zmianę w danych, np. przestawione kolumny w Excel, pomieszane rekordy itp.

Naruszeniu integralności:

- omyłkowo wprowadzisz błędne dane Klienta, np. przestawione cyfry w numerze telefonu, literówka w adresie e-mail, imieniu lub nazwisku, nieprawidłowy adres korespondencyjny itp.
- przeniesiesz folder z danymi osobowymi do innej lokalizacji (np. na dysku wspólnym) dostępnej również osobom nieuprawnionym do wglądu w te dane itp.

ABC - Przeciwdziałanie Korupcji, cz. 1

„Zero tolerancji dla korupcji”

W Banku BNP Paribas obowiązuje „Kodeks postępowania Grupy BNP Paribas”, który precyzuje wartości Grupy BNP Paribas w zakresie współpracy z Partnerami Banku. Jedną z takich wartości jest „Zero tolerancji dla korupcji”.

Wszyscy pracownicy BNP Paribas oraz pracownicy Partnerów współpracujących z Bankiem zobowiązani są do przestrzegania przyjętych wartości i standardów etycznych. Kluczowe zasady określone w Kodeksie powinny stanowić inspirację dla wszystkich wspólnych działań oraz podejmowanych decyzji biznesowych.

Tekst "Kodeksu Postępowania Grupy BNP Paribas" jest opublikowany na stronie internetowej Banku - https://www.bnpparibas.pl/csr/strategia-csr/lad-korporacyjny

Pracownicy BNP Paribas oraz pracownicy Partnerów nie mogą w żadnych okolicznościach uczestniczyć, bezpośrednio ani pośrednio, w aktach korupcji lub niedozwolonej protekcji, które to akty są zakazane zarówno mocą prawa jak i zapisami wewnętrznymi Grupy.

Bank BNP Paribas w relacjach biznesowych jest zobowiązany stosować:

- ocenę podmiotów świadczących usługi w imieniu Banku pod kątem ryzyka korupcji
- procedury monitorowania przestrzegania przyjętych wartości i standardów etycznych
- wymogi polityki antykorupcyjnej obowiązującej w Grupie
- odpowiednią dokumentację umowną (klauzule antykorupcyjne, klauzule wystąpienia itp.),
- określone procedury przetargowe, w tym powstrzymać się od korzystania z usług niezatwierdzonych dostawców,

Nie wolno zawierać relacji biznesowych ani zobowiązań umownych, oferować stawek ani przyznawać prowizji, ani produktów lub usług BNP Paribas w zamian za nienależne korzyści lub jako warunek wywarcia wpływu.

Zakazane praktyki korupcyjne -> zakazane jest oferowanie lub wręczanie gratyfikacji czy też zabieganie o nią.

ABC - Przeciwdziałanie Korupcji, cz. 2

Akt korupcji to oferowanie lub wręczanie gratyfikacji, zabieganie o nią lub jej przyjmowanie (dotyczy to także samej obietnicy gratyfikacji w jakiejkolwiek formie) w celu wykorzystania swoich zawodowych prerogatyw (zarówno w sektorze publicznym, jak i prywatnym) dla uzyskania nienależnej korzyści.

➢ Gratyfikacja i jej przykłady

- Gratyfikacja może mieć formę pieniężną lub niepieniężną.
- Gratyfikacja może przybierać różne formy: gotówka, prezenty lub usługi, darowizny, obietnica lub oferta zatrudnienia, przekazywanie informacji poufnych lub wewnętrznych itp.
- Gratyfikacja może być udzielana bezpośrednio lub pośrednio (np. przez pośrednika).
- Gratyfikacją może być korzyść dla osoby pełniącej daną funkcję lub dla innej osoby (jej rodziny, współpracowników lub innych osób).
- Gratyfikacja jest środkiem prowadzącym do przekazania tzw. nienależnej korzyści.

➢ Upominki i zaproszenia

Nigdy nie powinno się domagać w sposób jawny ani dorozumiany jakichkolwiek korzyści lub innych gratyfikacji w trakcie swojej działalności zawodowej w zamian za decyzję lub wpływanie na decyzję.

W szczególności w ramach swojej działalności zawodowej nie można bezpośrednio ani pośrednio:

- Oferować prezentów/zaproszeń na własny koszt;
- Prosić o prezent;
- Przyjmować ani oferować prezentów lub płatności gotówką lub ekwiwalentem gotówki;
- Otrzymywać wynagrodzenie za usługi profesjonalne;
- Przyjmować świadczeń (osobistych lub dla członka rodziny lub bliskiego krewnego) z zapisu klienta, darowizny lub ubezpieczenia na życie itp.

➢ Konflikty Interesów

Ponieważ większość sytuacji związanych z korupcją wiąże się z nieujawnionymi lub niezarządzanymi konfliktami interesów, to ważne jest, aby rozumieć i identyfikować potencjalne lub rzeczywiste konflikty interesów. Dzięki temu można zgłaszać konflikty interesów, gdy jest to stosowne, a Bank może zarządzać konfliktami interesów zgodnie z przyjętą regulacją w tym zakresie.

➢ Zgłaszanie

Należy zgłaszać wszelkie podejrzenia oraz zdarzenia mogące świadczyć o korupcji.

Podsumowanie

- Pranie pieniędzy i finansowanie terroryzmu to **problem społeczny i gospodarczy**, którym dotknięte są wszystkie nacje świata.

- Głównym ogniwem systemu **walczącego z tym zjawiskiem są instytucje bankowe.** Z tego właśnie powodu są one przedmiotem ścisłych uregulowań. Uregulowania te przewidują, zarówno dla instytucji, jak i ich pracowników **sankcje dyscyplinarne, finansowe i karne**.

- Oprócz tych sankcji instytucje i ich pracownicy ponoszą **ryzyko utraty reputacji**.

- Instytucje finansowe wykorzystują różnorodne środki, narzędzia IT i skomplikowane procesy, kluczową rolę odgrywa jednak **stała czujność wszystkich pracowników**.

AML/CTF to sprawa nas wszystkich!